AECOM

Project Manual

North Carolina Air National Guard, 145th Airlift Wing
Charlotte Air National Guard Base
Construct Security Forces Building

Project No.: FJRP229030

B-3 Submittal - Final
May 30, 2025

Volume 2: Divisions 22-33

SECTION TABLE OF CONTENTS

DIVISION 22 - PLUMBING

SECTION 22 00 00

PLUMBING, GENERAL PURPOSE

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 STANDARD PRODUCTS
1.3.1 Alternative Qualifications
1.3.2 Service Support
1.3.3 Manufacturer's Nameplate
1.3.4 Modification of References
1.3.4.1 Definitions
1.3.4.2 Administrative Interpretations
1.4 DELIVERY, STORAGE, AND HANDLING
1.5 PERFORMANCE REQUIREMENTS
1.5.1 Welding
1.6 REGULATORY REQUIREMENTS
1.7 PROJECT/SITE CONDITIONS
1.8 INSTRUCTION TO GOVERNMENT PERSONNEL
1.9 ACCESSIBILITY OF EQUIPMENT

PART 2 PRODUCTS

2.1 MATERIALS
2.1.1 Pipe Joint Materials
2.1.2 Miscellaneous Materials
2.1.3 Pipe Insulation Material
2.2 PIPE HANGERS, INSERTS, AND SUPPORTS
2.3 VALVES
2.3.1 Backwater Valves
2.3.2 Wall Faucets
2.3.3 Wall Hydrants (Frostproof)
2.3.4 Relief Valves
2.3.5 Thermostatic Mixing Valves
2.4 FIXTURES
2.5 BACKFLOW PREVENTERS
2.6 DRAINS
2.6.1 Floor and Shower Drains
2.6.1.1 Metallic Shower Pan Drains
2.6.1.2 Drains and Backwater Valves
2.6.2 Floor Sinks
2.6.3 Roof Drains and Expansion Joints
2.7 TRAPS
2.8 WATER HEATERS
2.9 PUMPS
2.9.1 Sump Pumps
2.9.2 Circulating Pumps
2.9.3 Flexible Connectors

2.10 DOMESTIC WATER SERVICE METER
2.11 ELECTRICAL WORK
2.12 Clean-outs
2.13 MISCELLANEOUS PIPING ITEMS
2.13.1 Escutcheon Plates
2.13.2 Pipe Sleeves
2.13.2.1 Sleeves in Masonry and Concrete
2.13.2.2 Sleeves Not in Masonry and Concrete
2.13.3 Pipe Hangers (Supports)
2.13.4 Nameplates

PART 3 EXECUTION

3.1 GENERAL INSTALLATION REQUIREMENTS
3.1.1 Water Pipe, Fittings, and Connections
3.1.1.1 Utilities
3.1.1.2 Cutting and Repairing
3.1.1.3 Protection of Fixtures, Materials, and Equipment
3.1.1.4 Mains, Branches, and Runouts
3.1.1.5 Pipe Drains
3.1.1.6 Expansion and Contraction of Piping
3.1.1.7 Thrust Restraint
3.1.1.8 Commercial-Type Water Hammer Arresters
3.1.2 Joints
3.1.2.1 Threaded
3.1.2.2 Mechanical Couplings
3.1.2.3 Unions and Flanges
3.1.2.4 Grooved Mechanical Joints
3.1.2.5 Cast Iron Soil, Waste and Vent Pipe
3.1.2.6 Copper Tube and Pipe
3.1.2.7 Plastic Pipe
3.1.2.8 Glass Pipe
3.1.2.9 Corrosive Waste Plastic Pipe
3.1.2.10 Polypropylene Pipe
3.1.2.11 Other Joint Methods
3.1.3 Dissimilar Pipe Materials
3.1.4 Corrosion Protection for Buried Pipe and Fittings
3.1.5 Pipe Sleeves and Flashing
3.1.5.1 Sleeve Requirements
3.1.5.2 Flashing Requirements
3.1.5.3 Waterproofing
3.1.5.4 Optional Counterflashing
3.1.5.5 Pipe Penetrations of Slab on Grade Floors
3.1.5.6 Pipe Penetrations
3.1.6 Fire Seal
3.1.7 Supports
3.1.7.1 General
3.1.7.2 Pipe Supports and Structural Bracing, Seismic Requirements
3.1.7.3 Pipe Hangers, Inserts, and Supports
3.1.7.4 Structural Attachments
3.1.8 Welded Installation
3.1.9 Pipe Cleanouts
3.2 WATER HEATERS AND HOT WATER STORAGE TANKS
3.2.1 Relief Valves
3.2.2 Heat Traps
3.2.3 Connections to Water Heaters
3.2.4 Expansion Tank
3.3 FIXTURES AND FIXTURE TRIMMINGS
3.3.1 Fixture Connections

3.3.2 Flushometer Valves
3.3.3 Height of Fixture Rims Above Floor
3.3.4 Shower Bath Outfits
3.3.5 Fixture Supports
3.3.5.1 Support for Solid Masonry Construction
3.3.5.2 Support for Concrete-Masonry Wall Construction
3.3.5.3 Support for Steel Stud Frame Partitions
3.3.5.4 Support for Wood Stud Construction
3.3.5.5 Wall-Mounted Water Closet Gaskets
3.3.6 Backflow Prevention Devices
3.3.7 Access Panels
3.3.8 Sight Drains
3.3.9 Traps
3.3.10 Shower Pans
3.3.10.1 General
3.3.10.2 Metal Shower Pans
3.3.10.3 Plasticized Chlorinated Polyethylene Shower Pans
3.3.10.4 Nonplasticized Polyvinyl Chloride (PVC) Shower Pans
3.4 VIBRATION-ABSORBING FEATURES
3.5 WATER METER REMOTE READOUT REGISTER
3.6 IDENTIFICATION SYSTEMS
3.6.1 Identification Tags
3.6.2 Pipe Color Code Marking
3.6.3 Color Coding Scheme for Locating Hidden Utility Components
3.7 ESCUTCHEONS
3.8 PAINTING
3.8.1 Painting of New Equipment
3.8.1.1 Factory Painting Systems
3.8.1.2 Shop Painting Systems for Metal Surfaces
3.9 TESTS, FLUSHING AND DISINFECTION
3.9.1 Plumbing System
3.9.1.1 Test of Backflow Prevention Assemblies
3.9.1.2 Shower Pans
3.9.2 Defective Work
3.9.3 System Flushing
3.9.3.1 During Flushing
3.9.3.2 After Flushing
3.9.4 Operational Test
3.9.5 Disinfection
3.10 POSTED INSTRUCTIONS
3.11 PERFORMANCE OF WATER HEATING EQUIPMENT
3.11.1 Storage Water Heaters
3.11.1.1 Electric
3.12 TABLES

-- End of Section Table of Contents --

SECTION 22 00 00

PLUMBING, GENERAL PURPOSE

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

ANSI Z21.22/CSA 4.4	(2015; R 2020) Relief Valves for Hot Water Supply Systems

AMERICAN SOCIETY OF MECHANICAL ENGINEERS (ASME)

ASME A112.1.2	(2012; R 2017; R 2022) Air Gaps in Plumbing Systems (For Plumbing Fixtures and Water-Connected Receptors)
ASME A112.6.1M	(1997; R 2017) Floor Affixed Supports for Off-the-Floor Plumbing Fixtures for Public Use
ASME A112.6.3	(2019) Standard for Floor and Trench Drains
ASME A112.6.4	(2003: R 2012) Roof, Deck and Balcony Drains
ASME A112.14.1	(2003; R 2017; R 2022) Backwater Valves
ASME A112.36.2M	(1991; R 2017) Cleanouts
ASME B1.20.1	(2013; R 2018) Pipe Threads, General Purpose (Inch)
ASME B16.3	(2021) Malleable Iron Threaded Fittings, Classes 150 and 300
ASME B16.5	(2020) Pipe Flanges and Flanged Fittings NPS 1/2 Through NPS 24 Metric/Inch Standard
ASME B16.15	(2018) Cast Copper Alloy Threaded Fittings Classes 125 and 250
ASME B16.18	(2021) Cast Copper Alloy Solder Joint Pressure Fittings
ASME B16.21	(2021) Nonmetallic Flat Gaskets for Pipe Flanges
ASME B16.22	(2021) Wrought Copper and Copper Alloy Solder Joint Pressure Fittings

ASME B16.23	(2021) Cast Copper Alloy Solder Joint Drainage Fittings - DWV
ASME B16.24	(2022) Cast Copper Alloy Pipe Flanges, Flanged Fittings, and Valves Classes 150, 300, 600, 900, 1500, and 2500
ASME B16.29	(2017) Wrought Copper and Wrought Copper Alloy Solder-Joint Drainage Fittings - DWV
ASME B16.34	(2021) Valves - Flanged, Threaded and Welding End
ASME B16.39	(2020) Standard for Malleable Iron Threaded Pipe Unions; Classes 150, 250, and 300
ASME B16.50	(2021) Wrought Copper and Copper Alloy Braze-Joint Pressure Fittings
ASME B16.51	(2013) Copper and Copper Alloy Press-Connect Pressure Fittings
ASME B31.1	(2020) Power Piping
ASME B31.5	(2020) Refrigeration Piping and Heat Transfer Components
ASME B40.100	(2013) Pressure Gauges and Gauge Attachments
ASME BPVC SEC IV	(2017) BPVC Section IV-Rules for Construction of Heating Boilers
ASME BPVC SEC IX	(2017; Errata 2018) BPVC Section IX-Welding, Brazing and Fusing Qualifications
ASME CSD-1	(2021) Control and Safety Devices for Automatically Fired Boilers

AMERICAN SOCIETY OF SANITARY ENGINEERING (ASSE)

ASSE 1001	(2021) Performance Requirements for Atmospheric Type Vacuum Breakers
ASSE 1003	(2020) Performance Requirements for Water Pressure Reducing Valves for Domestic Water Distribution Systems - (ANSI approved 2010)
ASSE 1010	(2021) Performance Requirements for Water Hammer Arresters
ASSE 1011	(2017) Performance Requirements for Hose Connection Vacuum Breakers
ASSE 1012	(2021) Performance Requirements for

	Backflow Preventer with an Intermediate Atmospheric Vent
ASSE 1013	(2021) Performance Requirements for Reduced Pressure Principle Backflow Prevention Assemblies
ASSE 1018	(2001; R 2021) Performance Requirements for Trap Seal Primer Valves - Potable Water Supplied (ANSI Approved 2002
ASSE 1019	(2011; R 2016) Performance Requirements for Wall Hydrant with Backflow Protection and Freeze Resistance
ASSE 1020	(2020) Performance Requirements for Pressure Vacuum Breaker Assemblies

AMERICAN WATER WORKS ASSOCIATION (AWWA)

AWWA B300	(2018) Hypochlorites
AWWA B301	(2018) Liquid Chlorine
AWWA C203	(2020) Coal-Tar Protective Coatings and Linings for Steel Water Pipelines - Enamel and Tape - Hot-Applied
AWWA C606	(2015) Grooved and Shouldered Joints
AWWA C651	(2014) Standard for Disinfecting Water Mains
AWWA C652	(2019) Disinfection of Water-Storage Facilities
AWWA C700	(2020) Cold-Water Meters - Displacement Type, Metal Alloy Main Case
AWWA C701	(2019) Cold-Water Meters - Turbine Type for Customer Service

AMERICAN WELDING SOCIETY (AWS)

AWS A5.8/A5.8M	(2019) Specification for Filler Metals for Brazing and Braze Welding
AWS B2.2/B2.2M	(2016) Specification for Brazing Procedure and Performance Qualification

ASTM INTERNATIONAL (ASTM)

ASTM A47/A47M	(1999; R 2018; E 2018) Standard Specification for Ferritic Malleable Iron Castings
ASTM A53/A53M	(2022) Standard Specification for Pipe, Steel, Black and Hot-Dipped, Zinc-Coated, Welded and Seamless

ASTM A74	(2021) Standard Specification for Cast Iron Soil Pipe and Fittings
ASTM A105/A105M	(2021) Standard Specification for Carbon Steel Forgings for Piping Applications
ASTM A183	(2014; R 2020) Standard Specification for Carbon Steel Track Bolts and Nuts
ASTM A193/A193M	(2020) Standard Specification for Alloy-Steel and Stainless Steel Bolting Materials for High-Temperature Service and Other Special Purpose Applications
ASTM A515/A515M	(2017) Standard Specification for Pressure Vessel Plates, Carbon Steel, for Intermediate- and Higher-Temperature Service
ASTM A516/A516M	(2017) Standard Specification for Pressure Vessel Plates, Carbon Steel, for Moderate- and Lower-Temperature Service
ASTM A536	(1984; R 2019; E 2019) Standard Specification for Ductile Iron Castings
ASTM A733	(2016) Standard Specification for Welded and Seamless Carbon Steel and Austenitic Stainless Steel Pipe Nipples
ASTM A888	(2021a) Standard Specification for Hubless Cast Iron Soil Pipe and Fittings for Sanitary and Storm Drain, Waste, and Vent Piping Applications
ASTM B32	(2020) Standard Specification for Solder Metal
ASTM B42	(2020) Standard Specification for Seamless Copper Pipe, Standard Sizes
ASTM B43	(2020) Standard Specification for Seamless Red Brass Pipe, Standard Sizes
ASTM B88	(2020) Standard Specification for Seamless Copper Water Tube
ASTM B88M	(2020) Standard Specification for Seamless Copper Water Tube (Metric)
ASTM B117	(2019) Standard Practice for Operating Salt Spray (Fog) Apparatus
ASTM B306	(2020) Standard Specification for Copper Drainage Tube (DWV)
ASTM B370	(2022) Standard Specification for Copper Sheet and Strip for Building Construction

ASTM B584	(2014; R 2022) Standard Specification for Copper Alloy Sand Castings for General Applications
ASTM B813	(2016) Standard Specification for Liquid and Paste Fluxes for Soldering of Copper and Copper Alloy Tube
ASTM B828	(2016) Standard Practice for Making Capillary Joints by Soldering of Copper and Copper Alloy Tube and Fittings
ASTM C564	(2020a) Standard Specification for Rubber Gaskets for Cast Iron Soil Pipe and Fittings
ASTM C920	(2018) Standard Specification for Elastomeric Joint Sealants
ASTM D1248	(2016) Standard Specification for Polyethylene Plastics Extrusion Materials for Wire and Cable
ASTM D2000	(2018) Standard Classification System for Rubber Products in Automotive Applications
ASTM D2657	(2007; R 2015) Heat Fusion Joining Polyolefin Pipe and Fittings
ASTM D2822/D2822M	(2005; R 2011; E 2011) Standard Specification for Asphalt Roof Cement, Asbestos-Containing
ASTM D2846/D2846M	(2019) Standard Specification for Chlorinated Poly(Vinyl Chloride) (CPVC) Plastic Hot- and Cold-Water Distribution Systems
ASTM D3138	(2004; R 2016) Standard Specification for Solvent Cements for Transition Joints Between Acrylonitrile-Butadiene-Styrene (ABS) and Poly(Vinyl Chloride) (PVC) Non-Pressure Piping Components
ASTM D3139	(2019) Joints for Plastic Pressure Pipes Using Flexible Elastomeric Seals
ASTM D3212	(2020) Standard Specification for Joints for Drain and Sewer Plastic Pipes Using Flexible Elastomeric Seals
ASTM D3311	(2017) Standard Specification for Drain, Waste, and Vent (DWV) Plastic Fittings Patterns
ASTM E1	(2014) Standard Specification for ASTM Liquid-in-Glass Thermometers

ASTM F437	(2021) Standard Specification for Threaded Chlorinated Poly(Vinyl Chloride) (CPVC) Plastic Pipe Fittings, Schedule 80
ASTM F438	(2017) Standard Specification for Socket-Type Chlorinated Poly(Vinyl Chloride) (CPVC) Plastic Pipe Fittings, Schedule 40
ASTM F439	(2019) Standard Specification for Chlorinated Poly(Vinyl Chloride) (CPVC) Plastic Pipe Fittings, Schedule 80
ASTM F441/F441M	(2020) Standard Specification for Chlorinated Poly(Vinyl Chloride) (CPVC) Plastic Pipe, Schedules 40 and 80
ASTM F442/F442M	(2020) Standard Specification for Chlorinated Poly(Vinyl Chloride) (CPVC) Plastic Pipe (SDR-PR)
ASTM F477	(2014; R 2021) Standard Specification for Elastomeric Seals (Gaskets) for Joining Plastic Pipe
ASTM F493	(2020) Standard Specification for Solvent Cements for Chlorinated Poly (Vinyl Chloride) (CPVC) Plastic Pipe and Fittings
ASTM F1290	(2019) Standard Practice for Electrofusion Joining Polyolefin Pipe and Fittings
ASTM F2389	(2021) Standard Specification for Pressure-rated Polypropylene (PP) Piping Systems

CAST IRON SOIL PIPE INSTITUTE (CISPI)

CISPI 301	(2018) Hubless Cast Iron Soil Pipe and Fittings for Sanitary and Storm Drain, Waste, and Vent Piping Applications
CISPI 310	(2012) Coupling for Use in Connection with Hubless Cast Iron Soil Pipe and Fittings for Sanitary and Storm Drain, Waste, and Vent Piping Applications

COPPER DEVELOPMENT ASSOCIATION (CDA)

CDA A4015	(2016; 14/17) Copper Tube Handbook

INTERNATIONAL ASSOCIATION OF PLUMBING AND MECHANICAL OFFICIALS (IAPMO)

IAPMO PS 117	(2005b) Press Type Or Plain End Rub Gasketed W/ Nail CU & CU Alloy Fittings 4 Install On CU Tubing
IAPMO UPC	(2003) Uniform Plumbing Code

INTERNATIONAL CODE COUNCIL (ICC)

ICC A117.1	(2017) Standard And Commentary Accessible and Usable Buildings and Facilities
ICC IPC	(2021) International Plumbing Code

MANUFACTURERS STANDARDIZATION SOCIETY OF THE VALVE AND FITTINGS INDUSTRY (MSS)

MSS SP-25	(2018) Standard Marking System for Valves, Fittings, Flanges and Unions
MSS SP-44	(2019) Steel Pipeline Flanges
MSS SP-58	(2018) Pipe Hangers and Supports - Materials, Design and Manufacture, Selection, Application, and Installation
MSS SP-67	(2022) Butterfly Valves
MSS SP-70	(2011) Gray Iron Gate Valves, Flanged and Threaded Ends
MSS SP-71	(2018) Gray Iron Swing Check Valves, Flanged and Threaded Ends
MSS SP-72	(2010a) Ball Valves with Flanged or Butt-Welding Ends for General Service
MSS SP-78	(2011) Cast Iron Plug Valves, Flanged and Threaded Ends
MSS SP-80	(2019) Bronze Gate, Globe, Angle and Check Valves
MSS SP-83	(2014) Class 3000 Steel Pipe Unions Socket Welding and Threaded
MSS SP-85	(2011) Gray Iron Globe & Angle Valves Flanged and Threaded Ends
MSS SP-110	(2010) Ball Valves Threaded, Socket-Welding, Solder Joint, Grooved and Flared Ends

NACE INTERNATIONAL (NACE)

NACE SP0169	(2013) Control of External Corrosion on Underground or Submerged Metallic Piping Systems

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA 250	(2020) Enclosures for Electrical Equipment (1000 Volts Maximum)
NEMA MG 1	(2021) Motors and Generators

NEMA MG 11	(1977; R 2012) Energy Management Guide for Selection and Use of Single Phase Motors

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 90A	(2021) Standard for the Installation of Air Conditioning and Ventilating Systems

NSF INTERNATIONAL (NSF)

NSF 372	(2016) Drinking Water System Components - Lead Content
NSF/ANSI 14	(2021) Plastics Piping System Components and Related Materials
NSF/ANSI 61	(2022) Drinking Water System Components - Health Effects

PLASTIC PIPE AND FITTINGS ASSOCIATION (PPFA)

PPFA Fire Man	(2016) Firestopping: Plastic Pipe in Fire Resistive Construction

PLUMBING AND DRAINAGE INSTITUTE (PDI)

PDI WH 201	(2010) Water Hammer Arresters Standard

SOCIETY OF AUTOMOTIVE ENGINEERS INTERNATIONAL (SAE)

SAE J1508	(2009) Hose Clamp Specifications

U.S. ENVIRONMENTAL PROTECTION AGENCY (EPA)

EPA SM 9223	(2004) Enzyme Substrate Coliform Test
PL 93-523	(1974; A 1999) Safe Drinking Water Act

U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)

40 CFR 141.80	National Primary Drinking Water Regulations; Control of Lead and Copper; General Requirements

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-03 Product Data

Backflow Prevention Assemblies

Fixtures

List of installed fixtures with manufacturer, model, and flow rate.

Water Heaters

Pumps

Welding

A copy of qualified procedures and a list of names and identification symbols of qualified welders and welding operators.

Vibration-Absorbing Features

Details of vibration-absorbing features, including arrangement, foundation plan, dimensions and specifications.

Plumbing System

Diagrams, instructions, and other sheets proposed for posting. Manufacturer's recommendations for the installation of bell and spigot and hubless joints for cast iron soil pipe.

SD-06 Test Reports

Tests, Flushing and Disinfection

Test reports in booklet form showing all field tests performed to adjust each component and all field tests performed to prove compliance with the specified performance criteria, completion and testing of the installed system. Each test report shall indicate the final position of controls.

Test of Backflow Prevention Assemblies.

Certification of proper operation shall be as accomplished in accordance with state regulations by an individual certified by the state to perform such tests. If no state requirement exists, the Contractor shall have the manufacturer's representative test the device, to ensure the unit is properly installed and performing as intended. The Contractor shall provide written documentation of the tests performed and signed by the individual performing the tests.

SD-07 Certificates

Materials and Equipment

Where equipment is specified to conform to requirements of the ASME Boiler and Pressure Vessel Code, the design, fabrication, and installation shall conform to the code.

Bolts

Written certification by the bolt manufacturer that the bolts furnished comply with the specified requirements.

SD-10 Operation and Maintenance Data

Plumbing System

Submit in accordance with Section 01 78 23 OPERATION AND MAINTENANCE DATA.

1.3 STANDARD PRODUCTS

Specified materials and equipment shall be standard products of a manufacturer regularly engaged in the manufacture of such products. Specified equipment shall essentially duplicate equipment that has performed satisfactorily at least two years prior to bid opening. Standard products shall have been in satisfactory commercial or industrial use for 2 years prior to bid opening. The 2-year use shall include applications of equipment and materials under similar circumstances and of similar size. The product shall have been for sale on the commercial market through advertisements, manufacturers' catalogs, or brochures during the 2 year period.

1.3.1 Alternative Qualifications

Products having less than a two-year field service record will be acceptable if a certified record of satisfactory field operation for not less than 6000 hours, exclusive of the manufacturer's factory or laboratory tests, can be shown.

1.3.2 Service Support

The equipment items shall be supported by service organizations. Submit a certified list of qualified permanent service organizations for support of the equipment which includes their addresses and qualifications. These service organizations shall be reasonably convenient to the equipment installation and able to render satisfactory service to the equipment on a regular and emergency basis during the warranty period of the contract.

1.3.3 Manufacturer's Nameplate

Each item of equipment shall have a nameplate bearing the manufacturer's name, address, model number, and serial number securely affixed in a conspicuous place; the nameplate of the distributing agent will not be acceptable.

1.3.4 Modification of References

In each of the publications referred to herein, consider the advisory provisions to be mandatory, as though the word, "shall" had been substituted for "should" wherever it appears. Interpret references in these publications to the "authority having jurisdiction", or words of similar meaning, to mean the Contracting Officer.

1.3.4.1 Definitions

For the International Code Council (ICC) Codes referenced in the contract documents, advisory provisions shall be considered mandatory, the word "should" shall be interpreted as "shall." Reference to the "code official" shall be interpreted to mean the "Contracting Officer." For Navy owned property, references to the "owner" shall be interpreted to mean the "Contracting Officer." For leased facilities, references to the "owner" shall be interpreted to mean the "lessor." References to the

"permit holder" shall be interpreted to mean the "Contractor."

1.3.4.2 Administrative Interpretations

For ICC Codes referenced in the contract documents, the provisions of Chapter 1, "Administrator," do not apply. These administrative requirements are covered by the applicable Federal Acquisition Regulations (FAR) included in this contract and by the authority granted to the Officer in Charge of Construction to administer the construction of this project. References in the ICC Codes to sections of Chapter 1, shall be applied appropriately by the Contracting Officer as authorized by his administrative cognizance and the FAR.

1.4 DELIVERY, STORAGE, AND HANDLING

Handle, store, and protect equipment and materials to prevent damage before and during installation in accordance with the manufacturer's recommendations, and as approved by the Contracting Officer. Replace damaged or defective items.

1.5 PERFORMANCE REQUIREMENTS

1.5.1 Welding

Piping shall be welded in accordance with qualified procedures using performance-qualified welders and welding operators. Procedures and welders shall be qualified in accordance with ASME BPVC SEC IX. Welding procedures qualified by others, and welders and welding operators qualified by another employer, may be accepted as permitted by ASME B31.1. The Contracting Officer shall be notified 24 hours in advance of tests, and the tests shall be performed at the work site if practicable. Welders or welding operators shall apply their assigned symbols near each weld they make as a permanent record.

1.6 REGULATORY REQUIREMENTS

Unless otherwise required herein, plumbing work shall be in accordance with ICC IPC.

1.7 PROJECT/SITE CONDITIONS

The Contractor shall become familiar with details of the work, verify dimensions in the field, and advise the Contracting Officer of any discrepancy before performing any work.

1.8 INSTRUCTION TO GOVERNMENT PERSONNEL

When specified in other sections, furnish the services of competent instructors to give full instruction to the designated Government personnel in the adjustment, operation, and maintenance, including pertinent safety requirements, of the specified equipment or system. Instructors shall be thoroughly familiar with all parts of the installation and shall be trained in operating theory as well as practical operation and maintenance work.

Instruction shall be given during the first regular work week after the equipment or system has been accepted and turned over to the Government for regular operation. The number of man-days (8 hours per day) of instruction furnished shall be as specified in the individual section.

When more than 4 man-days of instruction are specified, use approximately half of the time for classroom instruction. Use other time for instruction with the equipment or system.

When significant changes or modifications in the equipment or system are made under the terms of the contract, provide additional instruction to acquaint the operating personnel with the changes or modifications.

1.9 ACCESSIBILITY OF EQUIPMENT

Install all work so that parts requiring periodic inspection, operation, maintenance, and repair are readily accessible. Install concealed valves, expansion joints, controls, dampers, and equipment requiring access, in locations freely accessible through access doors.

PART 2 PRODUCTS

2.1 MATERIALS

Materials for various services shall be in accordance with TABLES I and II. Pipe schedules shall be selected based on service requirements. Pipe fittings shall be compatible with the applicable pipe materials. Plastic pipe, fittings, and solvent cement shall meet NSF/ANSI 14 and shall be NSF listed for the service intended. Plastic pipe, fittings, and solvent cement used for potable hot and cold water service shall bear the NSF seal "NSF-PW." Polypropylene pipe and fittings shall conform to dimensional requirements of Schedule 40, Iron Pipe size and shall comply with NSF/ANSI 14, NSF/ANSI 61 and ASTM F2389. Polypropylene piping that will be exposed to UV light shall be provided with a Factory applied UV resistant coating. Pipe threads (except dry seal) shall conform to ASME B1.20.1. Grooved pipe couplings and fittings shall be from the same manufacturer. Material or equipment containing a weighted average of greater than 0.25 percent lead shall not be used in any potable water system intended for human consumption, and shall be certified in accordance with NSF/ANSI 61, Annex G or NSF 372. In line devices such as water meters, building valves, check valves, meter stops, valves, fittings and back flow preventers shall comply with PL 93-523 and NSF/ANSI 61, Section 8. End point devices such as drinking water fountains, lavatory faucets, kitchen and bar faucets, residential ice makers, supply stops and end point control valves used to dispense water for drinking must meet the requirements of NSF/ANSI 61, Section 9. Hubless cast-iron soil pipe shall not be installed underground, under concrete floor slabs, or in crawl spaces below kitchen floors. Plastic pipe shall not be installed in air plenums. Plastic pipe shall not be installed in a pressure piping system in buildings greater than three stories including any basement levels.

2.1.1 Pipe Joint Materials

Grooved pipe and hubless cast-iron soil pipe shall not be used underground. Solder containing lead shall not be used with copper pipe. Cast iron soil pipe and fittings shall be marked with the collective trademark of the Cast Iron Soil Institute. Joints and gasket materials shall conform to the following:

a. Coupling for Cast-Iron Pipe: for hub and spigot type ASTM A74, AWWA C606. For hubless type: CISPI 310

b. Coupling for Steel Pipe: AWWA C606.

c. Couplings for Grooved Pipe: Ductile Iron ASTM A536 (Grade 65-45-12) ..

d. Flange Gaskets: Gaskets shall be made of non-asbestos material in accordance with ASME B16.21. Gaskets shall be flat, 1/16 inch thick, and contain Aramid fibers bonded with Styrene Butadiene Rubber (SBR) or Nitro Butadiene Rubber (NBR). Gaskets shall be the full face or self centering flat ring type. Gaskets used for hydrocarbon service shall be bonded with NBR.

e. Brazing Material: Brazing material shall conform to AWS A5.8/A5.8M, BCuP-5.

f. Brazing Flux: Flux shall be in paste or liquid form appropriate for use with brazing material. Flux shall be as follows: lead-free; have a 100 percent flushable residue; contain slightly acidic reagents; contain potassium borides; and contain fluorides.

g. Solder Material: Solder metal shall conform to ASTM B32.

h. Solder Flux: Flux shall be liquid form, non-corrosive, and conform to ASTM B813, Standard Test 1.

i. PTFE Tape: PTFE Tape, for use with Threaded Metal or Plastic Pipe.

j. Rubber Gaskets for Cast-Iron Soil-Pipe and Fittings (hub and spigot type and hubless type): ASTM C564.

k. Rubber Gaskets for Grooved Pipe: ASTM D2000, maximum temperature 230 degrees F.

l. Flexible Elastomeric Seals: ASTM D3139, ASTM D3212 or ASTM F477.

m. Bolts and Nuts for Grooved Pipe Couplings: Heat-treated carbon steel, ASTM A183.

n. Solvent Cement for Transition Joints between ABS and PVC Nonpressure Piping Components: ASTM D3138.

o. Plastic Solvent Cement for CPVC Plastic Pipe: ASTM F493.

p. Flanged fittings including, but not limited to, flanges, bolts, nuts and bolt patterns shall be in accordance with ASME B16.5 class 150 and shall have the manufacturer's trademark affixed in accordance with MSS SP-25. Flange material shall conform to ASTM A105/A105M. Blind flange material shall conform to ASTM A516/A516M cold service and ASTM A515/A515M for hot service. Bolts shall be high strength or intermediate strength with material conforming to ASTM A193/A193M.

q. Press fittings for Copper Pipe and Tube: Copper press fittings shall conform to the material and sizing requirements of ASME B16.51 and performance criteria of IAPMO PS 117. Sealing elements for copper press fittings shall be EPDM, FKM or HNBR. Sealing elements shall be factory installed or an alternative supplied fitting manufacturer. Sealing element shall be selected based on manufacturer's approved application guidelines.

r. Copper tubing shall conform to ASTM B88, Type K, L or M.

2.1.2 Miscellaneous Materials

Miscellaneous materials shall conform to the following:

a. Water Hammer Arrester: PDI WH 201. Water hammer arrester shall be bellows type.

b. Copper, Sheet and Strip for Building Construction: ASTM B370.

c. Asphalt Roof Cement: ASTM D2822/D2822M.

d. Hose Clamps: SAE J1508.

e. Supports for Off-The-Floor Plumbing Fixtures: ASME A112.6.1M.

f. Metallic Cleanouts: ASME A112.36.2M.

g. Plumbing Fixture Setting Compound: A preformed flexible ring seal molded from hydrocarbon wax material. The seal material shall be nonvolatile nonasphaltic and contain germicide and provide watertight, gastight, odorproof and verminproof properties.

h. Coal-Tar Protective Coatings and Linings for Steel Water Pipelines: AWWA C203.

i. Hypochlorites: AWWA B300.

j. Liquid Chlorine: AWWA B301.

k. Gauges - Pressure and Vacuum Indicating Dial Type - Elastic Element: ASME B40.100.

l. Thermometers: ASTM E1. Mercury shall not be used in thermometers.

2.1.3 Pipe Insulation Material

Insulation shall be as specified in Section 23 07 00 THERMAL INSULATION FOR MECHANICAL SYSTEMS.

2.2 PIPE HANGERS, INSERTS, AND SUPPORTS

Pipe hangers, inserts, and supports shall conform to MSS SP-58.

2.3 VALVES

Valves shall be provided on supplies to equipment and fixtures. Valves 2-1/2 inches and smaller shall be bronze with threaded bodies for pipe and solder-type connections for tubing. Valves 3 inches and larger shall have flanged iron bodies and bronze trim. Pressure ratings shall be based upon the application. Grooved end valves may be provided if the manufacturer certifies that the valves meet the performance requirements of applicable MSS standard. Valves shall conform to the following standards:

Description	Standard
Butterfly Valves	MSS SP-67

Cast-Iron Gate Valves, Flanged and Threaded Ends	MSS SP-70
Cast-Iron Swing Check Valves, Flanged and Threaded Ends	MSS SP-71
Ball Valves with Flanged Butt-Welding Ends for General Service	MSS SP-72
Ball Valves Threaded, Socket-Welding, Solder Joint, Grooved and Flared Ends	MSS SP-110
Cast-Iron Plug Valves, Flanged and Threaded Ends	MSS SP-78
Bronze Gate, Globe, Angle, and Check Valves	MSS SP-80
Steel Valves, Socket Welding and Threaded Ends	ASME B16.34
Cast-Iron Globe and Angle Valves, Flanged and Threaded Ends	MSS SP-85
Backwater Valves	ASME A112.14.1
Vacuum Relief Valves	ANSI Z21.22/CSA 4.4
Water Pressure Reducing Valves	ASSE 1003
Water Heater Drain Valves	ASME BPVC SEC IV, Part HLW-810: Requirements for Potable-Water Heaters Bottom Drain Valve
Trap Seal Primer Valves	ASSE 1018
Temperature and Pressure Relief Valves for Hot Water Supply Systems	ANSI Z21.22/CSA 4.4
Temperature and Pressure Relief Valves for Automatically Fired Hot Water Boilers	ASME CSD-1 Safety Code No., Part CW, Article 5

2.3.1 Backwater Valves

Backwater valves shall be either separate from the floor drain or a combination floor drain, P-trap, and backwater valve, as shown. Valves shall have cast-iron bodies with cleanouts large enough to permit removal

of interior parts. Valves shall be of the flap type, hinged or pivoted, with revolving disks. Hinge pivots, disks, and seats shall be nonferrous metal. Disks shall be slightly open in a no-flow no-backwater condition. Cleanouts shall extend to finished floor and be fitted with threaded countersunk plugs.

2.3.2 Wall Faucets

Wall faucets with vacuum-breaker backflow preventer shall be brass with 3/4 inch male inlet threads, hexagon shoulder, and 3/4 inch hose connection. Faucet handle shall be securely attached to stem.

2.3.3 Wall Hydrants (Frostproof)

ASSE 1019 with vacuum-breaker backflow preventer shall have a nickel-brass or nickel-bronze wall plate or flange with nozzle and detachable key handle. A brass or bronze operating rod shall be provided within a galvanized iron casing of sufficient length to extend through the wall so that the valve is inside the building, and the portion of the hydrant between the outlet and valve is self-draining. A brass or bronze valve with coupling and union elbow having metal-to-metal seat shall be provided. Valve rod and seat washer shall be removable through the face of the hydrant. The hydrant shall have 3/4 inch exposed hose thread on spout and 3/4 inch male pipe thread on inlet.

2.3.4 Relief Valves

Water heaters and hot water storage tanks shall have a combination pressure and temperature (P&T) relief valve. The pressure relief element of a P&T relief valve shall have adequate capacity to prevent excessive pressure buildup in the system when the system is operating at the maximum rate of heat input. The temperature element of a P&T relief valve shall have a relieving capacity which is at least equal to the total input of the heaters when operating at their maximum capacity. Relief valves shall be rated according to ANSI Z21.22/CSA 4.4. Relief valves for systems where the maximum rate of heat input is less than 200,000 Btuh shall have 3/4 inch minimum inlets, and 3/4 inch outlets. Relief valves for systems where the maximum rate of heat input is greater than 200,000 Btuh shall have 1 inch minimum inlets, and 1 inch outlets. The discharge pipe from the relief valve shall be the size of the valve outlet.

2.3.5 Thermostatic Mixing Valves

Provide thermostatic mixing valve for lavatory faucets. Mixing valves, thermostatic type, pressure-balanced or combination thermostatic and pressure-balanced shall be line size and shall be constructed with rough or finish bodies either with or without plating. Each valve shall be constructed to control the mixing of hot and cold water and to deliver water at a desired temperature regardless of pressure or input temperature changes. The control element shall be of an approved type. The body shall be of heavy cast bronze, and interior parts shall be brass, bronze, corrosion-resisting steel or copper. The valve shall be equipped with necessary stops, check valves, unions, and sediment strainers on the inlets. Mixing valves shall maintain water temperature within 5 degrees F of any setting.

2.4 FIXTURES

Refer to Drawings for Plumbing Fixture Schedule.

2.5 BACKFLOW PREVENTERS

Backflow prevention devices must be approved by the State or local regulatory agencies. If there is no State or local regulatory agency requirements, the backflow prevention devices must be listed by the Foundation for Cross-Connection Control & Hydraulic Research, or any other approved testing laboratory having equivalent capabilities for both laboratory and field evaluation of backflow prevention devices and assemblies.

Reduced pressure principle assemblies, double check valve assemblies, atmospheric (nonpressure) type vacuum breakers, and pressure type vacuum breakers shall be meet the above requirements.

Backflow preventers with intermediate atmospheric vent shall conform to ASSE 1012. Reduced pressure principle backflow preventers shall conform to ASSE 1013. Hose connection vacuum breakers shall conform to ASSE 1011. Pipe applied atmospheric type vacuum breakers shall conform to ASSE 1001. Pressure vacuum breaker assembly shall conform to ASSE 1020. Air gaps in plumbing systems shall conform to ASME A112.1.2.

2.6 DRAINS

2.6.1 Floor and Shower Drains

Floor and shower drains shall consist of a galvanized body, integral seepage pan, and adjustable perforated or slotted chromium-plated bronze, nickel-bronze, or nickel-brass strainer, consisting of grate and threaded collar. Floor drains shall be cast iron except where metallic waterproofing membrane is installed. Drains shall be of double drainage pattern for embedding in the floor construction. The seepage pan shall have weep holes or channels for drainage to the drainpipe. The strainer shall be adjustable to floor thickness. A clamping device for attaching flashing or waterproofing membrane to the seepage pan without damaging the flashing or waterproofing membrane shall be provided when required. Drains shall be provided with threaded connection. Between the drain outlet and waste pipe, a neoprene rubber gasket conforming to ASTM C564 may be installed, provided that the drain is specifically designed for the rubber gasket compression type joint. Floor and shower drains shall conform to ASME A112.6.3. Provide drain with trap primer connection, trap primer, and connection piping. Primer shall meet ASSE 1018.

2.6.1.1 Metallic Shower Pan Drains

Where metallic shower pan membrane is installed, polyethylene drain with corrosion-resistant screws securing the clamping device shall be provided. Polyethylene drains shall have fittings to adapt drain to waste piping. Polyethylene for floor drains shall conform to ASTM D1248. Drains shall have separate cast-iron "P" trap, circular body, seepage pan, and strainer, unless otherwise indicated.

2.6.1.2 Drains and Backwater Valves

Drains and backwater valves installed in connection with waterproofed floors or shower pans shall be equipped with bolted-type device to securely clamp flashing.

2.6.2 Floor Sinks

Floor sinks shall be square, with 12 inch nominal overall width or diameter and 10 inch nominal overall depth. Floor sink shall have an acid-resistant enamel interior finish with cast-iron body, aluminum sediment bucket, and perforated grate of cast iron in industrial areas and stainless steel in finished areas. The outlet pipe size shall be as indicated or of the same size as the connecting pipe.

2.6.3 Roof Drains and Expansion Joints

Roof drains shall conform to ASME A112.6.4, with dome and integral flange, and shall have a device for making a watertight connection between roofing and flashing. The whole assembly shall be galvanized heavy pattern cast iron. For aggregate surface roofing, the drain shall be provided with a gravel stop. On roofs other than concrete construction, roof drains shall be complete with underdeck clamp, sump receiver, and an extension for the insulation thickness where applicable. A clamping device for attaching flashing or waterproofing membrane to the seepage pan without damaging the flashing or membrane shall be provided when required to suit the building construction. Strainer openings shall have a combined area equal to twice that of the drain outlet. The outlet shall be equipped to make a proper connection to threaded pipe of the same size as the downspout. An expansion joint of proper size to receive the conductor pipe shall be provided. The expansion joint shall consist of a heavy cast-iron housing, brass or bronze sleeve, brass or bronze fastening bolts and nuts, and gaskets or packing. The sleeve shall have a nominal thickness of not less than 0.134 inch. Gaskets and packing shall be close-cell neoprene, O-ring packing shall be close-cell neoprene of 70 durometer. Packing shall be held in place by a packing gland secured with bolts.

2.7 TRAPS

Unless otherwise specified, traps shall be copper-alloy adjustable tube type with slip joint inlet and swivel. Traps shall be without a cleanout. Provide traps with removable access panels for easy clean-out at sinks and lavatories. Tubes shall be copper alloy with walls not less than 0.032 inch thick within commercial tolerances, except on the outside of bends where the thickness may be reduced slightly in manufacture by usual commercial methods. Inlets shall have rubber washer and copper alloy nuts for slip joints above the discharge level. Swivel joints shall be below the discharge level and shall be of metal-to-metal or metal-to-plastic type as required for the application. Nuts shall have flats for wrench grip. Outlets shall have internal pipe thread, except that when required for the application, the outlets shall have sockets for solder-joint connections. The depth of the water seal shall be not less than 2 inches. The interior diameter shall be not more than 1/8 inch over or under the nominal size, and interior surfaces shall be reasonably smooth throughout. A copper alloy "P" trap assembly consisting of an adjustable "P" trap and threaded trap wall nipple with cast brass wall flange shall be provided for lavatories. The assembly shall be a standard manufactured unit and may have a rubber-gasketed swivel joint.

2.8 WATER HEATERS

Electric type water heaters shall conform to UL 174 with dual heating elements. Each element shall be 12 KW. The elements shall be wired so that only one element can operate at a time. The Operating Set Point shall be adjustable from 90°F/42°C to 190°F/88°C. Each element shall be

constantly monitored and current on/off state is displayed, any element failure shall be reported and exact location shall be shown, eliminates needs for field testing of elements. Heater shall be listed with Underwriters' Laboratories and classified to The National Sanitation Foundation Standard No. 5. All internal surfaces of the tank shall be glass-lined with an alkaline borosilicate composition that has been fused-to-steel by firing at a temperature of 1600°F. Tank shall be cathodically protected with a combination of sacrificial and powered anodes. The entire vessel is to be enclosed in a round steel enclosure with baked enamel finish. Water heater shall have an electronic control with large LCD displaying current water heater status; provide real time element status and sensing, low water cutoff and economy mode operation. Heater shall have 120 volt control circuit transformer, transformer fusing, magnetic contactor(s), element fusing per N.E.C., and commercial grade Incoloy elements. Temperature controls shall include limiting switch which will require resetting manually in the event the temperature reaches 202°F. Foam insulation shall meet the thermal efficiency and/or standby loss requirements of the U. S. Department of Energy and current edition of ASHRAE/IES 90.1. Heater shall include a CSA Certified and ASME Rated T&P relief valve and a drain valve. Water heater units(s) shall be compatible with building management systems using Modbus or BACnet with optional ICC interface.

2.9 PUMPS

2.9.1 Sump Pumps

Sump pumps shall be of capacities indicated. The pumps shall be of the automatic, electric motor-driven, submerged type, complete with necessary control equipment and with a split or solid cast-iron or steel cover plate. The pumps shall be direct-connected by an approved flexible coupling to a vertical electric motor having a continuous oiling device or packed bearings sealed against dirt and moisture. Motors shall be totally enclosed, fan-cooled of sizes as indicated and shall be equipped with an across-the-line magnetic controller in a NEMA 250, Type 4 enclosure. Integral size motors shall be the premium efficiency type in accordance with NEMA MG 1. Each pump shall be fitted with a high-grade thrust bearing mounted above the floor. Each shaft shall have an alignment bearing at each end, and the suction inlet shall be between 3 and 6 inches above the sump bottom. The suction side of each pump shall have a strainer of ample capacity. A float switch assembly, with the switch completely enclosed in a NEMA 250, Type 4 enclosure, shall start and stop each motor at predetermined water levels. Duplex pumps shall be equipped with an automatic alternator to change the lead operation from one pump to the other, and for starting the second pump if the flow exceeds the capacity of the first pump. The discharge line from each pump shall be provided with a union or flange, a nonclog swing check valve, and a stop valve in an accessible location near the pump.

2.9.2 Circulating Pumps

Domestic hot water circulating pumps shall be electrically driven, single-stage, centrifugal, with mechanical seals, suitable for the intended service. Pump and motor shall be supported by the piping on which it is installed. The shaft shall be one-piece, heat-treated, corrosion-resisting steel with impeller and smooth-surfaced housing of bronze.

Motor shall be totally enclosed, fan-cooled and shall have sufficient

horsepower for the service required. Each pump motor shall be equipped with an across-the-line magnetic controller in a NEMA 250, Type 1 enclosure with "START-STOP" switch in cover.

2.9.3 Flexible Connectors

Flexible connectors shall be provided at the suction and discharge of each pump that is 1 hp or larger. Connectors shall be constructed of neoprene, rubber, or braided bronze, with Class 150 standard flanges. Flexible connectors shall be line size and suitable for the pressure and temperature of the intended service.

2.10 DOMESTIC WATER SERVICE METER

Cold water meters 2 inches and smaller shall be positive displacement type conforming to AWWA C700. Cold water meters 2-1/2 inches and larger shall be turbine type conforming to AWWA C701. Meter register may be round or straight reading type, as provided by the local utility. Meter shall be provided with a pulse generator, remote readout register and all necessary wiring and accessories.

Meters must be connected to the base wide energy and utility monitoring and control system (if this system exists) using the installation's advanced metering protocols.

2.11 ELECTRICAL WORK

Provide electrical motor driven equipment specified complete with motors, motor starters, and controls as specified herein and in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Provide internal wiring for components of packaged equipment as an integral part of the equipment. Provide high efficiency type, single-phase, fractional-horsepower alternating-current motors, including motors that are part of a system, corresponding to the applications in accordance with NEMA MG 11. In addition to the requirements of Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM, provide polyphase, squirrel-cage medium induction motors with continuous ratings, including motors that are part of a system, that meet the efficiency ratings for premium efficiency motors in accordance with NEMA MG 1. Provide motors in accordance with NEMA MG 1 and of sufficient size to drive the load at the specified capacity without exceeding the nameplate rating of the motor.

Motors shall be rated for continuous duty with the enclosure specified. Motor duty requirements shall allow for maximum frequency start-stop operation and minimum encountered interval between start and stop. Motor torque shall be capable of accelerating the connected load within 20 seconds with 80 percent of the rated voltage maintained at motor terminals during one starting period. Motor bearings shall be fitted with grease supply fittings and grease relief to outside of the enclosure.

Controllers and contactors shall have auxiliary contacts for use with the controls provided. Manual or automatic control and protective or signal devices required for the operation specified and any control wiring required for controls and devices specified, but not shown, shall be provided. For packaged equipment, the manufacturer shall provide controllers, including the required monitors and timed restart.

Power wiring and conduit for field installed equipment shall be provided under and conform to the requirements of Section 26 20 00 INTERIOR

DISTRIBUTION SYSTEM.

2.12 Clean-outs

Finished Floor Clean-outs: Cast iron body and frame with round adjustable scoriated nickel bronze top. Provide nickle bronze carpet clamping frame with vandal proof screw in carpeted areas.

Unfinished Floor and Equipment Area Floor: DCast iron body and frame with round adjustable scoriated cast iron top.

Corrosion Resistant: ABS body with round coated cast iron top.

Wall cleanouts: Cast iron caulk ferrule with vast bronze taper thread plug and prime-coated steel shallow cover. Vandalproof screws.

2.13 MISCELLANEOUS PIPING ITEMS

2.13.1 Escutcheon Plates

Provide one piece or split hinge metal plates for piping entering floors, walls, and ceilings in exposed spaces. Provide chromium-plated on copper alloy plates or polished stainless steel finish in finished spaces. Provide paint finish on plates in unfinished spaces.

2.13.2 Pipe Sleeves

Provide where piping passes entirely through walls, ceilings, roofs, and floors. Sleeves are not required where drain, waste, and vent (DWV) piping passes through concrete floor slabs located on grade, except where penetrating a membrane waterproof floor.

2.13.2.1 Sleeves in Masonry and Concrete

Provide steel pipe sleeves or schedule 40 PVC plastic pipe sleeves. Sleeves are not required where drain, waste, and vent (DWV) piping passes through concrete floor slabs located on grade. Core drilling of masonry and concrete may be provided in lieu of pipe sleeves when cavities in the core-drilled hole are completely grouted smooth.

2.13.2.2 Sleeves Not in Masonry and Concrete

Provide 26 gage galvanized steel sheet or PVC plastic pipe sleeves.

2.13.3 Pipe Hangers (Supports)

Provide MSS SP-58 Type 1 with adjustable type steel support rods, except as specified or indicated otherwise. Attach to steel joists with Type 19 or 23 clamps and retaining straps. Attach to Steel W or S beams with Type 21, 28, 29, or 30 clamps. Attach to steel angles and vertical web steel channels with Type 20 clamp with beam clamp channel adapter. Attach to horizontal web steel channel and wood with drilled hole on centerline and double nut and washer. Attach to concrete with Type 18 insert or drilled expansion anchor. Provide Type 40 insulation protection shield for insulated piping.

2.13.4 Nameplates

Provide 0.125 inch thick melamine laminated plastic nameplates, black

matte finish with white center core, for equipment, gages, thermometers, and valves; valves in supplies to faucets will not require nameplates. Accurately align lettering and engrave minimum of 0.25 inch high normal block lettering into the white core. Minimum size of nameplates shall be 1.0 by 2.5 inches. Key nameplates to a chart and schedule for each system. Frame charts and schedules under glass and place where directed near each system. Furnish two copies of each chart and schedule.

PART 3 EXECUTION

3.1 GENERAL INSTALLATION REQUIREMENTS

Piping located in air plenums shall conform to NFPA 90A requirements. Piping located in shafts that constitute air ducts or that enclose air ducts shall be noncombustible in accordance with NFPA 90A. Installation of plastic pipe where in compliance with NFPA may be installed in accordance with PPFA Fire Man. The plumbing system shall be installed complete with necessary fixtures, fittings, traps, valves, and accessories. Water and drainage piping shall be extended 5 feet outside the building, unless otherwise indicated. A full port ball valve and drain shall be installed on the water service line inside the building approximately 6 inches above the floor from point of entry. Piping shall be connected to the exterior service lines or capped or plugged if the exterior service is not in place. Sewer and water pipes shall be laid in separate trenches, except when otherwise shown. Exterior underground utilities shall be at least 12 inches below the average local frost depth or as indicated on the drawings. If trenches are closed or the pipes are otherwise covered before being connected to the service lines, the location of the end of each plumbing utility shall be marked with a stake or other acceptable means. Valves shall be installed with control no lower than the valve body.

3.1.1 Water Pipe, Fittings, and Connections

3.1.1.1 Utilities

The piping shall be extended to fixtures, outlets, and equipment. The hot-water and cold-water piping system shall be arranged and installed to permit draining. The supply line to each item of equipment or fixture, except faucets, flush valves, or other control valves which are supplied with integral stops, shall be equipped with a shutoff valve to enable isolation of the item for repair and maintenance without interfering with operation of other equipment or fixtures. Supply piping to fixtures, faucets, hydrants, shower heads, and flushing devices shall be anchored to prevent movement.

3.1.1.2 Cutting and Repairing

The work shall be carefully laid out in advance, and unnecessary cutting of construction shall be avoided. Damage to building, piping, wiring, or equipment as a result of cutting shall be repaired by mechanics skilled in the trade involved.

3.1.1.3 Protection of Fixtures, Materials, and Equipment

Pipe openings shall be closed with caps or plugs during installation. Fixtures and equipment shall be tightly covered and protected against dirt, water, chemicals, and mechanical injury. Upon completion of the work, the fixtures, materials, and equipment shall be thoroughly cleaned,

adjusted, and operated. Safety guards shall be provided for exposed rotating equipment.

3.1.1.4 Mains, Branches, and Runouts

Piping shall be installed as indicated. Pipe shall be accurately cut and worked into place without springing or forcing. Structural portions of the building shall not be weakened. Aboveground piping shall run parallel with the lines of the building, unless otherwise indicated. Branch pipes from service lines may be taken from top, bottom, or side of main, using crossover fittings required by structural or installation conditions. Supply pipes, valves, and fittings shall be kept a sufficient distance from other work and other services to permit not less than 1/2 inch between finished covering on the different services. Bare and insulated water lines shall not bear directly against building structural elements so as to transmit sound to the structure or to prevent flexible movement of the lines. Water pipe shall not be buried in or under floors unless specifically indicated or approved. Changes in pipe sizes shall be made with reducing fittings. Use of bushings will not be permitted except for use in situations in which standard factory fabricated components are furnished to accommodate specific accepted installation practice. Change in direction shall be made with fittings, except that bending of pipe 4 inches and smaller will be permitted, provided a pipe bender is used and wide sweep bends are formed. The center-line radius of bends shall be not less than six diameters of the pipe. Bent pipe showing kinks, wrinkles, flattening, or other malformations will not be acceptable.

3.1.1.5 Pipe Drains

Pipe drains indicated shall consist of 3/4 inch hose bibb with renewable seat and ball valve ahead of hose bibb. At other low points, 3/4 inch brass plugs or caps shall be provided. Disconnection of the supply piping at the fixture is an acceptable drain.

3.1.1.6 Expansion and Contraction of Piping

Allowance shall be made throughout for expansion and contraction of water pipe. Each hot-water and hot-water circulation riser shall have expansion loops or other provisions such as offsets and changes in direction where indicated and required. Risers shall be securely anchored as required or where indicated to force expansion to loops. Branch connections from risers shall be made with ample swing or offset to avoid undue strain on fittings or short pipe lengths. Horizontal runs of pipe over 50 feet in length shall be anchored to the wall or the supporting construction about midway on the run to force expansion, evenly divided, toward the ends. Sufficient flexibility shall be provided on branch runouts from mains and risers to provide for expansion and contraction of piping. Flexibility shall be provided by installing one or more turns in the line so that piping will spring enough to allow for expansion without straining. If mechanical grooved pipe coupling systems are provided, the deviation from design requirements for expansion and contraction may be allowed pending approval of Contracting Officer.

3.1.1.7 Thrust Restraint

Plugs, caps, tees, valves and bends deflecting 11.25 degrees or more, either vertically or horizontally, in waterlines 4 inches in diameter or larger shall be provided with thrust blocks, where indicated, to prevent movement. Thrust blocking shall be concrete of a mix not leaner than: 1

cement, 2-1/2 sand, 5 gravel; and having a compressive strength of not less than 2000 psi after 28 days. Blocking shall be placed between solid ground and the fitting to be anchored. Unless otherwise indicated or directed, the base and thrust bearing sides of the thrust block shall be poured against undisturbed earth. The side of the thrust block not subject to thrust shall be poured against forms. The area of bearing will be as shown. Blocking shall be placed so that the joints of the fitting are accessible for repair. Steel rods and clamps, protected by galvanizing or by coating with bituminous paint, shall be used to anchor vertical down bends into gravity thrust blocks.

3.1.1.8 Commercial-Type Water Hammer Arresters

Commercial-type water hammer arresters shall be provided on hot- and cold-water supplies and shall be located as generally indicated, with precise location and sizing to be in accordance with PDI WH 201. Water hammer arresters, where concealed, shall be accessible by means of access doors or removable panels. Commercial-type water hammer arresters shall conform to ASSE 1010. Vertical capped pipe columns will not be permitted.

3.1.2 Joints

Installation of pipe and fittings shall be made in accordance with the manufacturer's recommendations. Mitering of joints for elbows and notching of straight runs of pipe for tees will not be permitted. Joints shall be made up with fittings of compatible material and made for the specific purpose intended.

3.1.2.1 Threaded

Threaded joints shall have American Standard taper pipe threads conforming to ASME B1.20.1. Only male pipe threads shall be coated with graphite or with an approved graphite compound, or with an inert filler and oil, or shall have a polytetrafluoroethylene tape applied.

3.1.2.2 Mechanical Couplings

Mechanical couplings may be used in conjunction with grooved pipe for aboveground, ferrous or non-ferrous, domestic hot and cold water systems, in lieu of unions, brazed, soldered, welded, flanged, or threaded joints.

Mechanical couplings are permitted in accessible locations including behind access plates. Flexible grooved joints will not be permitted, except as vibration isolators adjacent to mechanical equipment. Rigid grooved joints shall incorporate an angle bolt pad design which maintains metal-to-metal contact with equal amount of pad offset of housings upon installation to ensure positive rigid clamping of the pipe.

Designs which can only clamp on the bottom of the groove or which utilize gripping teeth or jaws, or which use misaligned housing bolt holes, or which require a torque wrench or torque specifications will not be permitted.

Grooved fittings and couplings, and grooving tools shall be provided from the same manufacturer. Segmentally welded elbows shall not be used. Grooves shall be prepared in accordance with the coupling manufacturer's latest published standards. Grooving shall be performed by qualified grooving operators having demonstrated proper grooving procedures in accordance with the tool manufacturer's recommendations.

The Contracting Officer shall be notified 24 hours in advance of test to demonstrate operator's capability, and the test shall be performed at the work site, if practical, or at a site agreed upon. The operator shall demonstrate the ability to properly adjust the grooving tool, groove the pipe, and to verify the groove dimensions in accordance with the coupling manufacturer's specifications.

3.1.2.3 Unions and Flanges

Unions, flanges and mechanical couplings shall not be concealed in walls, ceilings, or partitions. Unions shall be used on pipe sizes 2-1/2 inches and smaller; flanges shall be used on pipe sizes 3 inches and larger.

3.1.2.4 Grooved Mechanical Joints

Grooves shall be prepared according to the coupling manufacturer's instructions. Grooved fittings, couplings, and grooving tools shall be products of the same manufacturer. Pipe and groove dimensions shall comply with the tolerances specified by the coupling manufacturer. The diameter of grooves made in the field shall be measured using a "go/no-go" gauge, vernier or dial caliper, narrow-land micrometer, or other method specifically approved by the coupling manufacturer for the intended application. Groove width and dimension of groove from end of pipe shall be measured and recorded for each change in grooving tool setup to verify compliance with coupling manufacturer's tolerances. Grooved joints shall not be used in concealed locations.

3.1.2.5 Cast Iron Soil, Waste and Vent Pipe

Bell and spigot compression and hubless gasketed clamp joints for soil, waste and vent piping shall be installed per the manufacturer's recommendations.

3.1.2.6 Copper Tube and Pipe

a. Brazed. Brazed joints shall be made in conformance with AWS B2.2/B2.2M, ASME B16.50, and CDA A4015 with flux and are acceptable for all pipe sizes. Copper to copper joints shall include the use of copper-phosphorus or copper-phosphorus-silver brazing metal without flux. Brazing of dissimilar metals (copper to bronze or brass) shall include the use of flux with either a copper-phosphorus, copper-phosphorus-silver or a silver brazing filler metal.

b. Soldered. Soldered joints shall be made with flux and are only acceptable for piping 2 inches and smaller. Soldered joints shall conform to ASME B31.5 and CDA A4015. Soldered joints shall not be used in compressed air piping between the air compressor and the receiver.

c. Copper Tube Extracted Joint. Mechanically extracted joints shall be made in accordance with ICC IPC.

d. Press connection. Copper press connections shall be made in **strict** accordance with the manufacturer's installation instructions for manufactured rated size. The joints shall be pressed using the tool(s) approved by the manufacturer **of that joint**. Minimum distance between fittings shall be in accordance with the manufacturer's requirements.

3.1.2.7 Plastic Pipe

Acrylonitrile-Butadiene-Styrene (ABS) pipe shall have joints made with solvent cement. PVC and CPVC pipe shall have joints made with solvent cement elastomeric, threading, (threading of Schedule 80 Pipe is allowed only where required for disconnection and inspection; threading of Schedule 40 Pipe is not allowed), or mated flanged.

3.1.2.8 Glass Pipe

Joints for corrosive waste glass pipe and fittings shall be made with corrosion-resisting steel compression-type couplings with acrylonitrile rubber gaskets lined with polytetrafluoroethylene.

3.1.2.9 Corrosive Waste Plastic Pipe

Joints for polyolefin pipe and fittings shall be made by mechanical joint or electrical fusion coil method in accordance with ASTM D2657 and ASTM F1290. Joints for filament-wound reinforced thermosetting resin pipe shall be made in accordance with manufacturer's instructions. Unions or flanges shall be used where required for disconnection and inspection.

3.1.2.10 Polypropylene Pipe

Joints for polypropylene pipe and fittings shall be made by heat fusion welding socket-type or butt-fusion type fittings and shall comply with ASTM F2389.

3.1.2.11 Other Joint Methods

3.1.3 Dissimilar Pipe Materials

Connections between ferrous and non-ferrous copper water pipe shall be made with dielectric unions or flange waterways. Dielectric waterways shall have temperature and pressure rating equal to or greater than that specified for the connecting piping. Waterways shall have metal connections on both ends suited to match connecting piping. Dielectric waterways shall be internally lined with an insulator specifically designed to prevent current flow between dissimilar metals. Dielectric flanges shall meet the performance requirements described herein for dielectric waterways. Connecting joints between plastic and metallic pipe shall be made with transition fitting for the specific purpose.

3.1.4 Corrosion Protection for Buried Pipe and Fittings

Ductile iron, cast iron, and steel pipe, fittings, and joints shall have a protective coating. Additionally, ductile iron, cast iron, and steel pressure pipe shall have a cathodic protection system and joint bonding. The cathodic protection system, protective coating system, and joint bonding for cathodically protected pipe shall be in accordance with . Coatings shall be selected, applied, and inspected in accordance with NACE SP0169 and as otherwise specified. The pipe shall be cleaned and the coating system applied prior to pipe tightness testing. Joints and fittings shall be cleaned and the coating system applied after pipe tightness testing. For tape coating systems, the tape shall conform to AWWA C203 and shall be applied with a 50 percent overlap. Primer utilized with tape type coating systems shall be as recommended by the tape manufacturer.

3.1.5 Pipe Sleeves and Flashing

Pipe sleeves shall be furnished and set in their proper and permanent location.

3.1.5.1 Sleeve Requirements

Unless indicated otherwise, provide pipe sleeves meeting the following requirements:

a. Secure sleeves in position and location during construction. Provide sleeves of sufficient length to pass through entire thickness of walls, ceilings, roofs, and floors.

b. A modular mechanical type sealing assembly may be installed in lieu of a waterproofing clamping flange and caulking and sealing of annular space between pipe and sleeve. The seals shall consist of interlocking synthetic rubber links shaped to continuously fill the annular space between the pipe and sleeve using galvanized steel bolts, nuts, and pressure plates. The links shall be loosely assembled with bolts to form a continuous rubber belt around the pipe with a pressure plate under each bolt head and each nut. After the seal assembly is properly positioned in the sleeve, tightening of the bolt shall cause the rubber sealing elements to expand and provide a watertight seal between the pipe and the sleeve. Each seal assembly shall be sized as recommended by the manufacturer to fit the pipe and sleeve involved.

c. Sleeves shall not be installed in structural members, except where indicated or approved. Rectangular and square openings shall be as detailed. Each sleeve shall extend through its respective floor, or roof, and shall be cut flush with each surface, except for special circumstances. Pipe sleeves passing through floors in wet areas such as mechanical equipment rooms, lavatories, kitchens, and other plumbing fixture areas shall extend a minimum of 4 inches above the finished floor.

d. Unless otherwise indicated, sleeves shall be of a size to provide a minimum of 1/4 inch clearance between bare pipe or insulation and inside of sleeve or between insulation and inside of sleeve. Sleeves in bearing walls and concrete slab on grade floors shall be steel pipe or cast-iron pipe. Sleeves in nonbearing walls or ceilings may be steel pipe, cast-iron pipe, galvanized sheet metal with lock-type longitudinal seam, or plastic.

e. Except as otherwise specified, the annular space between pipe and sleeve, or between jacket over insulation and sleeve, shall be sealed as indicated with sealants conforming to ASTM C920 and with a primer, backstop material and surface preparation as specified in Section 07 92 00 JOINT SEALANTS. The annular space between pipe and sleeve, between bare insulation and sleeve or between jacket over insulation and sleeve shall not be sealed for interior walls which are not designated as fire rated.

f. Sleeves through below-grade walls in contact with earth shall be recessed 1/2 inch from wall surfaces on both sides. Annular space between pipe and sleeve shall be filled with backing material and sealants in the joint between the pipe and concrete wall as specified

above. Sealant selected for the earth side of the wall shall be compatible with dampproofing/waterproofing materials that are to be applied over the joint sealant. Pipe sleeves in fire-rated walls shall conform to the requirements in Section 07 84 00 FIRESTOPPING.

3.1.5.2 Flashing Requirements

Pipes passing through roof shall be installed through a 16 ounce copper flashing, each within an integral skirt or flange. Flashing shall be suitably formed, and the skirt or flange shall extend not less than 8 inches from the pipe and shall be set over the roof or floor membrane in a solid coating of bituminous cement. The flashing shall extend up the pipe a minimum of 10 inches. For cleanouts, the flashing shall be turned down into the hub and caulked after placing the ferrule. Pipes passing through pitched roofs shall be flashed, using lead or copper flashing, with an adjustable integral flange of adequate size to extend not less than 8 inches from the pipe in all directions and lapped into the roofing to provide a watertight seal. The annular space between the flashing and the bare pipe or between the flashing and the metal-jacket-covered insulation shall be sealed as indicated. Flashing for dry vents shall be turned down into the pipe to form a waterproof joint. Pipes, up to and including 10 inches in diameter, passing through roof or floor waterproofing membrane may be installed through a cast-iron sleeve with caulking recess, anchor lugs, flashing-clamp device, and pressure ring with brass bolts. Flashing shield shall be fitted into the sleeve clamping device. Pipes passing through wall waterproofing membrane shall be sleeved as described above. A waterproofing clamping flange shall be installed.

3.1.5.3 Waterproofing

Waterproofing at floor-mounted water closets shall be accomplished by forming a flashing guard from soft-tempered sheet copper. The center of the sheet shall be perforated and turned down approximately 1-1/2 inches to fit between the outside diameter of the drainpipe and the inside diameter of the cast-iron or steel pipe sleeve. The turned-down portion of the flashing guard shall be embedded in sealant to a depth of approximately 1-1/2 inches; then the sealant shall be finished off flush to floor level between the flashing guard and drainpipe. The flashing guard of sheet copper shall extend not less than 8 inches from the drainpipe and shall be lapped between the floor membrane in a solid coating of bituminous cement. If cast-iron water closet floor flanges are used, the space between the pipe sleeve and drainpipe shall be sealed with sealant and the flashing guard shall be upturned approximately 1-1/2 inches to fit the outside diameter of the drainpipe and the inside diameter of the water closet floor flange. The upturned portion of the sheet fitted into the floor flange shall be sealed.

3.1.5.4 Optional Counterflashing

Instead of turning the flashing down into a dry vent pipe, or caulking and sealing the annular space between the pipe and flashing or metal-jacket-covered insulation and flashing, counterflashing may be accomplished by utilizing the following:

a. A standard roof coupling for threaded pipe up to 6 inches in diameter.

b. A tack-welded or banded-metal rain shield around the pipe.

3.1.5.5 Pipe Penetrations of Slab on Grade Floors

Where pipes, fixture drains, floor drains, cleanouts or similar items penetrate slab on grade floors, except at penetrations of floors with waterproofing membrane as specified in paragraphs FLASHING REQUIREMENTS and WATERPROOFING, a groove 1/4 to 1/2 inch wide by 1/4 to 3/8 inch deep shall be formed around the pipe, fitting or drain. The groove shall be filled with a sealant as specified in Section 07 92 00 JOINT SEALANTS.

3.1.5.6 Pipe Penetrations

Provide sealants for all pipe penetrations. All pipe penetrations shall be sealed to prevent infiltration of air, insects, and vermin.

3.1.6 Fire Seal

Where pipes pass through fire walls, fire-partitions, fire-rated pipe chase walls or floors above grade, a fire seal shall be provided as specified in Section 07 84 00 FIRESTOPPING.

3.1.7 Supports

3.1.7.1 General

Hangers used to support piping 2 inches and larger shall be fabricated to permit adequate adjustment after erection while still supporting the load. Pipe guides and anchors shall be installed to keep pipes in accurate alignment, to direct the expansion movement, and to prevent buckling, swaying, and undue strain. Piping subjected to vertical movement when operating temperatures exceed ambient temperatures shall be supported by variable spring hangers and supports or by constant support hangers. In the support of multiple pipe runs on a common base member, a clip or clamp shall be used where each pipe crosses the base support member. Spacing of the base support members shall not exceed the hanger and support spacing required for an individual pipe in the multiple pipe run. Threaded sections of rods shall not be formed or bent.

3.1.7.2 Pipe Supports and Structural Bracing, Seismic Requirements

Piping and attached valves shall be supported and braced to resist seismic loads as specified in Section 13 48 73 SEISMIC CONTROL FOR MISCELLANEOUS EQUIPMENT. Structural steel required for reinforcement to properly support piping, headers, and equipment, but not shown, shall be provided. Material used for supports shall be as specified in Section 05 12 00 STRUCTURAL STEEL.

3.1.7.3 Pipe Hangers, Inserts, and Supports

Installation of pipe hangers, inserts and supports shall conform to MSS SP-58 except as modified herein.

a. Types 5, 12, and 26 shall not be used.

b. Type 3 shall not be used on insulated pipe.

c. Type 18 inserts shall be secured to concrete forms before concrete is placed. Continuous inserts which allow more adjustment may be used if they otherwise meet the requirements for type 18 inserts.

d. Type 19 and 23 C-clamps shall be torqued per MSS SP-58 and shall have both locknuts and retaining devices furnished by the manufacturer. Field-fabricated C-clamp bodies or retaining devices are not acceptable.

e. Type 20 attachments used on angles and channels shall be furnished with an added malleable-iron heel plate or adapter.

f. Type 24 may be used only on trapeze hanger systems or on fabricated frames.

g. Type 39 saddles shall be used on insulated pipe 4 inches and larger when the temperature of the medium is 60 degrees F or higher. Type 39 saddles shall be welded to the pipe.

h. Type 40 shields shall:

(1) Be used on insulated pipe less than 4 inches.

(2) Be used on insulated pipe 4 inches and larger when the temperature of the medium is 60 degrees F or less.

(3) Have a high density insert for all pipe sizes. High density inserts shall have a density of 8 pcf or greater.

i. Horizontal pipe supports shall be spaced as specified in MSS SP-58 and a support shall be installed not over 1 foot from the pipe fitting joint at each change in direction of the piping. Pipe supports shall be spaced not over 5 feet apart at valves. Operating temperatures in determining hanger spacing for PVC or CPVC pipe shall be 120 degrees F for PVC and 180 degrees F for CPVC. Horizontal pipe runs shall include allowances for expansion and contraction.

j. Vertical pipe shall be supported at each floor, except at slab-on-grade, at intervals of not more than 15 feet nor more than 8 feet from end of risers, and at vent terminations. Vertical pipe risers shall include allowances for expansion and contraction.

k. Type 35 guides using steel, reinforced polytetrafluoroethylene (PTFE) or graphite slides shall be provided to allow longitudinal pipe movement. Slide materials shall be suitable for the system operating temperatures, atmospheric conditions, and bearing loads encountered. Lateral restraints shall be provided as needed. Where steel slides do not require provisions for lateral restraint the following may be used:

(1) On pipe 4 inches and larger when the temperature of the medium is 60 degrees F or higher, a Type 39 saddle, welded to the pipe, may freely rest on a steel plate.

(2) On pipe less than 4 inches a Type 40 shield, attached to the pipe or insulation, may freely rest on a steel plate.

(3) On pipe 4 inches and larger carrying medium less that 60 degrees F a Type 40 shield, attached to the pipe or insulation, may freely rest on a steel plate.

l. Pipe hangers on horizontal insulated pipe shall be the size of the outside diameter of the insulation. The insulation shall be continuous through the hanger on all pipe sizes and applications.

m. Where there are high system temperatures and welding to piping is not desirable, the type 35 guide shall include a pipe cradle, welded to the guide structure and strapped securely to the pipe. The pipe shall be separated from the slide material by at least 4 inches or by an amount adequate for the insulation, whichever is greater.

n. Hangers and supports for plastic pipe shall not compress, distort, cut or abrade the piping, and shall allow free movement of pipe except where otherwise required in the control of expansion/contraction.

3.1.7.4 Structural Attachments

Attachment to building structure concrete and masonry shall be by cast-in concrete inserts, built-in anchors, or masonry anchor devices. Inserts and anchors shall be applied with a safety factor not less than 5. Supports shall not be attached to metal decking. Supports shall not be attached to the underside of concrete filled floor or concrete roof decks unless approved by the Contracting Officer. Masonry anchors for overhead applications shall be constructed of ferrous materials only.

3.1.8 Welded Installation

Plumbing pipe weldments shall be as indicated. Changes in direction of piping shall be made with welding fittings only; mitering or notching pipe to form elbows and tees or other similar type construction will not be permitted. Branch connection may be made with either welding tees or forged branch outlet fittings. Branch outlet fittings shall be forged, flared for improvement of flow where attached to the run, and reinforced against external strains. Beveling, alignment, heat treatment, and inspection of weld shall conform to ASME B31.1. Weld defects shall be removed and repairs made to the weld, or the weld joints shall be entirely removed and rewelded. After filler metal has been removed from its original package, it shall be protected or stored so that its characteristics or welding properties are not affected. Electrodes that have been wetted or that have lost any of their coating shall not be used.

3.1.9 Pipe Cleanouts

Pipe cleanouts shall be the same size as the pipe except that cleanout plugs larger than 4 inches will not be required. A cleanout installed in connection with cast-iron soil pipe shall consist of a long-sweep 1/4 bend or one or two 1/8 bends extended to the place shown. An extra-heavy cast-brass or cast-iron ferrule with countersunk cast-brass head screw plug shall be caulked into the hub of the fitting and shall be flush with the floor. Cleanouts in connection with other pipe, where indicated, shall be T-pattern, 90-degree branch drainage fittings with cast-brass screw plugs, except plastic plugs shall be installed in plastic pipe. Plugs shall be the same size as the pipe up to and including 4 inches. Cleanout tee branches with screw plug shall be installed at the foot of soil and waste stacks, at the foot of interior downspouts, on each connection to building storm drain where interior downspouts are indicated, and on each building drain outside the building. Cleanout tee branches may be omitted on stacks in single story buildings with slab-on-grade construction or where less than 18 inches of crawl space is provided under the floor. Cleanouts on pipe concealed in partitions shall be provided with chromium plated bronze, nickel bronze, nickel brass or stainless steel flush type access cover plates. Round access covers shall be provided and secured to plugs with securing screw. Square access

covers may be provided with matching frames, anchoring lugs and cover screws. Cleanouts in finished walls shall have access covers and frames installed flush with the finished wall. Cleanouts installed in finished floors subject to foot traffic shall be provided with a chrome-plated cast brass, nickel brass, or nickel bronze cover secured to the plug or cover frame and set flush with the finished floor. Heads of fastening screws shall not project above the cover surface. Where cleanouts are provided with adjustable heads, the heads shall be cast iron or plastic.

3.2 WATER HEATERS AND HOT WATER STORAGE TANKS

3.2.1 Relief Valves

No valves shall be installed between a relief valve and its water heater or storage tank. The P&T relief valve shall be installed where the valve actuator comes in contact with the hottest water in the heater. Whenever possible, the relief valve shall be installed directly in a tapping in the tank or heater; otherwise, the P&T valve shall be installed in the hot-water outlet piping. A vacuum relief valve shall be provided on the cold water supply line to the hot-water storage tank or water heater and mounted above and within 6 inches above the top of the tank or water heater.

3.2.2 Heat Traps

Piping to and from each water heater and hot water storage tank shall be routed horizontally and downward a minimum of 2 feet before turning in an upward direction.

3.2.3 Connections to Water Heaters

Connections of metallic pipe to water heaters shall be made with dielectric unions or flanges.

3.2.4 Expansion Tank

A pre-charged expansion tank shall be installed on the cold water supply between the water heater inlet and the cold water supply shut-off valve. The Contractor shall adjust the expansion tank air pressure, as recommended by the tank manufacturer, to match incoming water pressure.

3.3 FIXTURES AND FIXTURE TRIMMINGS

Polished chromium-plated pipe, valves, and fittings shall be provided where exposed to view. Angle stops, straight stops, stops integral with the faucets, or concealed type of lock-shield, and loose-key pattern stops for supplies with threaded, sweat or solvent weld inlets shall be furnished and installed with fixtures. Where connections between copper tubing and faucets are made by rubber compression fittings, a beading tool shall be used to mechanically deform the tubing above the compression fitting. Exposed traps and supply pipes for fixtures and equipment shall be connected to the rough piping systems at the wall, unless otherwise specified under the item. Floor and wall escutcheons shall be as specified. Drain lines and hot water lines of fixtures for handicapped personnel shall be insulated and do not require polished chrome finish. Plumbing fixtures and accessories shall be installed within the space shown.

3.3.1 Fixture Connections

Where space limitations prohibit standard fittings in conjunction with the cast-iron floor flange, special short-radius fittings shall be provided. Connections between earthenware fixtures and flanges on soil pipe shall be made gastight and watertight with a closet-setting compound or neoprene gasket and seal. Use of natural rubber gaskets or putty will not be permitted. Fixtures with outlet flanges shall be set the proper distance from floor or wall to make a first-class joint with the closet-setting compound or gasket and fixture used.

3.3.2 Flushometer Valves

Flushometer valves shall be secured to prevent movement by anchoring the long finished top spud connecting tube to wall adjacent to valve with approved metal bracket. Flushometer valves for water closets shall be installed 39 inches above the floor, except at water closets intended for use by the physically handicapped where flushometer valves shall be mounted at approximately 30 inches above the floor and arranged to avoid interference with grab bars. In addition, for water closets intended for handicap use, the flush valve handle shall be installed on the wide side of the enclosure.

3.3.3 Height of Fixture Rims Above Floor

Lavatories shall be mounted with rim 31 inches above finished floor. Wall-hung drinking fountains and water coolers shall be installed with rim 42 inches above floor. Wall-hung service sinks shall be mounted with rim 28 inches above the floor. Installation of fixtures for use by the physically handicapped shall be in accordance with ICC A117.1.

3.3.4 Shower Bath Outfits

The area around the water supply piping to the mixing valves and behind the escutcheon plate shall be made watertight by caulking or gasketing.

3.3.5 Fixture Supports

Fixture supports for off-the-floor lavatories, urinals, water closets, and other fixtures of similar size, design, and use, shall be of the chair-carrier type. The carrier shall provide the necessary means of mounting the fixture, with a foot or feet to anchor the assembly to the floor slab. Adjustability shall be provided to locate the fixture at the desired height and in proper relation to the wall. Support plates, in lieu of chair carrier, shall be fastened to the wall structure only where it is not possible to anchor a floor-mounted chair carrier to the floor slab.

3.3.5.1 Support for Solid Masonry Construction

Chair carrier shall be anchored to the floor slab. Where a floor-anchored chair carrier cannot be used, a suitable wall plate shall be imbedded in the masonry wall.

3.3.5.2 Support for Concrete-Masonry Wall Construction

Chair carrier shall be anchored to floor slab. Where a floor-anchored chair carrier cannot be used, a suitable wall plate shall be fastened to the concrete wall using through bolts and a back-up plate.

3.3.5.3 Support for Steel Stud Frame Partitions

Chair carrier shall be used. The anchor feet and tubular uprights shall be of the heavy duty design; and feet (bases) shall be steel and welded to a square or rectangular steel tube upright. Wall plates, in lieu of floor-anchored chair carriers, shall be used only if adjoining steel partition studs are suitably reinforced to support a wall plate bolted to these studs.

3.3.5.4 Support for Wood Stud Construction

Where floor is a concrete slab, a floor-anchored chair carrier shall be used. Where entire construction is wood, wood crosspieces shall be installed. Fixture hanger plates, supports, brackets, or mounting lugs shall be fastened with not less than No. 10 wood screws, 1/4 inch thick minimum steel hanger, or toggle bolts with nut. The wood crosspieces shall extend the full width of the fixture and shall be securely supported.

3.3.5.5 Wall-Mounted Water Closet Gaskets

Where wall-mounted water closets are provided, reinforced wax, treated felt, or neoprene gaskets shall be provided. The type of gasket furnished shall be as recommended by the chair-carrier manufacturer.

3.3.6 Backflow Prevention Devices

Plumbing fixtures, equipment, and pipe connections shall not cross connect or interconnect between a potable water supply and any source of nonpotable water. Backflow preventers shall be installed where indicated and in accordance with IAPMO UPC at all other locations necessary to preclude a cross-connect or interconnect between a potable water supply and any nonpotable substance. In addition backflow preventers shall be installed at all locations where the potable water outlet is below the flood level of the equipment, or where the potable water outlet will be located below the level of the nonpotable substance. Backflow preventers shall be located so that no part of the device will be submerged. Backflow preventers shall be of sufficient size to allow unrestricted flow of water to the equipment, and preclude the backflow of any nonpotable substance into the potable water system. Bypass piping shall not be provided around backflow preventers. Access shall be provided for maintenance and testing. Each device shall be a standard commercial unit.

3.3.7 Access Panels

Access panels shall be provided for concealed valves and controls, or any item requiring inspection or maintenance. Access panels shall be of sufficient size and located so that the concealed items may be serviced, maintained, or replaced. Access panels shall be as specified in Section 08 31 00 ACCESS DOORS AND PANELS.

3.3.8 Sight Drains

Sight drains shall be installed so that the indirect waste will terminate 2 inches above the flood rim of the funnel to provide an acceptable air gap.

3.3.9 Traps

Each trap shall be placed as near the fixture as possible, and no fixture shall be double-trapped. Traps installed on cast-iron soil pipe shall be cast iron. Traps installed on steel pipe or copper tubing shall be recess-drainage pattern, or brass-tube type. Traps installed on plastic pipe may be plastic conforming to ASTM D3311. Traps for acid-resisting waste shall be of the same material as the pipe.

3.3.10 Shower Pans

Before installing shower pan, subfloor shall be free of projections such as nail heads or rough edges of aggregate. Drain shall be a bolt-down, clamping-ring type with weepholes, installed so the lip of the subdrain is flush with subfloor.

3.3.10.1 General

The floor of each individual shower, the shower-area portion of combination shower and drying room, and the entire shower and drying room where the two are not separated by curb or partition, shall be made watertight with a shower pan fabricated in place. The shower pan material shall be cut to size and shape of the area indicated, in one piece to the maximum extent practicable, allowing a minimum of 6 inches for turnup on walls or partitions, and shall be folded over the curb with an approximate return of 1/4 of curb height. The upstands shall be placed behind any wall or partition finish. Subflooring shall be smooth and clean, with nailheads driven flush with surface, and shall be sloped to drain. Shower pans shall be clamped to drains with the drain clamping ring.

3.3.10.2 Metal Shower Pans

When a shower pan of required size cannot be furnished in one piece, metal pieces shall be joined with a flintlock seam and soldered or burned. The corners shall be folded, not cut, and the corner seam shall be soldered or burned. Pans, including upstands, shall be coated on all surfaces with one brush coat of asphalt. Asphalt shall be applied evenly at not less than 1 gallon per 50 square feet. A layer of felt covered with building paper shall be placed between shower pans and wood floors. The joining surfaces of metal pan and drain shall be given a brush coat of asphalt after the pan is connected to the drain.

3.3.10.3 Plasticized Chlorinated Polyethylene Shower Pans

Corners of plasticized chlorinated polyethylene shower pans shall be folded against the upstand by making a pig-ear fold. Hot-air gun or heat lamp shall be used in making corner folds. Each pig-ear corner fold shall be nailed or stapled 1/2 inch from the upper edge to hold it in place. Nails shall be galvanized large-head roofing nails. On metal framing or studs, approved duct tape shall be used to secure pig-ear fold and membrane. Where no backing is provided between the studs, the membrane slack shall be taken up by pleating and stapling or nailing to studding 1/2 inch from upper edge. To adhere the membrane to vertical surfaces, the back of the membrane and the surface to which it will be applied shall be coated with adhesive that becomes dry to the touch in 5 to 10 minutes, after which the membrane shall be pressed into place. Surfaces to be solvent-welded shall be clean. Surfaces to be joined with xylene shall be initially sprayed and vigorously cleaned with a cotton cloth, followed by final coating of xylene and the joining of the surfaces by roller or

equivalent means. If ambient or membrane temperatures are below 40 degrees F the membrane and the joint shall be heated prior to application of xylene. Heat may be applied with hot-air gun or heat lamp, taking precautions not to scorch the membrane. Adequate ventilation and wearing of gloves are required when working with xylene. Membrane shall be pressed into position on the drain body, and shall be cut and fit to match so that membrane can be properly clamped and an effective gasket-type seal provided. On wood subflooring, two layers of 15 pound dry felt shall be installed prior to installation of shower pan to ensure a smooth surface for installation.

3.3.10.4 Nonplasticized Polyvinyl Chloride (PVC) Shower Pans

Nonplasticized PVC shall be turned up behind walls or wall surfaces a distance of not less than 6 inches in room areas and 3 inches above curb level in curbed spaces with sufficient material to fold over and fasten to outside face of curb. Corners shall be pig-ear type and folded between pan and studs. Only top 1 inch of upstand shall be nailed to hold in place. Nails shall be galvanized large-head roofing type. Approved duct tape shall be used on metal framing or studs to secure pig-ear fold and membrane. Where no backing is provided between studs, the membrane slack shall be taken up by pleating and stapling or nailing to studding at top inch of upstand. To adhere the membrane to vertical surfaces, the back of the membrane and the surface to which it is to be applied shall be coated with adhesive that becomes dry to the touch in 5 to 10 minutes, after which the membrane shall be pressed into place. Trim for drain shall be exactly the size of drain opening. Bolt holes shall be pierced to accommodate bolts with a tight fit. Adhesive shall be used between pan and subdrain. Clamping ring shall be bolted firmly. A small amount of gravel or porous materials shall be placed at weepholes so that holes remain clear when setting bed is poured. Membrane shall be solvent welded with PVC solvent cement. Surfaces to be solvent welded shall be clean (free of grease and grime). Sheets shall be laid on a flat surface with an overlap of about 2 inches. Top edge shall be folded back and surface primed with a PVC primer. PVC cement shall be applied and surfaces immediately placed together, while still wet. Joint shall be lightly rolled with a paint roller, then as the joint sets shall be rolled firmly but not so hard as to distort the material. In long lengths, about 2 or 3 feet at a time shall be welded. On wood subflooring, two layers of 15 pound felt shall be installed prior to installation of shower pan to ensure a smooth surface installation.

3.4 VIBRATION-ABSORBING FEATURES

Mechanical equipment, including compressors and pumps, shall be isolated from the building structure by approved vibration-absorbing features, unless otherwise shown. Each foundation shall include an adequate number of standard isolation units. Each unit shall consist of machine and floor or foundation fastening, together with intermediate isolation material, and shall be a standard product with printed load rating. Piping connected to mechanical equipment shall be provided with flexible connectors. Vibration isolators shall have a minimum isolation efficiency of 90 percent at the lowest disturbing frequency.

3.5 WATER METER REMOTE READOUT REGISTER

The remote readout register shall be mounted at the location indicated or as directed by the Contracting Officer.

3.6 IDENTIFICATION SYSTEMS

3.6.1 Identification Tags

Identification tags made of brass, engraved laminated plastic, or engraved anodized aluminum, indicating service and valve number shall be installed on valves, except those valves installed on supplies at plumbing fixtures. Tags shall be 1-3/8 inch minimum diameter, and marking shall be stamped or engraved. Indentations shall be black, for reading clarity. Tags shall be attached to valves with No. 12 AWG, copper wire, chrome-plated beaded chain, or plastic straps designed for that purpose.

3.6.2 Pipe Color Code Marking

Color code marking of piping shall be as specified in Section 09 90 00 PAINTS AND COATINGS.

3.6.3 Color Coding Scheme for Locating Hidden Utility Components

Scheme shall be provided in buildings having suspended grid ceilings. The color coding scheme shall identify points of access for maintenance and operation of operable components which are not visible from the finished space and installed in the space directly above the suspended grid ceiling. The operable components shall include valves, dampers, switches, linkages and thermostats. The color coding scheme shall consist of a color code board and colored metal disks. Each colored metal disk shall be approximately 3/8 inch in diameter and secured to removable ceiling panels with fasteners. The fasteners shall be inserted into the ceiling panels so that the fasteners will be concealed from view. The fasteners shall be manually removable without tools and shall not separate from the ceiling panels when panels are dropped from ceiling height. Installation of colored metal disks shall follow completion of the finished surface on which the disks are to be fastened. The color code board shall have the approximate dimensions of 3 foot width, 30 inches height, and 1/2 inch thickness. The board shall be made of wood fiberboard and framed under glass or 1/16 inch transparent plastic cover. Unless otherwise directed, the color code symbols shall be approximately 3/4 inch in diameter and the related lettering in 1/2 inch high capital letters. The color code board shall be mounted and located in the mechanical or equipment room. The color code system shall match the Base standard. Coordinate with COR.:

3.7 ESCUTCHEONS

Escutcheons shall be provided at finished surfaces where bare or insulated piping, exposed to view, passes through floors, walls, or ceilings, except in boiler, utility, or equipment rooms. Escutcheons shall be fastened securely to pipe or pipe covering and shall be satin-finish, corrosion-resisting steel, polished chromium-plated zinc alloy, or polished chromium-plated copper alloy. Escutcheons shall be either one-piece or split-pattern, held in place by internal spring tension or setscrew.

3.8 PAINTING

Painting of pipes, hangers, supports, and other iron work, either in concealed spaces or exposed spaces, is specified in Section 09 90 00 PAINTS AND COATINGS.

3.8.1 Painting of New Equipment

New equipment painting shall be factory applied or shop applied, and shall be as specified herein, and provided under each individual section.

3.8.1.1 Factory Painting Systems

Manufacturer's standard factory painting systems may be provided subject to certification that the factory painting system applied will withstand 125 hours in a salt-spray fog test, except that equipment located outdoors shall withstand 500 hours in a salt-spray fog test. Salt-spray fog test shall be in accordance with ASTM B117, and for that test the acceptance criteria shall be as follows: immediately after completion of the test, the paint shall show no signs of blistering, wrinkling, or cracking, and no loss of adhesion; and the specimen shall show no signs of rust creepage beyond 0.125 inch on either side of the scratch mark.

The film thickness of the factory painting system applied on the equipment shall not be less than the film thickness used on the test specimen. If manufacturer's standard factory painting system is being proposed for use on surfaces subject to temperatures above 120 degrees F, the factory painting system shall be designed for the temperature service.

3.8.1.2 Shop Painting Systems for Metal Surfaces

Clean, pretreat, prime and paint metal surfaces; except aluminum surfaces need not be painted. Apply coatings to clean dry surfaces. Clean the surfaces to remove dust, dirt, rust, oil and grease by wire brushing and solvent degreasing prior to application of paint, except metal surfaces subject to temperatures in excess of 120 degrees F shall be cleaned to bare metal.

Where more than one coat of paint is specified, apply the second coat after the preceding coat is thoroughly dry. Lightly sand damaged painting and retouch before applying the succeeding coat. Color of finish coat shall be aluminum or light gray.

a. Temperatures Less Than 120 Degrees F: Immediately after cleaning, the metal surfaces subject to temperatures less than 120 degrees F shall receive one coat of pretreatment primer applied to a minimum dry film thickness of 0.3 mil, one coat of primer applied to a minimum dry film thickness of one mil; and two coats of enamel applied to a minimum dry film thickness of one mil per coat.

b. Temperatures Between 120 and 400 Degrees F: Metal surfaces subject to temperatures between 120 and 400 degrees F shall receive two coats of 400 degrees F heat-resisting enamel applied to a total minimum thickness of 2 mils.

c. Temperatures Greater Than 400 Degrees F: Metal surfaces subject to temperatures greater than 400 degrees F shall receive two coats of 600 degrees F heat-resisting paint applied to a total minimum dry film thickness of 2 mils.

3.9 TESTS, FLUSHING AND DISINFECTION

3.9.1 Plumbing System

The following tests shall be performed on the plumbing system in accordance with IAPMO UPC, except that the drainage and vent system final test shall include the smoke test. The Contractor has the option to perform a peppermint test in lieu of the smoke test. If a peppermint test is chosen, the Contractor must submit a testing procedure and reasons for choosing this option in lieu of the smoke test to the Contracting Officer for approval.

a. Drainage and Vent Systems Test. The final test shall include a smoke test.

b. Building Sewers Tests.

c. Water Supply Systems Tests.

3.9.1.1 Test of Backflow Prevention Assemblies

Backflow prevention assembly shall be tested using gauges specifically designed for the testing of backflow prevention assemblies.

Backflow prevention assembly test gauges shall be tested annually for accuracy in accordance with the requirements of State or local regulatory agencies. If there is no State or local regulatory agency requirements, gauges shall be tested annually for accuracy in accordance with the requirements of University of Southern California's Foundation of Cross Connection Control and Hydraulic Research or the American Water Works Association Manual of Cross Connection (Manual M-14), or any other approved testing laboratory having equivalent capabilities for both laboratory and field evaluation of backflow prevention assembly test gauges. Report form for each assembly shall include, as a minimum, the following:

Data on Device	Data on Testing Firm
Type of Assembly	Name
Manufacturer	Address
Model Number	Certified Tester
Serial Number	Certified Tester No.
Size	Date of Test
Location	
Test Pressure Readings	Serial Number and Test Data of Gauges

If the unit fails to meet specified requirements, the unit shall be repaired and retested.

3.9.1.2 Shower Pans

After installation of the pan and finished floor, the drain shall be temporarily plugged below the weep holes. The floor area shall be flooded with water to a minimum depth of 1 inch for a period of 24 hours. Any drop in the water level during test, except for evaporation, will be reason for rejection, repair, and retest.

3.9.2 Defective Work

If inspection or test shows defects, such defective work or material shall be replaced or repaired as necessary and inspection and tests shall be repeated. Repairs to piping shall be made with new materials. Caulking of screwed joints or holes will not be acceptable.

3.9.3 System Flushing

3.9.3.1 During Flushing

Before operational tests or disinfection, potable water piping system shall be flushed with potable water. Sufficient water shall be used to produce a water velocity that is capable of entraining and removing debris in all portions of the piping system. This requires simultaneous operation of all fixtures on a common branch or main in order to produce a flushing velocity of approximately 4 fps through all portions of the piping system. In the event that this is impossible due to size of system, the Contracting Officer (or the designated representative) shall specify the number of fixtures to be operated during flushing. Contractor shall provide adequate personnel to monitor the flushing operation and to ensure that drain lines are unobstructed in order to prevent flooding of the facility. Contractor shall be responsible for any flood damage resulting from flushing of the system. Flushing shall be continued until entrained dirt and other foreign materials have been removed and until discharge water shows no discoloration. All faucets and drinking water fountains, to include any device considered as an end point device by NSF/ANSI 61, Section 9, shall be flushed a minimum of 0.25 gallons per 24 hour period, ten times over a 14 day period.

3.9.3.2 After Flushing

System shall be drained at low points. Strainer screens shall be removed, cleaned, and replaced. After flushing and cleaning, systems shall be prepared for testing by immediately filling water piping with clean, fresh potable water. Any stoppage, discoloration, or other damage to the finish, furnishings, or parts of the building due to the Contractor's failure to properly clean the piping system shall be repaired by the Contractor. When the system flushing is complete, the hot-water system shall be adjusted for uniform circulation. Flushing devices and automatic control systems shall be adjusted for proper operation according to manufacturer's instructions. Flow rates on fixtures must not exceed those stated in PART 2 of this Section. Unless more stringent local requirements exist, lead levels shall not exceed limits established by 40 CFR 141.80 (c)(1). The water supply to the building shall be tested separately to ensure that any lead contamination found during potable water system testing is due to work being performed inside the building.

3.9.4 Operational Test

Upon completion of flushing and prior to disinfection procedures, the

Contractor shall subject the plumbing system to operating tests to demonstrate satisfactory installation, connections, adjustments, and functional and operational efficiency. Such operating tests shall cover a period of not less than 8 hours for each system and shall include the following information in a report with conclusion as to the adequacy of the system:

a. Time, date, and duration of test.

b. Water pressures at the most remote and the highest fixtures.

c. Operation of each fixture and fixture trim.

d. Operation of each valve, hydrant, and faucet.

e. Pump suction and discharge pressures.

f. Temperature of each domestic hot-water supply.

g. Operation of each floor and roof drain by flooding with water.

h. Operation of each vacuum breaker and backflow preventer.

i. Complete operation of each water pressure booster system, including pump start pressure and stop pressure.

3.9.5 Disinfection

After all system components are provided and operational tests are complete, the entire domestic hot- and cold-water distribution system shall be disinfected. Before introducing disinfecting chlorination material, entire system shall be flushed with potable water until any entrained dirt and other foreign materials have been removed.

Water chlorination procedure shall be in accordance with AWWA C651 and AWWA C652 as modified and supplemented by this specification. The chlorinating material shall be hypochlorites or liquid chlorine. The chlorinating material shall be fed into the water piping system at a constant rate at a concentration of at least 50 parts per million (ppm). Feed a properly adjusted hypochlorite solution injected into the system with a hypochlorinator, or inject liquid chlorine into the system through a solution-feed chlorinator and booster pump until the entire system is completely filled.

Test the chlorine residual level in the water at 6 hour intervals for a continuous period of 24 hours. If at the end of a 6 hour interval, the chlorine residual has dropped to less than 25 ppm, flush the piping including tanks with potable water, and repeat the above chlorination procedures. During the chlorination period, each valve and faucet shall be opened and closed several times.

After the second 24 hour period, verify that no less than 25 ppm chlorine residual remains in the treated system. The 24 hour chlorination procedure must be repeated until no less than 25 ppm chlorine residual remains in the treated system.

Upon the specified verification, the system including tanks shall then be flushed with potable water until the residual chlorine level is reduced to less than one part per million. During the flushing

period, each valve and faucet shall be opened and closed several times.

Take additional samples of water in disinfected containers, for bacterial examination, at locations specified by the Contracting Officer. Test these samples for total coliform organisms (coliform bacteria, fecal coliform, streptococcal, and other bacteria) in accordance with EPA SM 9223. The testing method used shall be EPA approved for drinking water systems and shall comply with applicable local and state requirements.

Disinfection shall be repeated until bacterial tests indicate the absence of coliform organisms (zero mean coliform density per 100 milliliters) in the samples for at least 2 full days. The system will not be accepted until satisfactory bacteriological results have been obtained.

3.10 POSTED INSTRUCTIONS

Framed instructions under glass or in laminated plastic, including wiring and control diagrams showing the complete layout of the entire system, shall be posted where directed. Condensed operating instructions explaining preventive maintenance procedures, methods of checking the system for normal safe operation, and procedures for safely starting and stopping the system shall be prepared in typed form, framed as specified above for the wiring and control diagrams and posted beside the diagrams. The framed instructions shall be posted before acceptance testing of the systems.

3.11 PERFORMANCE OF WATER HEATING EQUIPMENT

Standard rating condition terms are as follows:

EF = Energy factor, minimum overall efficiency.

ET = Minimum thermal efficiency with 70 degrees F delta T.

SL = Standby loss is maximum (Btu/h) based on a 70 degrees F temperature difference between stored water and ambient requirements.

V = Rated volume in gallons

Q = Nameplate input rate in kW (Btu/h)

3.11.1 Storage Water Heaters

3.11.1.1 Electric

a. Storage capacity of 60 gallons shall have a minimum energy factor (EF) of 0.93 or higher per FEMP requirements.

b. Storage capacity of 60 gallons or more shall have a minimum energy factor (EF) of 0.91 or higher per FEMP requirements.

3.12 TABLES

TABLE I

PIPE AND FITTING MATERIALS FOR DRAINAGE, WASTE, VENT AND CONDENSATE DRAIN PIPING SYSTEMS

It #	Pipe and Fitting Materials	SERVICE A	SERVICE B	SERVICE C	SERVICE D	SERVICE E	SERVICE F	SERVICE G
1	Cast iron soil pipe and fittings, hub and spigot, ASTM A74 with compression gaskets. Pipe and fittings shall be marked with the CISPI trademark.	X	X	X	X	X		
2	Cast iron soil pipe and fittings hubless, CISPI 301 and ASTM A888. Pipe and fittings shall be marked with the CISPI trademark.		X	X	X	X		
16	Copper drainage tube, (DWV), ASTM B306	X*	X	X*	X	X		X
17	Wrought copper and wrought alloy solder-joint drainage fittings. ASME B16.29	X	X	X	X	X		X
18	Cast copper alloy solder joint drainage fittings, DWV, ASME B16.23	X	X	X	X	X		X

SERVICE:

A - Underground Building Soil, Waste and Storm Drain
B - Aboveground Soil, Waste, Drain In Buildings
C - Underground Vent
D - Aboveground Vent
E - Interior Rainwater Conductors Aboveground
F - Corrosive Waste And Vent Above And Belowground
G - Condensate Drain Aboveground

* - Hard Temper

TABLE II					
PIPE AND FITTING MATERIALS FOR PRESSURE PIPING SYSTEMS					
Item #	Pipe and Fitting Materials	SERVICE A	SERVICE B	SERVICE C	SERVICE D
1	Malleable-iron threaded fittings:				
	a. Galvanized, ASME B16.3 for use with Item 4a	X	X	X	X
	b. Same as "a" but not galvanized for use with Item 4b			X	
2	Grooved pipe couplings, ferrous pipe ASTM A536 and ASTM A47/A47M, non-ferrous pipe, ASTM A536 and ASTM A47/A47M	X	X	X	
3	Ductile iron grooved joint fittings for ferrous pipe ASTM A536 and ASTM A47/A47M, for use with Item 2	X	X	X	
4	Steel pipe:				
	a. Seamless, galvanized, ASTM A53/A53M, Type S, Grade B	X	X	X	X
	b. Seamless, black, ASTM A53/A53M, Type S, Grade B			X	
5	Seamless red brass pipe, ASTM B43	X	X		X
6	Bronze flanged fittings, ASME B16.24 for use with Items 5 and 7	X	X		X
7	Seamless copper pipe, ASTM B42	X	X		X
8	Seamless copper water tube, ASTM B88, ASTM B88M	X**	X**	X**	X***
9	Cast bronze threaded fittings, ASME B16.15 for use with Items 5 and 7	X	X		X

TABLE II					
PIPE AND FITTING MATERIALS FOR PRESSURE PIPING SYSTEMS					
Item #	Pipe and Fitting Materials	SERVICE A	SERVICE B	SERVICE C	SERVICE D
10	Wrought copper and bronze solder-joint pressure fittings, ASME B16.22 for use with Items 5, 7 and 8	X	X	X	X
11	Cast copper alloy solder-joint pressure fittings, ASME B16.18 for use with Item 8	X	X	X	X
12	Bronze and sand castings groovedjoint pressure fittings for non-ferrous pipe ASTM B584, for use with Item 2	X	X	X	
19	Chlorinated polyvinyl chloride (CPVC) plastic hot and cold water distribution system, ASTM D2846/D2846M	X	X		X
20	Chlorinated polyvinyl chloride (CPVC) plastic pipe, Schedule 40 and 80, ASTM F441/F441M	X	X		X
21	Chlorinated polyvinyl chloride (CPVC) plastic pipe (SDR-PR) ASTM F442/F442M	X	X		X
22	Threaded chlorinated polyvinyl chloride (chloride CPVC) plastic pipe fittings, Schedule 80, ASTM F437 for use with Items 20, and 21	X	X		X
23	Socket-type chlorinated polyvinyl chloride (CPVC) plastic pipe fittings, Schedule 40, ASTM F438 for use with Items 20, 21, and 22	X	X		X
24	Socket-type chlorinated polyvinyl chloride (CPVC) plastic pipe fittings Schedule 80, ASTM F439 for use with Items 20, 21, and 22	X	X		X
32	Steel pipeline flanges, MSS SP-44	X	X		

TABLE II					
PIPE AND FITTING MATERIALS FOR PRESSURE PIPING SYSTEMS					
Item #	Pipe and Fitting Materials	SERVICE A	SERVICE B	SERVICE C	SERVICE D
33	Fittings: brass or bronze; ASME B16.15, and ASME B16.18 ASTM B828	X	X		
34	Carbon steel pipe unions, socket-welding and threaded, MSS SP-83	X	X	X	
35	Malleable-iron threaded pipe unions ASME B16.39	X	X		
36	Nipples, pipe threaded ASTM A733	X	X	X	
38	Press Fittings	X	X		
	SERVICE: A - Cold Water Service Aboveground B - Hot and Cold Water Distribution 180 degrees F Maximum Aboveground C - Compressed Air Lubricated D - Cold Water Service Belowground Indicated types are minimum wall thicknesses. ** - Type L - Hard *** - Type K - Hard temper with brazed joints only or type K-soft temper without joints in or under floors **** - In or under slab floors only brazed joints				

-- End of Section --

PROJECT TABLE OF CONTENTS

DIVISION 00 - PROCUREMENT AND CONTRACTING REQUIREMENTS

00 01 15 LIST OF DRAWINGS

DIVISION 01 - GENERAL REQUIREMENTS

01 11 00 SUMMARY OF WORK
01 14 00 WORK RESTRICTIONS
01 30 00 ADMINISTRATIVE REQUIREMENTS
01 32 01.00 10 PROJECT SCHEDULE
01 33 00 SUBMITTAL PROCEDURES
01 33 29 SUSTAINABILITY REQUIREMENTS AND REPORTING
01 35 13 SPECIAL PROJECT PROCEDURES
01 35 26 GOVERNMENTAL SAFETY REQUIREMENTS
01 42 00 SOURCES FOR REFERENCE PUBLICATIONS
01 45 00 QUALITY CONTROL
01 45 35 SPECIAL INSPECTIONS
01 50 00 TEMPORARY CONSTRUCTION FACILITIES AND CONTROLS
01 57 19 TEMPORARY ENVIRONMENTAL CONTROLS
01 74 19 CONSTRUCTION WASTE MANAGEMENT AND DISPOSAL
01 78 00 CLOSEOUT SUBMITTALS
01 78 23 OPERATION AND MAINTENANCE DATA
01 91 00.15 10 TOTAL BUILDING COMMISSIONING

DIVISION 02 - Not Used

DIVISION 03 - CONCRETE

03 30 00 CAST-IN-PLACE CONCRETE
03 62 16 METALLIC NON-SHRINK GROUTING

DIVISION 04 - MASONRY

04 20 00 UNIT MASONRY

DIVISION 05 - METALS

05 05 20 POST-INSTALLED CONCRETE AND MASONRY ANCHORS
05 05 23.16 STRUCTURAL WELDING
05 12 00 STRUCTURAL STEEL
05 21 00 STEEL JOIST FRAMING
05 30 00 STEEL DECKS
05 40 00 COLD-FORMED METAL FRAMING
05 50 13 MISCELLANEOUS METAL FABRICATIONS
05 51 00 METAL STAIRS
05 51 33 METAL LADDERS
05 52 00 METAL RAILINGS

DIVISION 06 - WOOD, PLASTICS, AND COMPOSITES

06 10 00 ROUGH CARPENTRY
06 41 16.00 10 PLASTIC-LAMINATE-CLAD ARCHITECTURAL CABINETS
06 61 16 SOLID SURFACING FABRICATIONS

DIVISION 07 - THERMAL AND MOISTURE PROTECTION

07 13 53 ELASTOMERIC SHEET WATERPROOFING

07 21 13 BOARD AND BLOCK INSULATION
07 21 16 MINERAL FIBER BLANKET INSULATION
07 27 10 BUILDING AIR BARRIER SYSTEM
07 27 19.01 SELF-ADHERING AIR BARRIERS
07 42 13 METAL WALL PANELS
07 54 19 POLYVINYL-CHLORIDE ROOFING
07 60 00 FLASHING AND SHEET METAL
07 84 00 FIRESTOPPING
07 92 00 JOINT SEALANTS

DIVISION 08 - OPENINGS

08 11 13 STEEL DOORS AND FRAMES
08 14 00 WOOD DOORS
08 31 00 ACCESS DOORS AND PANELS
08 34 59 VAULT DOORS AND DAY GATES
08 41 13 ALUMINUM-FRAMED ENTRANCES AND STOREFRONTS
08 51 13 ALUMINUM WINDOWS
08 56 63 DETENTION AND SECURITY WINDOWS
08 71 00 DOOR HARDWARE
08 81 00 GLAZING
08 91 00 METAL WALL LOUVERS

DIVISION 09 - FINISHES

09 22 00 SUPPORTS FOR PLASTER AND GYPSUM BOARD
09 29 00 GYPSUM BOARD
09 30 10 CERAMIC, QUARRY, AND GLASS TILING
09 51 00 ACOUSTICAL CEILINGS
09 65 00 RESILIENT FLOORING
09 68 00 CARPETING
09 90 00 PAINTS AND COATINGS
09 96 00 HIGH-PERFORMANCE COATINGS

DIVISION 10 - SPECIALTIES

10 11 00 VISUAL DISPLAY UNITS
10 14 00.10 EXTERIOR SIGNAGE
10 14 00.20 INTERIOR SIGNAGE
10 21 13 TOILET COMPARTMENTS
10 22 39 FOLDING PANEL PARTITIONS
10 26 00 WALL AND DOOR PROTECTION
10 28 13 TOILET ACCESSORIES
10 44 16 FIRE EXTINGUISHERS
10 51 13 METAL LOCKERS
10 73 20 MANUFACTURED CANOPY

DIVISION 11 - EQUIPMENT

11 81 29 FACILITY FALL PROTECTION

DIVISION 12 - FURNISHINGS

12 21 00 WINDOW BLINDS

DIVISION 13 - SPECIAL CONSTRUCTION

13 48 73 SEISMIC CONTROL FOR MISCELLANEOUS EQUIPMENT

DIVISION 14 - CONVEYING EQUIPMENT

14 21 23 ELECTRIC TRACTION PASSENGER ELEVATORS

DIVISION 21 - FIRE SUPPRESSION

21 13 13 WET PIPE SPRINKLER SYSTEMS, FIRE PROTECTION

DIVISION 22 - PLUMBING

22 00 00 PLUMBING, GENERAL PURPOSE
22 05 48.00 20 MECHANICAL SOUND, VIBRATION, AND SEISMIC CONTROL
22 07 19.00 40 PLUMBING PIPING INSULATION
22 14 29.00 40 SUMP PUMPS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

23 03 00.00 20 BASIC MECHANICAL MATERIALS AND METHODS
23 05 48.00 40 VIBRATION AND SEISMIC CONTROLS FOR HVAC PIPING AND EQUIPMENT
23 05 48.19 SEISMIC BRACING FOR HVAC
23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC
23 07 00 THERMAL INSULATION FOR MECHANICAL SYSTEMS
23 08 00.00 20 COMMISSIONING OF MECHANICAL AND PLUMBING SYSTEMS
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC
23 09 13 INSTRUMENTATION AND CONTROL DEVICES FOR HVAC
23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS
23 23 00 REFRIGERANT PIPING
23 31 13.00 40 METAL DUCTS
23 34 23.00 40 HVAC POWER VENTILATORS
23 36 00.00 40 AIR TERMINAL UNITS
23 37 13.00 40 DIFFUSERS, REGISTERS, AND GRILLES
23 74 33.00 40 PACKAGED, OUTDOOR, HEATING AND COOLING MAKEUP AIR-CONDITIONERS
23 81 29 DUCTLESS SPLIT AIR CONDITIONERS
23 83 00.00 20 ELECTRIC SPACE HEATING EQUIPMENT

DIVISION 25 - INTEGRATED AUTOMATION

25 05 11.01 CYBERSECURITY FOR MECH-HVAC FACILITY-RELATED CONTROL SYSTEMS
25 05 11.02 CYBERSECURITY FOR FLS FACILITY-RELATED CONTROL SYSTEMS

DIVISION 26 - ELECTRICAL

26 05 00.00 40 COMMON WORK RESULTS FOR ELECTRICAL
26 05 13.00 40 MEDIUM-VOLTAGE CABLES
26 05 26.00 40 GROUNDING AND BONDING FOR ELECTRICAL SYSTEMS
26 05 71.00 40 LOW VOLTAGE OVERCURRENT PROTECTIVE DEVICES
26 09 23.00 40 LIGHTING CONTROL DEVICES
26 20 00 INTERIOR DISTRIBUTION SYSTEM
26 24 16.00 40 PANELBOARDS
26 32 15.00 ENGINE-GENERATOR SET STATIONARY 15-2500 KW, WITH AUXILIARIES
26 41 00 LIGHTNING PROTECTION SYSTEM
26 51 00 INTERIOR LIGHTING
26 52 00.00 40 EMERGENCY LIGHTING
26 53 00.00 40 EXIT SIGNS

26 55 53.00 40 SECURITY LIGHTING

DIVISION 27 - COMMUNICATIONS

27 05 13.43 TELEVISION DISTRIBUTION SYSTEM
27 05 28.36 40 CABLE TRAYS FOR COMMUNICATIONS SYSTEMS
27 10 00 BUILDING TELECOMMUNICATIONS CABLING SYSTEM
27 13 23.00 40 COMMUNICATIONS OPTICAL BACKBONE CABLING

DIVISION 28 - ELECTRONIC SAFETY AND SECURITY

28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE

DIVISION 31 - EARTHWORK

31 00 00 EARTHWORK
31 23 00.00 20 EXCAVATION AND FILL

DIVISION 32 - EXTERIOR IMPROVEMENTS

32 12 16.16 ROAD-MIX ASPHALT PAVING
32 13 13.06 PORTLAND CEMENT CONCRETE PAVEMENT FOR ROADS AND SITE FACILITIES
32 16 19 CONCRETE CURBS, GUTTERS AND SIDEWALKS
32 17 23 PAVEMENT MARKINGS
32 34 13 FABRICATED PEDESTRIAN BRIDGES
32 92 19 SEEDING

DIVISION 33 - UTILITIES

33 11 00 WATER UTILITY DISTRIBUTION PIPING
33 30 00 SANITARY SEWERAGE
33 40 00 STORMWATER UTILITIES
33 46 13 FOUNDATION DRAINAGE
33 46 16 SUBDRAINAGE PIPING

DIVISION 34 - Not Used

DIVISION 35 - Not Used

DIVISION 40 - Not Used

DIVISION 41 - Not Used

DIVISION 42 - Not Used

DIVISION 43 - Not Used

DIVISION 44 - Not Used

DIVISION 45 - Not Used

DIVISION 46 - Not Used

DIVISION 48 - Not Used

-- End of Project Table of Contents --

SECTION TABLE OF CONTENTS

DIVISION 22 - PLUMBING

SECTION 22 05 48.00 20

MECHANICAL SOUND, VIBRATION, AND SEISMIC CONTROL

PART 1 GENERAL

1.1 REFERENCES
1.2 RELATED REQUIREMENTS
1.3 DEFINITIONS
1.3.1 Decibels dB
1.3.2 Manufacturer
1.3.3 Micropascal uPa
1.3.4 Picowatt pW
1.4 SYSTEM DESCRIPTION
1.4.1 Spring Isolator Data
1.4.2 Seismic Protection Criteria
1.4.3 Welding
1.5 SUBMITTALS
1.6 QUALITY ASSURANCE
1.6.1 Vibration Isolator Procurement
1.6.2 Unitized Machinery Assemblies

PART 2 PRODUCTS

2.1 CORROSION PROTECTION FOR STEEL PARTS
2.2 NEOPRENE
2.3 FLOOR-MOUNTED ISOLATORS
2.3.1 Neoprene Isolation Pads
2.3.2 Neoprene Isolators
2.4 SPRING ISOLATORS AND PROTECTED SPRING ISOLATORS
2.4.1 Springs
2.4.2 Mounting and Adjustment
2.5 SUSPENSION ISOLATORS
2.5.1 Suspension Neoprene Isolators
2.5.2 Suspension Spring Isolators
2.6 FLEXIBLE CONNECTORS FOR PIPING
2.6.1 Elastomeric Flexible Connectors
2.6.2 Metal Flexible Connectors
2.7 SEISMIC SNUBBERS FOR EQUIPMENT
2.8 PIPE GUIDES
2.9 THRUST RESTRAINTS
2.10 SEISMIC PROTECTION COMPONENTS FOR PIPING

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Vibration and Noise Isolation Components
3.1.2 Suspension Vibration Isolators
3.1.3 Vertical Stops
3.1.4 Thrust Restraints

3.1.5 Flexible Pipe and Duct Connectors
3.1.6 Seismic Snubbers
3.1.7 Piping
3.1.7.1 Piping Connected to Vibration Isolated Machinery
3.1.7.2 Steam Pressure Reducing Valves
3.1.7.3 Condenser Water
3.1.7.4 Chilled, Hot, and Dual Temperature Piping
3.1.8 Water and Steam Distribution Piping Application
3.1.9 Pipe Hanger and Support Installation
3.1.9.1 Pipe Hangers
3.1.9.2 High Temperatures
3.1.9.3 Valves
3.1.9.4 Machinery Without Flexible Connections
3.1.9.5 Twelve Inch and Larger Pipe
3.1.9.6 Pipe Risers
3.1.9.7 Supports at Base of Pipe Risers
3.1.9.8 Pipe Anchors
3.1.10 Equipment Room Sound Isolation
3.1.10.1 Pipe Penetrations
3.1.11 Seismic Restraints for Piping
3.1.12 Suspended Machinery Platforms
3.1.13 Electrical Connections
3.1.14 Systems Not To Be Vibration Isolated
3.2 FIELD QUALITY CONTROL
3.2.1 Field Inspections
3.2.2 Spring Isolator Inspection
3.2.3 Tests
3.2.3.1 Equipment Vibration Tests

-- End of Section Table of Contents --

SECTION 22 05 48.00 20

MECHANICAL SOUND, VIBRATION, AND SEISMIC CONTROL

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN WELDING SOCIETY (AWS)

AWS D1.1/D1.1M	(2020; Errata 1 2021) Structural Welding Code - Steel

ASTM INTERNATIONAL (ASTM)

ASTM A653/A653M	(2020) Standard Specification for Steel Sheet, Zinc-Coated (Galvanized) or Zinc-Iron Alloy-Coated (Galvannealed) by the Hot-Dip Process
ASTM D471	(2016a) Standard Test Method for Rubber Property - Effect of Liquids
ASTM D2240	(2015; E 2017) Standard Test Method for Rubber Property - Durometer Hardness
ASTM E84	(2020) Standard Test Method for Surface Burning Characteristics of Building Materials

SHEET METAL AND AIR CONDITIONING CONTRACTORS' NATIONAL ASSOCIATION (SMACNA)

SMACNA 1981	(2008) Seismic Restraint Manual Guidelines for Mechanical Systems, 3rd Edition

1.2 RELATED REQUIREMENTS

The provisions of Section 23 03 00.00 20 BASIC MECHANICAL MATERIALS AND METHODS apply to this section.

1.3 DEFINITIONS

1.3.1 Decibels dB

Measure of sound level. Decibels are referenced to either 20 uPa for sound pressure levels or one pW for sound power levels. dBA is the overall "A" weighted sound level.

1.3.2 Manufacturer

The fabricator or supplier of vibration-isolation or seismic-protection

materials and equipment. For mechanical equipment and machinery the term machinery manufacturer will be used.

1.3.3 Micropascal uPa

10 to the minus 6 power newtons per square meter.

1.3.4 Picowatt pW

10 to the minus 12 power watts.

1.4 SYSTEM DESCRIPTION

1.4.1 Spring Isolator Data

For each type and size of spring isolator, submit the spring outside diameter, deflection, operating spring height, unloaded spring height, solid spring height, the ratio of the outside diameter to the operating spring height, the load to deflection ratio of the springs, and weight and sizes of structural steel members.

1.4.2 Seismic Protection Criteria

Use a Horizontal Force Factor minimum 60 percent of the machinery weight considered passing through the machinery center of gravity in any horizontal direction. Unless vibration isolation is required to protect machinery against unacceptable structure transmitted noise or vibration, protect the structure or machinery from earthquakes by rigid structurally sound attachment to the load-supporting structure. Protect each piece of vibration-isolated machinery with protected spring isolators or separate seismic restraint devices. Determine by calculations the number and size of seismic restraints needed for each machinery. Verify seismic restraint vendor's calculations by a registered professional engineer. Provide seismic snubbers and protected spring isolators rated in three principle axes. Verify ratings by independent laboratory testing, by analysis of an independent licensed structural engineer.

1.4.3 Welding

AWS D1.1/D1.1M.

1.5 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Isolators

Protected Spring Isolators

Flexible Connectors

Pipe Guides

Seismic Snubbers

Thrust Restraints

SD-03 Product Data

Isolators

Protected Spring Isolators

Flexible Connectors

Pipe Guides

Seismic Snubbers

Vertical Stops

Thrust Restraints

SD-05 Design Data

Isolators

Protected Spring Isolators

Flexible Connectors

Pipe Guides

Seismic Snubbers

Thrust Restraints

SD-06 Test Reports

Seismic Snubbers

Equipment Vibration Tests

Protected Spring Isolators

SD-08 Manufacturer's Instructions

Vibration and Noise Isolation Components

Seismic Protection Components

1.6 QUALITY ASSURANCE

1.6.1 Vibration Isolator Procurement

For each piece of machinery to be isolated from vibration, supply the inertia base, machinery base, platform, rails, saddles, vibration isolators, seismic snubbers, and other associated materials and equipment as a coordinated package by a single manufacturer or by the machinery manufacturer. Select isolators that provide uniform deflection even when machinery weight is not evenly distributed. This requirement does not

include the flexible connectors or the hangers for the associated piping and ductwork.

1.6.2 Unitized Machinery Assemblies

Mounting of unitized assemblies directly on vibration isolation springs is acceptable if machinery manufacturer certifies that the end supports of the assemblies have been designed for such installation.

PART 2 PRODUCTS

2.1 CORROSION PROTECTION FOR STEEL PARTS

ASTM A653/A653M hot-dipped galvanized, or equivalent manufacturer standard coatings. Where steel parts are exposed to the weather, provide galvanized coating of at least 2 ounces of zinc per square foot of surface. Coat springs with neoprene.

2.2 NEOPRENE

ASTM D471 and ASTM D2240, Grade Durometer 40, 50, or 60, and oil resistant.

2.3 FLOOR-MOUNTED ISOLATORS

2.3.1 Neoprene Isolation Pads

Provide pads at least 1/4 inch thick with cross-ribbed or waffle design. For concentrated loads, provide steel bearing plates bonded or cold cemented to the pads.

2.3.2 Neoprene Isolators

Provide molded neoprene isolators having steel base plates with mounting holes and, at the top, steel mounting plates with mounting holes or threaded inserts. Provide elements of type and size coded with molded letters or color-coded for capacity identification. Embed metal parts completely in neoprene.

2.4 SPRING ISOLATORS AND PROTECTED SPRING ISOLATORS

Provide spring isolators or protected spring isolators that are adjustable and laterally stable with free-standing springs of horizontal stiffness at minimum 80 percent of the vertical (axial) stiffness. For machine-attached and floor-attached restraining elements, separate from metal-to-metal contact by neoprene cushions 1/8 inch thick minimum. Provide neoprene acoustic friction pads at least 1/4 inch thick.

2.4.1 Springs

Provide springs with base and compression plates, to keep spring ends parallel during and after deflection to operating height. Provide outside coil diameters at least 0.8 of the operating height. At operating height, springs shall have additional travel to complete (solid) compression equal to at least 50 percent of the operating deflection.

2.4.2 Mounting and Adjustment

Provide base and compression plates with mounting holes or threaded fittings. Bolt leveling adjustment bolts to machinery or base.

2.5 SUSPENSION ISOLATORS

Provide hangers with suspension isolators encased in open steel brackets. Isolate hanger rods from isolator steel brackets with neoprene-lined opening.

2.5.1 Suspension Neoprene Isolators

Provide double-deflection elements with minimum 3/8 inch deflection.

2.5.2 Suspension Spring Isolators

Provide hangers with springs and molded neoprene elements in series. Provide isolators with adjustable spring-preloading devices where required to maintain constant pipe elevations during installation and when pipe operational loads are transferred to the springs.

2.6 FLEXIBLE CONNECTORS FOR PIPING

Straight or elbow flexible connectors rated for temperatures, pressures, and fluids to be conveyed. Provide flexible connectors with the strength 4 times operating pressure at highest system operating temperature. Provide elbow flexible connectors with a permanently set angle.

2.6.1 Elastomeric Flexible Connectors

Fabricated of multiple plies of tire cord fabric and elastomeric materials with integral reinforced elastomeric flanges with galvanized malleable iron back up rings.

2.6.2 Metal Flexible Connectors

Fabricated of Grade E phosphor bronze, monel or corrugated stainless steel tube covered with comparable bronze or stainless steel braid restraining and pressure cover.

2.7 SEISMIC SNUBBERS FOR EQUIPMENT

Factory-fabricated, omni-directional with factory set air gaps between 1/8 inch minimum and 1/4 inch maximum. Load capacity of each snubber at 50 percent neoprene element deflection shall be 0.5g minimum. Provide replaceable neoprene elements 1/4 inch minimum thickness.

2.8 PIPE GUIDES

Factory-fabricated. Weld steel bar guides to the pipe at a maximum radial spacing of 60 degrees. The outside diameter around the guide bars shall be smaller than the inside diameter of the guide sleeve in accordance with standard field construction practice. For pipe temperatures below 60 degrees F, provide metal sleeve, minimum one pound per cubic foot density insulation.

2.9 THRUST RESTRAINTS

Adjustable spring thrust restraints, able to resist the thrust force with at least 25 percent unused capacity. The operating spring deflection shall be not less than 50 percent of the static deflection of the isolation supporting the machinery.

2.10 SEISMIC PROTECTION COMPONENTS FOR PIPING

Section 23 03 00.00 20 BASIC MECHANICAL MATERIALS AND METHODS.

PART 3 EXECUTION

3.1 INSTALLATION

3.1.1 Vibration and Noise Isolation Components

Install vibration-and-noise isolation materials and equipment in accordance with machinery manufacturer's instructions.

3.1.2 Suspension Vibration Isolators

Provide suspension isolation hangers for piping, suspended equipment, and suspended equipment platforms in mechanical equipment rooms, as specified. For operating load static deflections of 1/4 inch or less, provide neoprene pads or single deflection neoprene isolators. For operating load static deflections over 5/16 to 3/8 inch, provide double-deflection neoprene element isolators. For operating load static deflections over 3/8 inch, provide isolators with spring and neoprene elements in series.

3.1.3 Vertical Stops

For machinery affected by wind pressure or having an operational weight different from installed weight, provide resilient vertical limit stops which prevent spring extension when weight is removed. Provide vertical stops for machinery containing liquid, such as water chillers, evaporative coolers, boilers, and cooling towers. Spring isolated or protected spring isolated machinery must rock and move freely within limits of stops or seismic restraint devices.

3.1.4 Thrust Restraints

Where required, provide pairs of thrust restraints, symmetrically installed on both sides of the steady state line of thrust.

3.1.5 Flexible Pipe and Duct Connectors

Install flexible connectors in accordance with the manufacturer's instructions. When liquid pulsation dampening is required, flexible connectors with spherical configuration may be used. Provide restraints for pipe connectors at pumps to prevent connector failure upon pump startup.

3.1.6 Seismic Snubbers

Provide snubbers as close as possible to each vibration isolator as indicated. After installing and leveling of the machinery, adjust snubbers in accordance with the snubber manufacturer's instructions.

3.1.7 Piping

Provide vibration isolation for piping. The isolator deflections shall be equal to or greater than the static deflection of the vibration isolators provided for the connected machinery as follows:

3.1.7.1 Piping Connected to Vibration Isolated Machinery

For a distance of 50 feet or 50 pipe diameters, whichever is greater.

3.1.7.2 Steam Pressure Reducing Valves

Connected piping for a distance of 50 feet or 50 pipe diameters, whichever is greater.

3.1.7.3 Condenser Water

For the full length of the piping.

3.1.7.4 Chilled, Hot, and Dual Temperature Piping

For risers from pumps and for the first 20 feet of the branch connection of the main supply and return piping at each floor.

3.1.8 Water and Steam Distribution Piping Application

Resiliently support piping with combination spring and neoprene isolation hangers. Provide spring elements with 5/8 inch static deflection; install the hanger with spacing so that the first harmonic natural frequency is not less than 360 Hz. Provide double-deflection neoprene elements. For the first two isolation hangers from the rotating equipment of 3 1/2 inch and smaller piping systems, ensure a deflection equal to the equipment-isolation static deflection. For the first four piping isolation hanger supports from rotating equipment of 4 inch and larger piping systems, use resilient hanger-rod isolators at a fixed elevation regardless of load changes. Incorporate an adjustable preloading device to transfer the load to the spring element within the hanger mounting after the piping system has been filled with water.

3.1.9 Pipe Hanger and Support Installation

3.1.9.1 Pipe Hangers

Provide eye-bolts or swivel joints for pipe hangers to permit pipe thermal or mechanical movement without angular misalignment of hanger vibration isolator.

3.1.9.2 High Temperatures

Where neoprene elements of vibration isolator may be subjected to high pipe temperatures, above 160 degrees F, provide metal heat shields or thermal isolators.

3.1.9.3 Valves

Provide vibration isolation hangers and supports at modulating, pressure reducing, or control valves which will induce fluid pulsations. When required or indicated, isolate valves with flexible connectors.

3.1.9.4 Machinery Without Flexible Connections

When piping is not connected to vibrating machinery with flexible connectors, provide the first four hangers with isolation elements designed for deflections equal to equipment vibration isolator deflections (including static, operating, and start-up).

3.1.9.5 Twelve Inch and Larger Pipe

Suspend 12 inch and larger pipe vibration hangers from resilient hanger rod isolators. Resilient hanger rod isolators shall be capable of supporting pipe during installation at a fixed elevation regardless of load changes. Provide an adjustable preloading device to transfer the load to isolation element after operational load is applied. Provide 12 inch and larger pipe supports with unrestrained stable springs for one inch deflection and with built-in leveling device and resilient vertical limit stops to prevent spring elongation when partial load is removed. Provide isolators capable of providing rigid anchoring during erection of piping so that it can be erected at a fixed elevation.

3.1.9.6 Pipe Risers

Provide pipe riser supports with bearing plates and two layers of 1/4 inch thick ribbed or waffled neoprene pad loaded to not more than 50 psi. Separate isolation pads with 1/4 inch steel plate. Weld pipe riser clamps at anchor points to the pipe and to pairs of vertical acoustical pipe anchor mountings which shall be rigidly fastened to the steel framing.

3.1.9.7 Supports at Base of Pipe Risers

Piping isolation supports at the base of risers shall be two layers of 1/2 inch thick heavy-duty neoprene pad separated by 1/4 inch thick steel plate. Use bearing plates sized to provide a pad loading of not more than 500 psi. Weld the stanchion between the pipe and isolation support to the pipe and weld or bolt to the isolation support. Bolt isolation support to the floor slab with resilient sleeves and washers. Where supplementary steel is required to support piping, provide a maximum deflection of 0.08 inches at the mid-span of this steel under the load. Rigidly support piping from the supplementary steel with the supplementary steel isolated from the building structure with isolators.

3.1.9.8 Pipe Anchors

Attach each end of the pipe anchor to an omni-directional pipe isolator which in turn shall be rigidly fastened to the steel framing or structural concrete. Provide a telescoping pipe isolator of two sizes of steel tubing separated by a minimum 1/2 inch thick pad of heavy-duty neoprene or heavy-duty neoprene and canvas. Provide vertical restraints by similar material to prevent vertical travel in either direction. The load on the isolation material shall not exceed 500 psi.

3.1.10 Equipment Room Sound Isolation

Do not allow direct contact between pipe or ducts and walls, floor slabs, roofs, ceilings or partitions of equipment rooms.

3.1.10.1 Pipe Penetrations

Provide galvanized Schedule 40 pipe sleeves and tightly pack annular space between sleeves and pipe with insulation having a flame spread rating not more than 25 and a smoke developed rating not more than 50 when tested in accordance with ASTM E84, maximum effective temperature 1000 degrees F, bulk density 6 pounds/cu. ft. minimum. Provide uninsulated pipe with a one inch thick mineral fiber sleeve the full length of the penetration and seal each end with an interior or exterior and weather resistant

non-hardening compound. Provide sealant and mineral-fiber sleeve of a flame spread rating not more than 25 and a smoke developed rating not more than 50 when tested in accordance with ASTM E84.

3.1.11 Seismic Restraints for Piping

Provide seismic restraints in accordance with SMACNA 1981.

3.1.12 Suspended Machinery Platforms

Provide with vibration-isolation hangers.

3.1.13 Electrical Connections

Provide flexible conduit or multiple conductor cable connections for machinery with sufficient extra length to permit 2 inch minimum displacement in any direction without damage.

3.1.14 Systems Not To Be Vibration Isolated

Do not provide vibration isolation for electrical raceways and conduits or for fire protection, storm, sanitary, and domestic water piping systems which do not include pumps or other vibrating, rotating, or pulsating equipment including control and pressure reducing valves.

3.2 FIELD QUALITY CONTROL

Provide equipment and apparatus required for performing inspections and tests. Notify Contracting Officer 14 days prior to machinery vibration testing. Rebalance, adjust, or replace machinery with noise or vibration levels in excess of those given in the machinery specifications, or machinery manufacturer's data.

3.2.1 Field Inspections

Prior to initial operation, inspect the vibration isolators and seismic snubbers for conformance to drawings, specifications, and manufacturer's data and instructions. Check for vibration and noise transmission through connections, piping, ductwork, foundations, and walls. Check connector alignment before and after filling of system and during operation. Correct misalignment without damage to connector and in accordance with manufacturer's recommendations.

3.2.2 Spring Isolator Inspection

After installation of spring isolators or protected spring isolators, and seismic restraint devices, the machinery shall rock freely on its spring isolators within limits of stops or seismic restraint devices. Eliminate or correct interferences.

3.2.3 Tests

Adjust, repair, or replace isolators as required to reduce vibration and noise transmissions to specified levels.

3.2.3.1 Equipment Vibration Tests

Perform vibration tests to determine conformance with vibration isolation schedule specified .

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 22 - PLUMBING

SECTION 22 07 19.00 40

PLUMBING PIPING INSULATION

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 QUALITY CONTROL
1.3.1 Recycled Materials

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION
2.1.1 Performance Requirements
2.2 COMPONENTS
2.2.1 Insulation
2.2.1.1 Cellular Elastomer Insulation
2.2.1.2 Fiberglass Insulation
2.2.1.3 Pipe Fittings
2.2.1.4 Flexible Blankets
2.2.2 Adhesives
2.2.2.1 Lagging Adhesive
2.2.2.2 Vapor-Barrier Material Adhesives
2.2.2.3 Cellular Elastomer Insulation Adhesive
2.2.3 Insulating Cement
2.2.3.1 General Purpose Insulating Cement
2.2.3.2 Finishing Insulating Cement
2.2.4 Caulk
2.2.5 Corner Angles
2.2.6 Jacketing
2.2.6.1 Aluminum Jacket
2.2.6.2 PVC Jacket
2.2.7 Coatings
2.2.7.1 Indoor Vapor-Barrier Finishing
2.2.7.2 Vapor Retarder
2.2.7.3 Cellular-Elastomer Finishing
2.2.7.4 Coating Color
2.2.8 Tape
2.3 MATERIALS

PART 3 EXECUTION

3.1 PREPARATION
3.2 INSTALLATION OF INSULATION SYSTEMS
3.2.1 Hot-Water, Steam, and Condensate-Return Piping
3.2.2 Cold-Water and Condensate-Drain Piping
3.3 APPLICATION
3.3.1 Type T-3, Cellular Elastomer
3.4 CLOSEOUT ACTIVITIES

-- End of Section Table of Contents --

SECTION 22 07 19.00 40

PLUMBING PIPING INSULATION

PART 1 GENERAL

Section 22 00 00 PLUMBING, GENERAL PURPOSE applies to work specified in this section.

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ASTM INTERNATIONAL (ASTM)

ASTM B209	(2014) Standard Specification for Aluminum and Aluminum-Alloy Sheet and Plate
ASTM C195	(2007; R 2013) Standard Specification for Mineral Fiber Thermal Insulating Cement
ASTM C449	(2007; R 2013) Standard Specification for Mineral Fiber Hydraulic-Setting Thermal Insulating and Finishing Cement
ASTM C534/C534M	(2020a) Standard Specification for Preformed Flexible Elastomeric Cellular Thermal Insulation in Sheet and Tubular Form
ASTM C547	(2022) Standard Specification for Mineral Fiber Pipe Insulation
ASTM C647	(2008; R 2013) Properties and Tests of Mastics and Coating Finishes for Thermal Insulation
ASTM C795	(2008; R 2018) Standard Specification for Thermal Insulation for Use in Contact with Austenitic Stainless Steel
ASTM C916	(2020) Standard Specification for Adhesives for Duct Thermal Insulation
ASTM C920	(2018) Standard Specification for Elastomeric Joint Sealants
ASTM C921	(2010; R 2015) Standard Practice for Determining the Properties of Jacketing Materials for Thermal Insulation
ASTM C1136	(2021) Standard Specification for Flexible, Low Permeance Vapor Retarders for Thermal Insulation

ASTM D579/D579M	(2015) Standard Specification for Greige Woven Glass Fabrics
ASTM D5590	(2000; R 2010; E 2012) Standard Test Method for Determining the Resistance of Paint Films and Related Coatings to Fungal Defacement by Accelerated Four-Week Agar Plate Assay
ASTM E84	(2020) Standard Test Method for Surface Burning Characteristics of Building Materials
ASTM E96/E96M	(2022) Standard Test Methods for Gravimetric Determination ofWater Vapor Transmission Rate of Materials

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 220	(2021) Standard on Types of Building Construction

SOCIETY OF AUTOMOTIVE ENGINEERS INTERNATIONAL (SAE)

SAE AMS 3779	(2016; Rev B) Tape Adhesive, Pressure Sensitive Thermal Radiation Resistant, Aluminum Foil/Glass Cloth

U.S. DEPARTMENT OF DEFENSE (DOD)

MIL-A-3316	(1987; Rev C; Am 2 1990) Adhesives, Fire-Resistant, Thermal Insulation
MIL-PRF-19565	(1988; Rev C) Coating Compounds, Thermal Insulation, Fire- and Water-Resistant, Vapor-Barrier

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Installation Drawings

SD-03 Product Data

Adhesives

Coatings

Insulating Cement

Insulation Materials

Jacketing

Tape

SD-08 Manufacturer's Instructions

Installation Manual

SD-11 Closeout Submittals

Record Drawings

Adhesives

Coatings

Insulation Materials

Recycled Materials

1.3 QUALITY CONTROL

1.3.1 Recycled Materials

Provide thermal insulation containing recycled materials to the extent practicable, provided that the material meets all other requirements of this section. The minimum recycled material content of the following insulation types are:

a. Rock Wool - 75 percent slag by weight

b. Fiberglass - 20-25 percent glass cullet by weight

c. Plastic Rigid Foam - 9 percent recovered material

d. Polyisocyanurate/Polyurethane - 9 percent recovered material

e. Rigid Foam - 9 percent recovered material

Submit recycled materials documentation indicating percentage of post-industrial and post-consumer recycled content per unit of product. Indicate relative dollar value of recycled content products to total dollar value of products included in project.

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION

2.1.1 Performance Requirements

Provide noncombustible thermal-insulation system materials, as defined by NFPA 220. Provide adhesives, coatings, sealants, facings, jackets, and thermal-insulation materials, except cellular elastomers, with a flame-spread classification (FSC) of 25 or less , and a smoke-developed classification (SDC) of 50 or less . Determine these maximum values in accordance with ASTM E84 . Provide coatings and sealants that are nonflammable in their wet state.

Provide adhesives, coatings, and sealants with published or certified temperature ratings suitable for the entire range of working temperatures normal for the surfaces to which they are to be applied.

2.2 COMPONENTS

2.2.1 Insulation

2.2.1.1 Cellular Elastomer Insulation

Provide cellular elastomer insulation conforming to ASTM C534/C534M. Ensure the water vapor permeability does not exceed 0.30 grain per foot per inch per hour per square foot mercury pressure difference for 1-inch thickness of cellular elastomer.

2.2.1.2 Fiberglass Insulation

Conform to ASTM C547. Ensure the apparent thermal conductivity does not exceed 0.23 Btu-inch per hour per square foot per degree F at 75 degrees F mean.

Fiber glass pipe insulation having an insulating efficiency not less than that of the specified thickness of mineral fiber pipe insulation may be provided in lieu of mineral fiber pipe insulation for aboveground piping.

2.2.1.3 Pipe Fittings

Provide molded pipe fitting insulation covering for use at temperatures up to and including 1200 degrees F.

2.2.1.4 Flexible Blankets

Provide flexible blankets and felts for use at temperatures up to and including 350 degrees F with a density of 1 pound per cubic foot. Ensure thermal conductivity is no greater than 0.26 Btu per hour per square foot per degree F at 75 degrees F mean.

2.2.2 Adhesives

2.2.2.1 Lagging Adhesive

Lagging is the material used for thermal insulation, especially around a cylindrical object. This may include the insulation as well as the cloth/material covering the insulation. To resist mold/mildew, ensure lagging adhesive conforms to ASTM D5590 with 0 growth rating. Provide nonflammable and fire-resistant lagging adhesives with a maximum flame spread index of 25 and a maximum smoke developed index of 50 when tested in accordance with ASTM E84. Adhesive are MIL-A-3316, Class 1, pigmented white and suitable for bonding fibrous glass cloth to faced and unfaced fibrous glass insulation board; for bonding cotton brattice cloth to faced and unfaced fibrous glass insulation board; for sealing edges of and bonding glass tape to joints of fibrous glass board; for bonding lagging cloth to thermal insulation; or Class 2 for attaching fibrous glass insulation to metal surfaces. Apply lagging adhesives in strict accordance with the manufacturer's recommendations for pipe and duct insulation.

2.2.2.2 Vapor-Barrier Material Adhesives

Ensure adhesives conform to the requirements of ASTM C916, Type I, when attaching fibrous-glass insulation to metal surfaces or attaching insulation to itself, to metal, and to various other substrates.

2.2.2.3 Cellular Elastomer Insulation Adhesive

For cellular elastomer insulation adhesive, provide a solvent cutback chloroprene elastomer conforming to ASTM C916, Type I, and is approved by the manufacturer of the cellular elastomer for the intended use.

2.2.3 Insulating Cement

2.2.3.1 General Purpose Insulating Cement

Provide general purpose insulating cement, mineral fiber, conforming to ASTM C195. Ensure composite is rated for1800 degrees F service, with a thermal-conductivity maximum of 0.85 Btu per inch per hour per square foot for each degree F temperature differential at 200 degrees F mean temperature for a 1 inch thickness.

2.2.3.2 Finishing Insulating Cement

Provide finishing insulating cement of a mineral-fiber, hydraulic-setting type conforming to ASTM C449.

2.2.4 Caulk

Provide elastomeric joint sealant in accordance with ASTM C920, Type S, Grade NS, Class 25, Use A.

2.2.5 Corner Angles

Provide a nominal 0.016 inch thick aluminum 1 by 1 inch corner angle piping insulation with factory applied kraft backing. Ensure aluminum conforms to ASTM B209, Alloy 3003 .

2.2.6 Jacketing

2.2.6.1 Aluminum Jacket

Provide aluminum jackets conforming ASTM B209, Temper H14, minimum thickness of 0.016 inch, with factory-applied polyethylene and kraft paper moisture barrier on the inside surface. Provide smooth surface jackets for jacket outside diameters less than 8 inches. Provide corrugated surface jackets for jacket outside diameters 8 inches and larger. Provide stainless steel bands, minimum width of 0.5 inch. Provide factory prefabricated aluminum covers for insulation on fittings, valves, and flanges.

2.2.6.2 PVC Jacket

Provide 0.010 inch thick, factory-premolded polyvinylchloride, one-piece fitting pipe-barrel sheeting vapor-barrier jacketing that is self-extinguishing, with high-impact strength and moderate chemical resistance. Ensure jacket has a permeability rating of 0.01 grain per hour per square foot per inch of mercury pressure difference, determined in accordance with ASTM E96/E96M. Provide manufacturer's standard

solvent-weld type vapor-barrier joint adhesive.

Ensure conformance to ASTM C1136 for, Type I, low-vapor transmission, high-puncture resistance vapor barriers.

2.2.7 Coatings

2.2.7.1 Indoor Vapor-Barrier Finishing

Provide a pigmented resin and solvent compound coatings conforming to ASTM C1136, Type II.

2.2.7.2 Vapor Retarder

The vapor retarder coating shall be fire and water resistant and appropriately selected for either outdoor or indoor service. Color shall be white. The water vapor permeance of the compound shall be 0.013 perms or less at 43 mils dry film thickness as determined according to procedure B of ASTM E96/E96M utilizing apparatus described in ASTM E96/E96M. The coating shall be nonflammable, fire resistant type. To resist mold/mildew, coating shall meet ASTM D5590 with 0 growth rating. Coating shall meet MIL-PRF-19565 Type II (if selected for indoor service) and be Qualified Products Database listed. All other application and service properties shall be in accordance with ASTM C647.

2.2.7.3 Cellular-Elastomer Finishing

Provide a polyvinylchloride lacquer coating recommended by the manufacturer of the cellular elastomer finish.

2.2.7.4 Coating Color

Provide as specified by the Contracting Officer for the coating color.

2.2.8 Tape

Provide a knitted elastic cloth glass lagging specifically suitable for continuous spiral wrapping of insulated pipe bends and fittings that produces a smooth, tight, wrinkle-free surface. Conform to requirements of SAE AMS 3779, ASTM D579/D579M, and ASTM C921 for tape, weighing not less than 10 ounces per square yard.

2.3 MATERIALS

Submit manufacturer's catalog data for the following items:

a. Adhesives

b. Coatings

c. Insulating Cement

d. Insulation Materials

e. Jacketing

f. Tape

Provide compatible materials that do not contribute to corrosion, soften,

or otherwise attack surfaces to which applied, in either the wet or dry state. Meet ASTM C795 requirements for materials to be used on stainless steel surfaces. Provide materials that are asbestos free.

PART 3 EXECUTION

Apply insulation only to the system or component surfaces that have previously been tested and approved by the Contracting Officer.

3.1 PREPARATION

Submit installation drawings for pipe insulation, conforming with the adhesive manufacturer's written instructions for installation. Submit installation manual clearly stating the manufacturer's instructions for insulation materials.

Clean surfaces to remove oil and grease before insulation adhesives or mastics are applied. Provide solvent cleaning required to bring metal surfaces to such condition.

3.2 INSTALLATION OF INSULATION SYSTEMS

Apply materials in conformance with the recommendations of the manufacturer.

Install smooth and continuous contours on exposed work. Smoothly and securely paste down cemented laps, flaps, bands, and tapes. Apply adhesives on a full-coverage basis.

Install insulation lengths tightly butted against each other at joints. Where lengths are cut, provide smooth and square and without breakage of end surfaces. Where insulation terminates, neatly taper and effectively seal ends, or finish as specified. Direct longitudinal seams of exposed insulation away from normal view.

Use insulation meeting maximum value conductance as tested at any point, do not use an average. Meet or exceed the specified maximum conductance by adding additional insulation thickness.

3.2.1 Hot-Water, Steam, and Condensate-Return Piping

Install a fiberglass insulation with all service jacket, with a thickness of not less than 1 inch for piping 1-1/4 inch and smaller, 1-1/2 inch for piping 1-1/2 inch and larger.. Insulate aboveground pipes, valve bodies, fittings, unions, flanges, and miscellaneous surfaces.

3.2.2 Cold-Water and Condensate-Drain Piping

Insulate aboveground pipes, valve bodies, fittings, unions, flanges, and miscellaneous surfaces.

Providefiberglass insulation for cold water piping, with a thickness of 1/2 inch for pipe 1-1/4 inch and smaller, 1 inch for pipe 1-1/2 inch and larger. Use expanded, closed-cell pipe insulation only aboveground, not for underground piping.

3.3 APPLICATION

3.3.1 Type T-3, Cellular Elastomer

Cover piping-system surfaces with flexible cellular-elastomer sheet or preformed insulation. Maintain vapor seal. Cement insulation into continuous material using a solvent cutback chloroprene adhesive recommended by the manufacturer for the specific purpose. Apply adhesive to both of the contact surfaces on a 100-percent coverage basis to a minimum thickness of 10-mils wet or approximately 150 square feet per gallon of undiluted adhesive.

Set cold water piping insulation into an outdoor vapor-barrier coating applied intermittently over a minimum length of 6 inches at maximum intervals of 12 feet. At piping supports, ensure insulation is continuous by using outside-carrying type clevis hangers with insulation shield. Install Wood dowel load-bearing inserts between the pipe and insulation shields to prevent insulation compression.

At pipe hangers or supports where the insulation rests on the pipe hanger strap, cut the insulation with a brass cork borer and insert a No. 3 superior grade cork. Seal seams with approved adhesive. Insulate sweat fitting with miter-cut pieces of cellular elastomer insulation of the same nominal pipe size and thickness as the insulation on the adjacent piping or tubing. Join miter-cut pieces with approved adhesive. Slit and snap covers over the fitting, and seal joints with approved adhesive.

Insulate screwed fittings with sleeve-type covers formed from miter-cut pieces of cellular elastomer thermal insulation having an inside diameter large enough to overlap adjacent pipe insulation. Lap pipe insulation against fittings, and overlap not less than 1 inch. Use adhesive to join cover pieces and cement the cover to the pipe insulation.

Finish surfaces exposed to view or ultraviolet light with not less than a 2 mil minimum dry-film thickness application of a polyvinylchloride lacquer recommended by the manufacturer. Apply in not less than two coats.

3.4 CLOSEOUT ACTIVITIES

Final acceptance of the performed work is dependent upon providing Record Drawings details to the Contracting Officer. Include construction details, by building area, the insulation material type, amount, and installation method. An illustration or map of the pipe routing locations may serve this purpose.

Provide a cover letter/sheet clearly marked with the system name, date, and the words "Record Drawings Insulation/Material" for the data. Forward to the Condition Monitoring Office for inclusion in the Maintenance Database."

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 22 - PLUMBING

SECTION 22 14 29.00 40

SUMP PUMPS

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 DELIVERY, STORAGE, AND HANDLING

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION
2.2 EQUIPMENT
2.2.1 Submersible Pumps
2.2.1.1 Pump Selection
2.2.1.2 Pump Housing
2.2.1.3 Impeller
2.2.1.4 Pump Shaft
2.2.1.5 Mechanical Seal
2.2.1.6 Bearings and Lubrication
2.2.1.7 Motor and Power Cord
2.2.1.8 Liquid-Level Control
2.2.1.9 Sump Tank and Coverplate
2.3 High-Water Alarm
2.4 Painting

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Alignment
3.2 FIELD QUALITY CONTROL
3.2.1 Vibration Analyzer
3.2.2 Pump Acceptance
3.3 CLOSEOUT ACTIVITIES

-- End of Section Table of Contents --

SECTION 22 14 29.00 40

SUMP PUMPS

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

HYDRAULIC INSTITUTE (HI)

HI M100	(2009) HI Pump Standards Set

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

ISO 1940-1	(2003; R 2008) Mechanical Vibration - Balance Quality Requirements for Rotors in a Constant (Rigid) State - Part 1: Specification and Verification of Balance Tolerances

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA 250	(2020) Enclosures for Electrical Equipment (1000 Volts Maximum)
NEMA MG 1	(2021) Motors and Generators

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Connection Diagrams

Control Diagrams

Installation Drawings

SD-03 Product Data

Manufacturer's Catalog Data

Pump Performance Curve

Spare Parts List

Special Tools

Submersible Pumps

Accessories

SD-06 Test Reports

Hydrostatic Leak

Static Heads

Pump Flow Capacity

SD-08 Manufacturer's Instructions

Manufacturer's Installation Instructions

Vibration Specifications

1.3 DELIVERY, STORAGE, AND HANDLING

Inspect the pump for damage or other distress when received at the project site. Store the pump and associated equipment indoors as recommended by the pump manufacturer, protected from construction or weather hazards at the project site. Before installation, provide adequate short-term storage for the pump and equipment in a covered, dry, and ventilated location. Follow the manufacturer's instructions for extended storage.

PART 2 PRODUCTS

Provide a pump and motor with vibration levels conforming to ISO 1940-1 unless otherwise noted. Ensure that motor vibration levels conform to NEMA MG 1, Motors and Generators, Part 7, unless otherwise noted.

2.1 SYSTEM DESCRIPTION

Show details of connection of cables and pump motors on connection diagrams for sump pumps.

Submit control diagrams for sump pumps showing motor starters, relays, or any other component necessary for safe operation.

Ensure that installation drawings for sump pumps are in accordance with the manufacturer's recommended instructions.

Submit manufacturer's catalog data for sump pumps showing the sump pump size, type, and efficiency rating along with performance data, including pump performance curve, indicating brake horsepower, head, flow rate, and NPSH (net positive suction head). Also include equipment foundation data and equipment data.

Provide manufacturer's installation instructions and vibration specifications.

2.2 EQUIPMENT

2.2.1 Submersible Pumps

Construct and furnish pumps and accessories in accordance with the requirements of HI M100 standards and those specified herein.

Provide a duplex pump unit that includes a submersible pump with an automatic level-control mechanism mounted above water level.

Install an operating switch such that in case of failure, the operating switch does not require breaking of pump-motor seals for repairs.

Ensure that requirements for each material designation are in accordance with the applicable definition listed in the centrifugal pump section of HI M100 standards.

Avoid contact between dissimilar metals. Where such contact cannot be avoided, protect joints between dissimilar metals against galvanic corrosion by plating, organic-insulation coatings, gaskets, or other suitable means.

2.2.1.1 Pump Selection

Provide a pump with duty conditions as indicated on drawings.

Ensure that pump seals, lubricant, and electrical insulation are suitable for service in liquids up to 140 degrees F.

2.2.1.2 Pump Housing

Provide a pump housing that encloses the pump motor and volute with its integrally cast feet. Provide a cast-iron pump housing that is watertight under all heads normal to the service, and constructed to permit inspection and repair. Furnish a volute designed to withstand a hydrostatic pressure of not less than 1-1/2 times the design shutoff head of the pump.

2.2.1.3 Impeller

Provide a cast-iron nonclogging impeller designed to provide maximum freedom from clogging when liquid-containing rags and stringy material is handled. Provide an impeller that is dynamically balanced and that has a minimum solid-sphere handling capability of 1-1/2 inches.

2.2.1.4 Pump Shaft

Provide a pump shaft that is an extension of the motor shaft and constructed of ground and polished AISI Type 300 or 400 series corrosion-resistant steel with hard-wearing surfaces (over 300 Brinell).

2.2.1.5 Mechanical Seal

Provide the manufacturer's standard mechanical pump shaft seal specifically constructed for the service duty temperature and resistance to pumped fluid.

2.2.1.6 Bearings and Lubrication

Furnish antifriction ball- or roller-bearings with full provision for the mechanical and hydraulic, radial, and thrust loads imposed. Seal and permanently grease- or oil-lubricate the bearings.

2.2.1.7 Motor and Power Cord

Provide a permanently sealed, oil-filled, and watertight motor of the manufacturer's standard construction for the service. Fit the motor space with watertight expansion provisions to accommodate the temperature normal to the specified duty. Ensure that the motor seals remain watertight under any pressure developed in the volute and under a sump-level static head of not less than 30 feet of water.

Ensure that circuits for three-phase motors provide overload protection.

Provide single-phase motors with automatic-reset thermal-overload protection.

Provide a waterproof, internally grounded, oil-resistant, Type SO chloroprene power cord, with a three-prong plug of the indicated length.

2.2.1.8 Liquid-Level Control

Furnish simplex units with a float-operated switch mechanism to ensure automatic operation of the pump unit when the liquid in the sump rises to a predetermined level. Provide a cover-mounted switch and Type 1, general-purpose enclosure in accordance with NEMA 250. Provide a means of adjustment such as float-rod stops to allow for variation in the start and stop level-control points. Provide an AISI Type 304 or 316 corrosion-resistant steel float and stem. Provide bronze, brass, or materials of equivalent resistance to the corrosive effects of the pumped fluid for all other wetted parts of the fluid-level sensing mechanism.

Furnish a duplex pump unit with the electrical and mechanical devices necessary to provide automatic operation of the pump unit when the liquid in the sump rises to a predetermined level. Provide controls that automatically transfer the operating cycle from one pump to the other and that operate both pumps simultaneously whenever the inflow to the sump exceeds the capacity of the operating pump. Provide a means of adjustment such as float-rod stops to allow for variations in the start and stop level-control points. Provide an AISI Type 304 or 316 corrosion-resistant steel float and rod. For all other wetted parts of the fluid-level sensing mechanism, use bronze, brass, or other material of equivalent resistance to the corrosive effects of the pumped fluid.

Mount the controls on the discharge pipe below the basin cover. Provide Type 6 enclosures in accordance with NEMA 250.

Pedestal-mount the controls above the coverplate. Provide Type 1, general-purpose enclosures conforming to NEMA 250.

Provide stilling tubes where indicated.

Floatless electrode level controls may be submitted for approval provided that the electrodes are isolated from the fluid being sensed.

2.2.1.9 Sump Tank and Coverplate

a. Tank

Provide a cast-iron, sump tank sized as indicated.

Furnish a standard opening for connection to the drainage inflow pipe in the indicated size and location with respect to the top of the tank.

Protect the interior surfaces of the concrete-sump by not less than a two-coat, two-component system of amine-cured coal-tar epoxy totaling 15 mils in thickness.

b. Coverplate

Provide a cast-iron or steel sump coverplate, of adequate strength to support not less than 200 pounds per square foot without distortion. Seal all openings through the sump cover to be gastight and watertight. Provide a standard outlet for a vent pipe. Ensure that the sump cover provides a manhole access to the interior.

2.3 High-Water Alarm

Provide a high-water alarm switch complete with actuating mechanism for operation on an electrical circuit other than the motor circuit. Design the switch to operate the indicated alarm devices whenever a predetermined high-water level is reached in the sump. Provide a switch enclosure that is the same as the level-control switch.

2.4 Painting

Treat and paint equipment in accordance with the manufacturer's standard practice for the specified duty.

PART 3 EXECUTION

3.1 INSTALLATION

Install equipment in accordance with manufacturer's recommendations.

3.1.1 Alignment

Before attempting alignment, demonstrate that the pump does not have any load/force imposed by the piping system. Minimum alignment values (below) are for pump and driver at normal running temperatures. Compensate values for thermal growth. Correct limited movement of the pump or driver (commonly known as bolt-bound) to ensure alignment capability. Ensure that holddown bolts are not undercut in order to perform adjustment.

Ensure that shims are commercially die-cut, without seams or folds, and are made of corrosion-resistant stainless steel. Do not use more than four shims at any single point.

For units with drive motors over 7.5 hp, install alignment jack bolts.

Pump and driver may have an intermediate shaft, spacer, or spool piece (sometimes called a jackshaft) Based on the motor's nominal operating speed, align the pump and driver to the following minimum specifications:

Speed(RPM)	close-coupled offset(mils)	close-coupled angle(mils/in)	spool piece angle (mils/in @ coupling pt.)
600	6.0	2.0	3.0
900	5.0	1.5	2.0
1200	4.0	1.0	1.5
1800	3.0	0.5	1.0
3600	1.5	0.4	0.5
7200	1.0	0.3	0.4

Provide final alignment settings as part of the final test data.

3.2 FIELD QUALITY CONTROL

3.2.1 Vibration Analyzer

Use a Fast Fourier Transform (FFT) analyzer to measure vibration levels. Provide an FFT analyzer with the following characteristics: a dynamic range greater than 70 dB; a minimum of 400 line resolution; a frequency response range of 5 Hz to 10 kHz (300 to 600,000 cpm); the capacity to perform ensemble averaging; the capability to use a Hanning window; autoranging frequency amplitude; a minimum amplitude accuracy over the selected frequency range of plus or minus 20 percent or plus or minus 1.5 dB.

Use an accelerometer (either stud-mounted or mounted using a rare-earth, low-mass magnet) and sound disk(or finished surface) with the FFT analyzer to collect data. Ensure that the mass of the accelerometer and its mounting has minimal influence on the frequency response of the system over the selected measurement range.

3.2.2 Pump Acceptance

Ensure that vibration analysis verifies pump conformance to specifications. Ensure that vibration levels are not more than 0.075 in/sec at 1 times run speed and at pump frequency, and 0.04 in/sec at other multiples of run speed.

Perform tests, including hydrostatic leak checking of piping and operation of equipment, in accordance with the manufacturer's instructions.

Operate pumps against static heads indicated, and verify pump flow capacity.

Provide final test reports to the Contracting Officer. Provide reports with a cover letter/sheet clearly marked with the System name, Date, and the words "Final Test Reports - Forward to the Systems Engineer/Condition Monitoring Office/Predictive Testing Group for inclusion in the Maintenance Database."

3.3 CLOSEOUT ACTIVITIES

Submit six copies of the manufacturer' complete spare parts list, showing

all parts, spare parts, and bulletins for pumps. Clearly show all details and parts, and adequately describe parts or furnish proper identification marks. Drawings incorporated in the parts lists may be reduced to one-page size provided that they are clear and legible, or the full-size drawings may be folded to the size of the list pages. Photographs or catalog cuts of components may be included for identification.

Furnish one set of all special tools necessary to completely assemble, disassemble, or maintain the pumps. "Special tools" refers to oversized or specially dimensioned tools, special attachments or fixtures, or any similar items.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 03 00.00 20

BASIC MECHANICAL MATERIALS AND METHODS

PART 1 GENERAL

1.1 REFERENCES
1.2 RELATED REQUIREMENTS
1.3 QUALITY ASSURANCE
1.3.1 Material and Equipment Qualifications
1.3.2 Alternative Qualifications
1.3.3 Service Support
1.3.4 Manufacturer's Nameplate
1.3.5 Modification of References
1.3.5.1 Definitions
1.3.5.2 Administrative Interpretations
1.4 DELIVERY, STORAGE, AND HANDLING
1.5 ELECTRICAL REQUIREMENTS
1.6 INSTRUCTION TO GOVERNMENT PERSONNEL
1.7 ACCESSIBILITY

PART 2 PRODUCTS

PART 3 EXECUTION

3.1 PAINTING OF NEW EQUIPMENT
3.1.1 Factory Painting Systems
3.1.2 Shop Painting Systems for Metal Surfaces

-- End of Section Table of Contents --

SECTION 23 03 00.00 20

BASIC MECHANICAL MATERIALS AND METHODS

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ASTM INTERNATIONAL (ASTM)

ASTM B117	(2019) Standard Practice for Operating Salt Spray (Fog) Apparatus

1.2 RELATED REQUIREMENTS

This section applies to all sections of Divisions: 21, FIRE SUPPRESSION; 22, PLUMBING; and 23, HEATING, VENTILATING, AND AIR CONDITIONING of this project specification, unless specified otherwise in the individual section.

1.3 QUALITY ASSURANCE

1.3.1 Material and Equipment Qualifications

Provide materials and equipment that are standard products of manufacturers regularly engaged in the manufacture of such products, which are of a similar material, design and workmanship. Standard products must have been in satisfactory commercial or industrial use for 2 years prior to bid opening. The 2-year use must include applications of equipment and materials under similar circumstances and of similar size. The product must have been for sale on the commercial market through advertisements, manufacturers' catalogs, or brochures during the 2 year period.

1.3.2 Alternative Qualifications

Products having less than a two-year field service record will be acceptable if a certified record of satisfactory field operation for not less than 6000 hours, exclusive of the manufacturer's factory or laboratory tests, can be shown.

1.3.3 Service Support

The equipment items must be supported by service organizations. Submit a certified list of qualified permanent service organizations for support of the equipment which includes their addresses and qualifications. These service organizations must be reasonably convenient to the equipment installation and able to render satisfactory service to the equipment on a regular and emergency basis during the warranty period of the contract.

1.3.4 Manufacturer's Nameplate

For each item of equipment, provide a nameplate bearing the manufacturer's

name, address, model number, and serial number securely affixed in a conspicuous place; the nameplate of the distributing agent will not be acceptable.

1.3.5 Modification of References

In each of the publications referred to herein, consider the advisory provisions to be mandatory, as though the word, "must" had been substituted for "should" wherever it appears. Interpret references in these publications to the "authority having jurisdiction", or words of similar meaning, to mean the Contracting Officer.

1.3.5.1 Definitions

For the International Code Council (ICC) Codes referenced in the contract documents, advisory provisions must be considered mandatory, the word "should" is interpreted as "must." Reference to the "code official" must be interpreted to mean the "Contracting Officer." For Navy owned property, references to the "owner" must be interpreted to mean the "Contracting Officer." For leased facilities, references to the "owner" must be interpreted to mean the "lessor." References to the "permit holder" must be interpreted to mean the "Contractor."

1.3.5.2 Administrative Interpretations

For ICC Codes referenced in the contract documents, the provisions of Chapter 1, "Administrator," do not apply. These administrative requirements are covered by the applicable Federal Acquisition Regulations (FAR) included in this contract and by the authority granted to the Officer in Charge of Construction to administer the construction of this project. References in the ICC Codes to sections of Chapter 1, must be applied appropriately by the Contracting Officer as authorized by his administrative cognizance and the FAR.

1.4 DELIVERY, STORAGE, AND HANDLING

Handle, store, and protect equipment and materials to prevent damage before and during installation in accordance with the manufacturer's recommendations, and as approved by the Contracting Officer. Replace damaged or defective items.

1.5 ELECTRICAL REQUIREMENTS

Furnish motors, controllers, disconnects and contactors with their respective pieces of equipment. Motors, controllers, disconnects and contactors must conform to and have electrical connections provided under Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Furnish internal wiring for components of packaged equipment as an integral part of the equipment. Extended voltage range motors will not be permitted. Controllers and contactors shall have a maximum of 120 volt control circuits, and must have auxiliary contacts for use with the controls furnished. When motors and equipment furnished are larger than sizes indicated, the cost of additional electrical service and related work must be included under the section that specified that motor or equipment. Power wiring and conduit for field installed equipment must be provided under and conform to the requirements of Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM.

1.6 INSTRUCTION TO GOVERNMENT PERSONNEL

When specified in other sections, furnish the services of competent instructors to give full instruction to the designated Government personnel in the adjustment, operation, and maintenance, including pertinent safety requirements, of the specified equipment or system. Instructors must be thoroughly familiar with all parts of the installation and must be trained in operating theory as well as practical operation and maintenance work.

Instruction must be given during the first regular work week after the equipment or system has been accepted and turned over to the Government for regular operation. The number of man-days (8 hours per day) of instruction furnished must be as specified in the individual section. When more than 4 man-days of instruction are specified, use approximately half of the time for classroom instruction. Use other time for instruction with the equipment or system.

When significant changes or modifications in the equipment or system are made under the terms of the contract, provide additional instruction to acquaint the operating personnel with the changes or modifications.

1.7 ACCESSIBILITY

Install all work so that parts requiring periodic inspection, operation, maintenance, and repair are readily accessible. Install concealed valves, expansion joints, controls, dampers, and equipment requiring access, in locations freely accessible through access doors.

PART 2 PRODUCTS

Not Used

PART 3 EXECUTION

3.1 PAINTING OF NEW EQUIPMENT

New equipment painting must be factory applied or shop applied, and must be as specified herein, and provided under each individual section.

3.1.1 Factory Painting Systems

Manufacturer's standard factory painting systems may be provided subject to certification that the factory painting system applied will withstand 125 hours in a salt-spray fog test, except that equipment located outdoors must withstand 500 hours in a salt-spray fog test. Salt-spray fog test must be in accordance with ASTM B117, and for that test the acceptance criteria must be as follows: immediately after completion of the test, the paint must show no signs of blistering, wrinkling, or cracking, and no loss of adhesion; and the specimen must show no signs of rust creepage beyond 0.125 inch on either side of the scratch mark.

The film thickness of the factory painting system applied on the equipment must not be less than the film thickness used on the test specimen. If manufacturer's standard factory painting system is being proposed for use on surfaces subject to temperatures above 120 degrees F, the factory painting system must be designed for the temperature service.

3.1.2 Shop Painting Systems for Metal Surfaces

Clean, pretreat, prime and paint metal surfaces; except aluminum surfaces need not be painted. Apply coatings to clean dry surfaces. Clean the surfaces to remove dust, dirt, rust, oil and grease by wire brushing and solvent degreasing prior to application of paint, except metal surfaces subject to temperatures in excess of 120 degrees F must be cleaned to bare metal.

Where more than one coat of paint is specified, apply the second coat after the preceding coat is thoroughly dry. Lightly sand damaged painting and retouch before applying the succeeding coat. Color of finish coat must be aluminum or light gray.

a. Temperatures Less Than 120 Degrees F: Immediately after cleaning, the metal surfaces subject to temperatures less than 120 degrees F must receive one coat of pretreatment primer applied to a minimum dry film thickness of 0.3 mil, one coat of primer applied to a minimum dry film thickness of 1 mil; and two coats of enamel applied to a minimum dry film thickness of 1 mil per coat.

b. Temperatures Between 120 and 400 Degrees F: Metal surfaces subject to temperatures between 120 and 400 degrees F must receive two coats of 400 degrees F heat-resisting enamel applied to a total minimum thickness of 2 mils.

c. Temperatures Greater Than 400 Degrees F: Metal surfaces subject to temperatures greater than 400 degrees F must receive two coats of 600 degrees F heat-resisting paint applied to a total minimum dry film thickness of 2 mils.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 05 48.00 40

VIBRATION AND SEISMIC CONTROLS FOR HVAC PIPING AND EQUIPMENT

PART 1 GENERAL

1.1 REFERENCES
1.2 ADMINISTRATIVE REQUIREMENTS
1.3 SUBMITTALS
1.4 QUALITY CONTROL

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION
2.1.1 Design Requirements
2.1.1.1 Mountings
2.1.1.2 Bases
2.2 EQUIPMENT
2.2.1 Air-Cooled Condensing Unit Locations
2.2.2 Air-Moving Device Locations
2.2.3 Pipe And Duct Vibration Isolation
2.2.3.1 Floor-Mounted Piping
2.2.3.2 Vertical Piping
2.3 MATERIALS
2.4 TESTS, INSPECTIONS, AND VERIFICATIONS

PART 3 EXECUTION

3.1 INSTALLATION
3.2 FIELD QUALITY CONTROL
3.2.1 Tests and Reports

-- End of Section Table of Contents --

SECTION 23 05 48.00 40

VIBRATION AND SEISMIC CONTROLS FOR HVAC PIPING AND EQUIPMENT

PART 1 GENERAL

Section 23 31 13.00 40 METAL DUCTS applies to work specified in this section to the extent applicable.

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ACOUSTICAL SOCIETY OF AMERICA (ASA)

ASA S2.71	(1983; R 2006) Guide to the Evaluation of Human Exposure to Vibration in Buildings

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS (ASHRAE)

ASHRAE HVAC APP IP HDBK	(2016) HVAC Applications Handbook, I-P Edition

NATIONAL ENVIRONMENTAL BALANCING BUREAU (NEBB)

NEBB MASV	(2006) Procedural Standards for Measurements and Assessment of Sound and Vibration

1.2 ADMINISTRATIVE REQUIREMENTS

Within ten working days of Contract Award, submit equipment and performance data for vibration isolator systems including equipment base design; inertia-block mass relative to support equipment weight; spring loads and free, operating, and solid heights of spring; spring diameters; nonmetallic isolator loading and deflection; disturbing frequency; natural frequency of mounts; deflection of working member; and anticipated amount of physical movement at the reference points.

Ensure the data includes information on the following:

a. Mountings

b. Bases

c. Isolators

d. Floor-Mounted Piping

e. Vertical Piping

Five working days prior to commencement of installation, submit installation drawings for vibration isolator systems including equipment

and performance requirements.

Indicate within outline drawings for vibration isolator systems, overall physical features, dimensions, ratings, service requirements, and weights of equipment.

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Installation Drawings

Outline Drawings

SD-03 Product Data

Equipment and Performance Data

Isolators

SD-06 Test Reports

Type of Isolator

Type of Base

Allowable Deflection

Measured Deflection

1.4 QUALITY CONTROL

Ensure all vibration-control apparatus is the product of a single manufacturing source, where possible. Human exposure levels should be considered using ASA S2.71 and NEBB MASV.

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION

Scheduled isolation mounting is in inches and is a minimum static deflection.

Spans referred to in paragraph EQUIPMENT, means longest bay dimension.

Determine exact mounting sizes and number of isolators by the isolator manufacturer based on equipment that will be installed. Check equipment revolutions per minute (rpm) and spring deflections to verify that resonance cannot occur.

2.1.1 Design Requirements

Design for vibration isolation using ASHRAE HVAC APP IP HDBK, Chapter 48, as applicable to the following sections.

2.1.1.1 Mountings

Provide the following mountings:

Type A: Composite pad, with 0.25-inch thick elastomer top and bottom layers, molded to contain a pattern with nonslip characteristics in all horizontal directions. Elastomer loading is not to exceed 40 pounds per square inch (psi). Ensure minimum overall thickness is 1 inch. Maximum deflections up to 0.25-inch are allowed.

Type B: Double rubber-in-shear with molded-in steel reinforcement in top and bottom. Maximum deflections up to 0.50-inch are allowed.

Type C: Free-standing laterally stable open-spring type for deflections over 0.50-inch, with built-in bearing and leveling provisions, 0.25-inch thick Type A base elastomer pads, and accessories. Ensure outside diameter of each spring is equal to or greater than 0.9 times the operating height of the spring under rated load.

Type D: Partially housed type, containing one or more vertically restrained springs with at least 0.50-inch clearance maintained around springs, with adjustable limit stops, 0.25-inch thick Type A base elastomer pads, and accessories.

Type E: Pendulum-suspension configuration with free-standing stable spring with resilient horizontal and vertical restraints to allow maximum movements of 0.25-inch in each direction, 0.25-inch thick Type A base elastomer pads.

Type F: Combination spring and rubber-in-shear steel framed for hanger-rod mounting, with minimum total static deflection of 1-inch.

2.1.1.2 Bases

Provide the following bases:

Type U: Unit isolators without rails, structural-steel bases, or inertia blocks.

Type R: Rails, connected mill-rolled structural steel, of sufficient dimension to preclude deflection at midpoint of unsupported span in excess of 1/1,440th of the span between isolators, power transmission, component misalignment, and any overhung weight. Where Type R bases are specified and the equipment proposed requires additional base support, use a Type S base.

Type S: Structural-steel bases common to a supported assembly, made from welded-joint mill-rolled structural steel with closed-perimeter configuration, isolators attached to outrigger supports.

Ensure height of steel members is sufficient to provide stiffness required to maintain equipment manufacturer's recommended alignment and duty efficiency of power-transmission components. Ensure height

of steel member does not result in member deflection at midpoint of unsupported span of more than 1/1,440th of the span between isolators. Minimum height is 5-inches.

Type CIB: Provide concrete inertia blocks common to the entire assembly, with welded-joint construction, mill-rolled structural-steel perimeters, welded-in No. 4 reinforcing bars 8-inches on center each way near the bottom of the block, outrigger-isolator mounting provisions, anchor bolts. Fill with 3,000 psi cured-strength concrete.

Configure rectangular inertia bases to accommodate equipment supported.

Ensure minimum thickness of inertia base, in addition to providing suitable mass, is sufficient to provide stiffness to maintain equipment manufacturer's recommended alignment and duty efficiency of power-transmission components, and is sufficient to result in base deflection at midpoint of unsupported span of not more than 1/1,440th of the span between isolators. Verify minimum thickness, the preceding requirements notwithstanding, is 8 percent of the longest base dimension.

Ensure pumps with flexible couplings do not have inertia base less than 8-inches thick, and the minimum mass of concrete inertia block is equal in weight to supported equipment.

2.2 EQUIPMENT

Vibration isolation design per ASHRAE HVAC APP IP HDBK, Chapter 37.

2.2.1 Air-Cooled Condensing Unit Locations

TYPE EQUIPMENT	20-FOOT ROOF-SPAN PROVISIONS*	30-FOOT ROOF-SPAN PROVISIONS*	40-FOOT ROOF-SPAN PROVISIONS*
Through 5 hp over 900 rpm	B-U-0.5	D-U-1.0	D-U-1.75
Over 5 hp to 500 rpm	B-U-0.5	D-U-1.75	D-U-2.5
500 rpm and over	B-U-0.5	D-U-1.0	D-U-1.75
*TYPE OF MOUNTING, BASE, AND MINIMUM DEFLECTION IN INCHES			

2.2.2 Air-Moving Device Locations

Vibration-isolation provisions apply to housed free-standing fans of any pressure rating, located in field-erected factory- fabricated central-station units .

TYPE EQUIPMENT	BASEMENT BELOW-GRADE PROVISIONS*	ON/ABOVE GRADE 20-FOOT FLOOR-SPAN PROVISIONS*	ON/ABOVE GRADE 30-FOOT FLOOR-SPAN PROVISIONS*	ON/ABOVE GRADE 40-FOOT FLOOR-SPAN PROVISIONS*
Through 20 hp 250 to 300 rpm	B-U-0.35	C-S-2.5	C-S-2.5	C-S-3.5

TYPE EQUIPMENT	BASEMENT BELOW-GRADE PROVISIONS*	ON/ABOVE GRADE 20-FOOT FLOOR-SPAN PROVISIONS*	ON/ABOVE GRADE 30-FOOT FLOOR-SPAN PROVISIONS*	ON/ABOVE GRADE 40-FOOT FLOOR-SPAN PROVISIONS*
300 to 500 rpm	B-U-0.35	C-S-1.75	C-S-1.75	C-S-2.5
500 rpm and over	B-U-0.35	C-S-1.0	C-S-1.5	C-S-1.75
Over 20 hp 250 to 300 rpm	B-U-0.35	C-S-2.75	C-CIB-3.5	C-CIB-5.0
300 to 500 rpm	B-U-0.35	C-S-1.75	C-CIB-2.5	C-CIB-3.5
500 rpm and over	B-U-0.35	C-S-1.0	C-CIB-1.75	C-CIB-2.5
*TYPE OF MOUNTING, BASE, AND MINIMUM DEFLECTION IN INCHES				

2.2.3 Pipe And Duct Vibration Isolation

Type G: Provide isolators with in-series contained steel springs and preformed fibrous-glass or chloroprene-elastomer elements for connecting to building-structure attachments. Load devices by supported system during operating conditions to produce a minimum spring and elastomer static deflection of 1-inch and 3/8-inch, respectively.

Type H: Provide isolators with contained chloroprene-elastomer elements for connecting to building-structure attachments. Load devices by supported system during operating conditions to produce a minimum elastomer static deflection of 3/8-inch.

Type J: Provide isolators with elastomers mounted on floor-supported columns or directly on the floor. Load devices by supported system during operating conditions to produce a minimum elastomer static deflection of 3/8-inch.

2.2.3.1 Floor-Mounted Piping

Type K: Provide isolators with springs mounted on floor-supported columns or directly on the floor. Load devices by supported system during operating conditions to produce a minimum spring static deflection of 1-inch.

2.2.3.2 Vertical Piping

Type L: Provide isolators which are pipe base-support devices with one or more contained steel springs. Load devices by supported system during operating conditions to produce a minimum static deflection of 1-inch. Equip devices with precompression and vertical-limit features, as well as a minimum 1/4-inch thick elastomer sound pad and isolation washers, for mounting to floor.

Type M: Provide isolators which are elastomer mounted baseplate and riser pipe-guide devices, with contained double acting elastomer elements which under rated load have a minimum static deflection of 3/8-inch. Size isolator to accommodate thermal insulation within the stationary guide ring.

2.3 MATERIALS

Ensure rubber is natural rubber and elastomer is chloroprene. Shore A durometer measurement of both materials and range between 40 and 60.

Inorganic materials such as precompressed, high-density, fibrous glass encased in a resilient moisture-impervious membrane may be used in lieu of specified natural rubber and elastomers. Where this substitution is made, ensure specified deflections are modified by the manufacturing source to accommodate physical characteristics of inorganic materials and to provide equal or better vibration isolation.

Ensure weather-exposed metal vibration-isolator parts are corrosion protected. Chloroprene coat springs.

2.4 TESTS, INSPECTIONS, AND VERIFICATIONS

Submit test reports for testing vibration isolation for each type of isolator and each type of base. Meet referenced standards contained within this section. Include in test reports allowable deflection and measured deflection also meeting referenced standards within this section.

PART 3 EXECUTION

3.1 INSTALLATION

Install equipment in accordance with manufacturer's recommendations.

Ensure rails, structural steel bases, and concrete inertia blocks are raised not less than 1-inch above the floor and are level when equipment supported is under operating load.

Ensure vibration-isolation installation and deflection testing after equipment start-up is directed by a competent representative of the manufacturer.

3.2 FIELD QUALITY CONTROL

3.2.1 Tests and Reports

Ensure vibration-isolation devices are deflection tested. Submit test reports substantiating that all equipment has been isolated as specified and that minimum specified deflections have been met. Make all measurements in the presence of the Contracting Officer.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 05 48.19

SEISMIC BRACING FOR HVAC

PART 1 GENERAL

1.1 REFERENCES
1.2 SYSTEM DESCRIPTION
1.2.1 General Requirements
1.2.2 Mechanical Equipment
1.2.3 Mechanical Systems
1.2.4 Contractor Designed Bracing
1.2.5 Items Not Covered By This Section
1.2.5.1 Fire Protection Systems
1.2.5.2 Items Requiring No Seismic Restraints
1.3 SUBMITTALS

PART 2 PRODUCTS

2.1 GENERAL DESIGN REQUIREMENTS
2.2 PERFORMANCE REQUIREMENTS
2.2.1 Wind-Restraint Loading
2.2.2 Seismic Load
2.3 EQUIPMENT RESTRAINT
2.3.1 Rigidly (Base and Suspended) Mounted Equipment
2.3.2 Nonrigid or Flexibly-Mounted Equipment
2.4 BOLTS AND NUTS
2.5 SWAY BRACING MATERIALS
2.6 MULTIDIRECTIONAL SEISMIC SNUBBERS

PART 3 EXECUTION

3.1 COUPLING AND BRACING
3.2 BUILDING DRIFT
3.3 FLEXIBLE COUPLINGS OR JOINTS
3.3.1 Building Piping
3.4 PIPE SLEEVES
3.5 SPREADERS
3.6 SWAY BRACES FOR PIPING
3.6.1 Transverse Sway Bracing
3.6.2 Longitudinal Sway Bracing
3.6.3 Vertical Runs
3.6.4 Clamps and Hangers
3.7 SWAY BRACES FOR DUCTS
3.7.1 Braced Ducts
3.7.2 Unbraced Ducts
3.8 EQUIPMENT
3.8.1 General
3.8.2 Controls
3.9 ANCHOR BOLTS

3.9.1 Cast-in-Place Anchor Bolts
3.9.2 Drilled-In Anchor Bolts
3.9.2.1 Wedge Anchors, Heavy-Duty Sleeve Anchors, and Undercut Anchors
3.9.2.2 Cartridge Injection Adhesive Anchors
3.9.2.3 Capsule Anchors
3.10 ANCHOR BOLT TESTING
3.10.1 Torque Wrench Testing

-- End of Section Table of Contents --

SECTION 23 05 48.19

SEISMIC BRACING FOR HVAC

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN CONCRETE INSTITUTE (ACI)

ACI 355.2	(2007) Qualification of Post-Installed Mechanical Anchors in Concrete and Commentary
ACI 355.4	(2011) Qualification of Post-Installed Adhesive Anchors in Concrete (ACI 355.4) and Commentary

AMERICAN INSTITUTE OF STEEL CONSTRUCTION (AISC)

AISC 325	(2017) Steel Construction Manual

AMERICAN SOCIETY OF CIVIL ENGINEERS (ASCE)

ASCE 7-16	(2017; Errata 2018; Supp 1 2018) Minimum Design Loads and Associated Criteria for Buildings and Other Structures

ASTM INTERNATIONAL (ASTM)

ASTM A36/A36M	(2019) Standard Specification for Carbon Structural Steel
ASTM A53/A53M	(2022) Standard Specification for Pipe, Steel, Black and Hot-Dipped, Zinc-Coated, Welded and Seamless
ASTM A153/A153M	(2016a) Standard Specification for Zinc Coating (Hot-Dip) on Iron and Steel Hardware
ASTM A325	(2014) Standard Specification for Structural Bolts, Steel, Heat Treated, 120/105 ksi Minimum Tensile Strength
ASTM A490	(2014a) Standard Specification for Structural Bolts, Alloy Steel, Heat Treated, 150 ksi Minimum Tensile Strength
ASTM A500/A500M	(2021a) Standard Specification for Cold-Formed Welded and Seamless Carbon Steel Structural Tubing in Rounds and

	Shapes
ASTM A563	(2015) Standard Specification for Carbon and Alloy Steel Nuts
ASTM A603	(2019) Standard Specification for Zinc-Coated Steel Structural Wire Rope
ASTM F1554	(2020) Standard Specification for Anchor Bolts, Steel, 36, 55, and 105-ksi Yield Strength

FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

FEMA P-414	(January 2004) Installing Seismic Restraints for Duct and Pipe

METAL FRAMING MANUFACTURERS ASSOCIATION (MFMA)

MFMA-4	(2004) Metal Framing Standards Publication

SHEET METAL AND AIR CONDITIONING CONTRACTORS' NATIONAL ASSOCIATION (SMACNA)

SMACNA 1981	(2008) Seismic Restraint Manual Guidelines for Mechanical Systems, 3rd Edition

U.S. DEPARTMENT OF DEFENSE (DOD)

UFC 3-301-01	(2019, with Change 1, 2022) Structural Engineering
UFC 4-010-01	(2018; with Change 1, 2020; Change 2, 2022) DoD Minimum Antiterrorism Standards for Buildings

VIBRATION ISOLATION AND SEISMIC CONTROL MANUFACTURERS ASSOCIATION (VISCMA)

VISCMA 412	(2014) Installing Seismic Restraints for Mechanical Equipment

1.2 SYSTEM DESCRIPTION

1.2.1 General Requirements

Apply the requirements for seismic protection measures described in this section and on the drawings to the mechanical equipment and mechanical systems both inside and outside of the building along with exterior utilities and systems listed below. Where there is a conflict between the specifications and the drawings, the specifications will take precedence. Accomplish resistance to lateral forces induced by earthquakes without consideration of friction resulting from gravity loads.

1.2.2 Mechanical Equipment

Mechanical equipment to be seismically protected must include the following items to the extent required on the drawings or in other sections of these specifications:

Equipment/Components with Ip = 1.5

Water Heaters	
Air Terminal Units	Unitary HVAC Systems

Equipment/Components with Ip = 1.5 (Designated Seismic Systems)
Insert edited list here similar to one above for Ip = 1.0

1.2.3 Mechanical Systems

Mechanical systems to be seismically protected must include the following items to the extent required on the drawings or in this or other sections of these specifications:

Mechanical systems with Ip = 1.5

a. All Piping and Ducts Inside the Building Except as Specifically Stated Below Under "Items Not Covered By This Section".

b. All Process Piping Outside of Buildings.

c. Ductwork Outside of Buildings.

1.2.4 Contractor Designed Bracing

Submit copies of the design calculations with the drawings. Calculations must be approved, certified, stamped and signed by a registered Professional Structural Engineer. Calculations must verify the capability of structural members to which bracing is attached for carrying the load from the brace. Design the bracing in accordance with UFC 3-301-01, , UFC 4-010-01 and additional data furnished by the Contracting Officer. Resistance to lateral forces induced by earthquakes must be accomplished without consideration of friction resulting from gravity loads. UFC 3-301-01 uses parameters for the building, not for the equipment in the building; therefore, corresponding adjustments to the formulas must be required. Loadings determined using UFC 3-301-01 are based on strength design; therefore, AISC 325 Specifications must be used for the design. The bracing for the mechanical equipment designated in paragraph 1.2.2 and systems designated in paragraph 1.2.3 must be developed by the Contractor.

1.2.5 Items Not Covered By This Section

1.2.5.1 Fire Protection Systems

Install seismic protection of piping for fire protection systems as specified in Section 21 13 13 WET PIPE SPRINKLER SYSTEMS.

1.2.5.2 Items Requiring No Seismic Restraints

Seismic restraints are not required for the following items:

a. Gas piping less than 1 inch nominal pipe size.

b. Piping in boiler and mechanical equipment rooms less than 1-1/4 inches

nominal pipe size.

c. All other piping equal to or less than 3 inches nominal pipe size.

d. Rectangular air handling ducts less than 6 square feet in cross sectional area.

e. Round air handling ducts less than 28 inches in diameter.

f. Piping suspended by individual hangers 12 inches or less in length from the top of pipe to the bottom of the supporting structural member where the hanger is attached, except as noted below.

g. Ducts suspended by hangers 12 inches or less in length from the top of the duct to the bottom of the supporting structural member, except as noted below.

In exemptions f. and g. all hangers must meet the length requirements. If the length requirement is exceeded by one hanger in the run, brace the entire run. Seismically protect interior piping and ducts not listed above in accordance with the provisions of this specification.

Non-critical items may require seismic restraints if adjacent to critical equipment or systems that must remain operational after an earthquake and could be compromised by impact with non-critical adjacent components.

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Coupling and Bracing

Flexible Couplings or Joints

Equipment Restraint

Contractor Designed Bracing; G

SD-03 Product Data

Coupling and Bracing; G

Flexible Couplings Or Joints; G

Equipment Restraint; G

Contractor Designed Bracing; G

Snubbers

Anchor Bolts

Vibration Isolators

SD-05 Design Data

Design Calculations

SD-06 Test Reports

Anchor Bolts; G

PART 2 PRODUCTS

2.1 GENERAL DESIGN REQUIREMENTS

Submit detailed seismic restraint drawings for mechanical equipment, duct systems, piping systems and any other mechanical systems along with calculations, catalog cuts, templates, and erection and installation details, as appropriate, for the items listed below. Indicate thickness, type, grade, class of metal, and dimensions; and show construction details, reinforcement, anchorage, and installation with relation to the building construction. Calculations must be stamped, by a registered structural engineer, and verify the capability of structural members to which bracing is attached for carrying the load from the brace. Include drawing for Mission Critical Equipment indicating the equipment location in the facility sufficient to be used for the installation. Design must be based on actual equipment and system layout. Design must include calculated dead loads, static seismic loads and capacity of materials utilized for the connection of the equipment or system to the structure. Analysis must detail anchoring methods.

2.2 PERFORMANCE REQUIREMENTS

2.2.1 Wind-Restraint Loading

1. Ultimate Design Wind Speed = 124 miles per hour(mph).
2. Serviceability Design Wind Speed (10-Year Wind Speed) = 73 mph.
3. Risk Category IV.
4. Exposure Category C.

2.2.2 Seismic Load

1. Site Class D.
2. Risk Category IV.
3. Seismic Design Category C.

2.3 EQUIPMENT RESTRAINT

Equipment must be rigidly or flexibly mounted as indicated in the specifications and/or drawings depending on vibration isolation requirements as follows below.

Roof mounted equipment such as cooling towers and condensers, both vibration isolated and nonisolated, must have support members designed and anchored to building structural steel or concrete as required for seismic restraint and wind loads.

2.3.1 Rigidly (Base and Suspended) Mounted Equipment

HVAC equipment furnished under this contract must be rigidly mounted using

cast-in-place anchor bolts or post-installed anchors that are qualified for earthquake loading in accordance with ACI 355.2 and ACI 355.4. Anchor bolts must conform to ASTM F1554. For any rigid equipment which is rigidly anchored, provide flexible joints for piping, ductwork, electrical conduit, etc., that are capable of accommodating displacements equal to the full width of the joint in both orthogonal directions. Suspended equipment bracing attachments should be located just above the center of gravity to minimize swinging. Use the ratio of the overturning moment from seismic forces to the resisting moment due to gravity loads to determine if overturning forces need to be considered in the sizing of anchor bolts. Provide calculations to verify the adequacy of the anchor bolts for combined shear and overturning.

Roof mounted HVAC equipment roof curbs, framing and attachment to equipment and structure must be designed and braced to withstand seismic loads. Designated Seismic Systems (DSS) assigned to Seismic Design Category (SDC) C, D, E, or F and Risk Category IV components needed for continued operation after an earthquake must have two nuts provided on each anchor bolt.

2.3.2 Nonrigid or Flexibly-Mounted Equipment

Select vibration isolation devices so that the maximum movement of equipment from the static deflection point is 1/4 inch. Equipment flexibly mounted on vibration isolators must have a bumper restraint or snubber in each horizontal direction and vertical restraints must be provided where required to resist overturning. Isolator housing and restraints must be constructed of ductile materials. A viscoelastic pad or similar material of appropriate thickness must be used between the bumper and components to limit the impact load. Restraints must be designed to resist the calculated horizontal lateral and vertical forces.

Spring vibration isolators must be seismically rated, restrained isolators for equipment subject to load variations and large external forces. The seismically rated housing must be sized to meet or exceed the force requirements applicable to the project and meet the required isolation criteria. Spring vibration isolator manufacturer's will be a member of VISCMA. Design force, Fp, must be doubled for vibration isolators with an air gap greater than 0.25 inches as specified in ASCE 7-16, Chapter 13. Housed springs must not be used for seismic restraint applications because they cannot resist uplift.

2.4 BOLTS AND NUTS

Hex head bolts, and heavy hexagon nuts must be ASTM A325 or ASTM A490 bolts and ASTM A563 nuts. Provide bolts and nuts galvanized in accordance with ASTM A153/A153M when used underground or exposed to weather.

2.5 SWAY BRACING MATERIALS

Material used for members listed in this section and on the drawings, must be structural steel conforming with the following:

a. Plates, rods, and rolled shapes, ASTM A36/A36M.

b. Wire rope, ASTM A603 pre-stretched. Class B galv coating Ferrule clamps must be qualified by testing for use in seismic applications per VISCMA 412. A minimum of two clamps are required on each end of wire rope.

c. Tubes, ASTM A500/A500M, Grade B.

d. Pipes, ASTM A53/A53M, Grade B.

e. Angles, ASTM A36/A36M.

f. Channels (Struts) with in-turned lips and associated hardware for fastening to channels at random points conforming to MFMA-4

2.6 MULTIDIRECTIONAL SEISMIC SNUBBERS

Install multidirectional seismic snubbers employing elastomeric pads on floor- or slab-mounted equipment and as detailed on drawings. These snubbers must provide 1/4 inch free vertical and horizontal movement from the static deflection point. Snubber medium must consist of multiple pads of cotton duct and neoprene or other suitable materials arranged around a flanged steel trunnion so both horizontal and vertical forces are resisted by the snubber medium.

PART 3 EXECUTION

3.1 COUPLING AND BRACING

a. Submit detail drawings, as specified here and throughout this specification, along with catalog cuts, templates, and erection and installation details, as appropriate, for the items listed. Submittals must be complete in detail; must indicate thickness, type, grade, class of metal, and dimensions; and must show construction details, reinforcement, anchorage, and installation with relation to the building construction.

b. Provide coupling installation conforming to the details shown on the drawings. Provisions of this paragraph apply to all piping within a 5 foot line around outside of building unless buried in the ground. Piping grouped for support on trapeze-type hangers must be braced at the most frequent interval as determined by applying the requirements of this specification to each piping run on the common support.

c. Size bracing components as required for the total load carried by the common supports. Bracing rigidly attached to pipe flanges, or similar, must not be used where it would interfere with thermal expansion of piping.

d. Adjust isolators and restraints after piping systems has been filled and equipment is at its operating weight, following the manufacturer's written instructions.

e. Install cables at a 45-degree slope. Where interference is present, the slope may be minimum of 30 degrees or a maximum of 60 degrees per VISCMA 412.

3.2 BUILDING DRIFT

Provide joints capable of accommodating seismic displacements for vertical piping between floors of the building, where pipes pass through a building seismic or expansion joint, or where rigidly supported pipes connect to equipment with vibration isolators. Provide horizontal piping across expansion joints to accommodate the resultant of the drifts of each

building unit in each orthogonal direction. For threaded piping, provide swing joints made of the same piping material. For piping with manufactured ball joints the seismic drift must be 0.015 feet per foot of height above the base where the seismic separation occurs; this drift value must be used in place of the expansion given in the manufacturer's selection table.

3.3 FLEXIBLE COUPLINGS OR JOINTS

3.3.1 Building Piping

Provide flexible couplings or joints in building piping at bottom of all pipe risers for pipe larger than 3-1/2 inches in diameter. Laterally brace flexible couplings or joints without interfering with the action of the flexible coupling or joint. Cast iron waste and vent piping need only comply with these provisions when caulked joints are used. Flexible bell and spigot pipe joints using rubber gaskets may be used at each branch adjacent to tees and elbows for underground waste piping inside of building to satisfy these requirements.

3.4 PIPE SLEEVES

Size pipe sleeves in interior non-fire rated walls as indicated on the drawings to provide clearances that will permit differential movement of piping without the piping striking the pipe sleeve. Pipe sleeves in fire rated walls must conform to the requirements in Section 07 84 00 FIRESTOPPING.

3.5 SPREADERS

Provide spreaders between adjacent piping runs to prevent contact during seismic activity whenever pipe or insulated pipe surfaces are less than 4 inches apart. Apply spreaders at same interval as sway braces at an equal distance between the sway braces. If rack type hangers are used where the pipes are restrained from contact by mounting to the rack, spreaders are not required for pipes mounted in the rack. Apply spreaders to surface of bare pipe and over insulation on insulated pipes utilizing high-density inserts and pipe protection shields in accordance with the requirements of Section 23 07 00 THERMAL INSULATION FOR MECHANICAL SYSTEMS.

3.6 SWAY BRACES FOR PIPING

Provide sway braces to prevent movement of the pipes under seismic loading. Provide braces in both the longitudinal and transverse directions, relative to the axis of the pipe. Provide sufficient braces for equipment to resist a horizontal force as specified in UFC 3-301-01 without exceeding safe working stress of bracing components. Provide bracing that does not interfere with thermal expansion requirements for the pipes as described in other sections of these specifications. For seismic analysis of horizontal pipes, the equivalent static force should be considered to act concurrently with the full dead load of the pipe, including contents.

3.6.1 Transverse Sway Bracing

Provide transverse sway bracing for steel and copper pipe at intervals not to exceed those shown on the drawings. All runs (length of pipe between end joints) must have a minimum of transverse bracing at each end. Provide transverse sway bracing for pipes of materials other than steel

and copper at intervals not to exceed the hanger spacing as specified in Section 22 00 00 PLUMBING, GENERAL PURPOSE.

3.6.2 Longitudinal Sway Bracing

Provide longitudinal sway bracing at 40 foot intervals unless otherwise indicated. All runs (length of pipe between end joints) must have one longitudinal brace minimum. Construct sway braces in accordance with the drawings. Do not use branch lines, walls, or floors as sway braces.

3.6.3 Vertical Runs

Run is defined as length of pipe between end joints. Do not brace vertical runs of piping no more than 10 foot vertical intervals. Braces for vertical runs must be above the center of gravity of the segment being braced. Flexible couplings should be provided at the bottoms of risers for pipes larger than 3.5 in. (89 mm) in diameter. Flexible couplings and expansion joints should be braced laterally and longitudinally unless such bracing would interfere with the action of the couplings or joints. When pipes enter buildings, flexible couplings should be provided to allow for relative movement between the soil and building. Construct all sway braces in accordance with the drawings. Attach sway braces to the structural system. Do not connect to branch lines, walls, or floors.

3.6.4 Clamps and Hangers

Apply clamps or hangers on uninsulated pipes directly to pipe. Insulated piping must have clamps or hangers applied over insulation in accordance with Section 23 07 00 THERMAL INSULATION FOR MECHANICAL SYSTEMS.

Hanger rod stiffener angle or strut bracing must be securely attached by a series of attachment clamps manufactured from a one piece metal stamping and must include all require attachment hardware and locking nuts. Attachment clamps made from aluminum or cast iron must not be used in seismic applications. Do not weld vertical braces to hanger rods.

3.7 SWAY BRACES FOR DUCTS

3.7.1 Braced Ducts

Provide bracing details and spacing for rectangular and round ducts in accordance with SMACNA 1981. However, the design seismic loadings for these items must not be less than loadings obtained using the procedures in UFC 3-301-01. Bracing must not attach to duct joints. Use shortest screws possible when penetrating ductwork to minimize airflow noise inside duct.

3.7.2 Unbraced Ducts

Attach hangers for unbraced ducts to the duct within 2 inches of the top of the duct with a minimum of two #10 sheet metal screws in accordance with FEMA P-414. Use shortest screws possible when penetrating ductwork to minimize airflow noise inside duct. Install unbraced ducts with a 6 inch minimum clearance to vertical ceiling hanger wires.

3.8 EQUIPMENT

3.8.1 General

Ensure housekeeping pads have adequate space to mount equipment and seismic restraint devices allowing adequate edge distance and embedment depth for restraint anchor bolts. Identify position of reinforcing steel and other embedded items prior to drilling holes for anchors. Do not drill holes in concrete or masonry until concrete, mortar, or grout has achieved full design strength. Install neoprene grommet washers or till the gap with epoxy on equipment anchor bolts where clearance between anchor and equipment support hole exceeds 0.125 inches.

3.8.2 Controls

Ensure that controls for critical equipment that must remain operational after an earthquake are certified per paragraph 3.11 SPECIAL TESTING FOR SEISMIC-RESISTING EQUIPMENT and are served by emergency power as required.

3.9 ANCHOR BOLTS

3.9.1 Cast-in-Place Anchor Bolts

Use templates to locate cast-in-place bolts accurately and securely in formwork. Anchor bolts must have an embedded straight length equal to at least 12 times nominal diameter of the bolt. Anchor bolts that exceed the normal depth of equipment foundation piers or pads must either extend into concrete floor or the foundation or be increased in depth to accommodate bolt lengths.

3.9.2 Drilled-In Anchor Bolts

Drill holes with rotary impact hammer drills Drill bits must be of diameters as specified by the anchor manufacturer. Unless otherwise shown on the Drawings, all holes must be drilled perpendicular to the concrete surface. Where anchors are permitted to be installed in cored holes, use core bits with matched tolerances as specified by the manufacturer. Properly clean cored hole per manufacturer's instructions. Identify position of reinforcing steel and other embedded items prior to drilling holes for anchors. Exercise care in coring or drilling to avoid damaging existing reinforcing or embedded items. Notify the COR if reinforcing steel or other embedded items are encountered during drilling. Take precautions as necessary to avoid damaging prestressing tendons, electrical and telecommunications conduit, and gas lines. Unless otherwise specified, do not drill holes in concrete or masonry until concrete, mortar, or grout has achieved full design strength. Perform anchor installation in accordance with manufacturer instructions.

3.9.2.1 Wedge Anchors, Heavy-Duty Sleeve Anchors, and Undercut Anchors

Protect threads from damage during anchor installation. Heavy-duty sleeve anchors must be installed with sleeve fully engaged in part to be fastened. Set anchors to manufacturer's recommended torque, using a torque wrench. Following attainment of 10% of the specified torque, 100% of the specified torque must be reached within 7 or fewer complete turns of the nut. If the specified torque is not achieved within the required number of turns, the anchor must be removed and replaced unless otherwise directed by the Engineer.

3.9.2.2 Cartridge Injection Adhesive Anchors

Where approved for seismic application, clean all holes per manufacturer instructions to remove loose material and drilling dust prior to installation of adhesive. Inject adhesive into holes proceeding from the bottom of the hole and progressing toward the surface in such a manner as to avoid introduction of air pockets in the adhesive. Follow manufacturer recommendations to ensure proper mixing of adhesive components. Sufficient adhesive must be injected in the hole to ensure that the annular gap is filled to the surface. Remove excess adhesive from the surface. Shim anchors with suitable device to center the anchor in the hole. Do not disturb or load anchors before manufacturer specified cure time has elapsed.

3.9.2.3 Capsule Anchors

Where approved for seismic application, perform drilling and setting operations in accordance with manufacturer instructions. Clean all holes to remove loose material and drilling dust prior to installation of adhesive. Remove water from drilled holes in such a manner as to achieve a surface dry condition. Capsule anchors must be installed with equipment conforming to manufacturer recommendations. Do not disturb or load anchors before manufacturer specified cure time has elapsed.

Observe manufacturer recommendations with respect to installation temperatures for cartridge injection adhesive anchors and capsule anchors.

3.10 ANCHOR BOLT TESTING

Test in place expansion and chemically bonded anchors not more than 24 hours after installation of the anchor, conducted by an independent testing agency; testing must be performed on random anchor bolts as described below.

3.10.1 Torque Wrench Testing

Perform torque wrench testing on not less than 50 percent of the total installed applied torque expansion anchors and at least one anchor for every piece of equipment containing more than two anchors. The test torque must equal the minimum required installation torque as required by the bolt manufacturer. Calibrate torque wrenches at the beginning of each day the torque tests are performed. Recalibrate torque wrenches for each bolt diameter whenever tests are run on bolts of various diameters. Apply torque between 20 and 100 percent of wrench capacity. Reach the test torque within one half turn of the nut, except for 3/8 inch sleeve anchors which must reach their torque by one quarter turn of the nut. If any anchor fails the test, test similar anchors not previously tested until 20 consecutive anchors pass. Failed anchors must be retightened and retested to the specified torque; if the anchor still fails the test it must be replaced.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 05 93

TESTING, ADJUSTING, AND BALANCING FOR HVAC

PART 1 GENERAL

1.1 REFERENCES
1.2 DEFINITIONS
1.2.1 Similar Terms
1.3 WORK DESCRIPTION
1.3.1 Air Distribution Systems
1.3.2 Water Distribution Systems
1.3.3 TAB SCHEMATIC DRAWINGS
1.4 SUBMITTALS
1.5 QUALITY ASSURANCE
1.5.1 Independent TAB Agency and Personnel Qualifications

PART 2 PRODUCTS

PART 3 EXECUTION

3.1 WORK DESCRIPTIONS OF PARTICIPANTS
3.2 PRE-DALT/TAB MEETING
3.3 DALT PROCEDURES
3.3.1 Instruments, Consumables and Personnel
3.3.2
3.3.3 Ductwork To Be DALT'd
3.3.4 DALT Testing
3.3.5 Completed Pre-Final DALT Report
3.3.6 Quality Assurance - COTR DALT Field Acceptance Testing
3.3.7 Additional COTR Field Acceptance Testing
3.3.8 Certified Final DALT Report
3.3.9 Prerequisite for TAB Field Work
3.4 TAB PROCEDURES
3.4.1 TAB Field Work
3.4.2 Preliminary Procedures
3.4.3 TAB Air Distribution Systems
3.4.3.1 Units With Coils
3.4.3.2 Rooftop Air Conditioning
3.4.3.3 Exhaust Fans
3.4.4 TAB Work on Performance Tests Without Seasonal Limitations
3.4.4.1 Performance Tests
3.4.4.2 Ambient Temperatures
3.4.4.3 Sound Measurements
3.4.5 Workmanship
3.4.6 Deficiencies
3.4.7 TAB Reports
3.4.8 Quality Assurance - COTR TAB Field Acceptance Testing
3.4.8.1 TAB Field Acceptance Testing

3.4.8.2 Additional COTR TAB Field Acceptance Testing
3.4.8.3 Prerequisite for Approval
3.5 MARKING OF SETTINGS
3.6 MARKING OF TEST PORTS

-- End of Section Table of Contents --

SECTION 23 05 93

TESTING, ADJUSTING, AND BALANCING FOR HVAC

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ASSOCIATED AIR BALANCE COUNCIL (AABC)

AABC MN-1	(2002; 6th ed) National Standards for Total System Balance
AABC MN-4	(1996) Test and Balance Procedures

NATIONAL ENVIRONMENTAL BALANCING BUREAU (NEBB)

NEBB MASV	(2006) Procedural Standards for Measurements and Assessment of Sound and Vibration
NEBB PROCEDURAL STANDARDS	(2015) Procedural Standards for TAB (Testing, Adjusting and Balancing) Environmental Systems

SHEET METAL AND AIR CONDITIONING CONTRACTORS' NATIONAL ASSOCIATION (SMACNA)

SMACNA 1780	(2002) HVAC Systems - Testing, Adjusting and Balancing, 3rd Edition
SMACNA 1858	(2004) HVAC Sound And Vibration Manual - First Edition
SMACNA 1972 CD	(2012) HVAC Air Duct Leakage Test Manual - 2nd Edition

1.2 DEFINITIONS

a. AABC: Associated Air Balance Council

b. COTR: Contracting Officer's Technical Representative

c. DALT: Duct air leakage test

d. DALT'd: Duct air leakage tested

e. HVAC: Heating, ventilating, and air conditioning; or heating, ventilating, and cooling

f. NEBB: National Environmental Balancing Bureau

g. Out-of-tolerance data: Pertains only to field acceptance testing of Final DALT or TAB report. When applied to DALT work, this phase means When applied to TAB work this phase means "a measurement taken during TAB field acceptance testing which does not fall within the range of plus 5 to minus 5 percent of the original measurement reported on the TAB Report for a specific parameter."

h. Season of maximum heating load: The time of year when the outdoor temperature at the project site remains within plus or minus 30 degrees Fahrenheit of the project site's winter outdoor design temperature, throughout the period of TAB data recording.

i. Season of maximum cooling load: The time of year when the outdoor temperature at the project site remains within plus or minus 5 degrees Fahrenheit of the project site's summer outdoor design temperature, throughout the period of TAB data recording.

j. Season 1, Season 2: Depending upon when the project HVAC is completed and ready for TAB, Season 1 is defined, thereby defining Season 2. Season 1 could be the season of maximum heating load, or the season of maximum cooling load.

k. Sound measurements terminology: Defined in AABC MN-1, NEBB MASV, or SMACNA 1858 (TABB).

l. TAB: Testing, adjusting, and balancing (of HVAC systems)

m. TAB'd: HVAC Testing/Adjusting/Balancing procedures performed

n. TAB Agency: TAB Firm
r. TABB: Testing Adjusting and Balancing Bureau

1.2.1 Similar Terms

In some instances, terminology differs between the Contract and the TAB Standard primarily because the intent of this Section is to use the industry standards specified, along with additional requirements listed herein to produce optimal results.

The following table of similar terms is provided for clarification only. Contract requirements take precedent over the corresponding AABC, NEBB, or TABB requirements where differences exist.

SIMILAR TERMS			
Contract Term	AABC Term	NEBB Term	TABB Term
TAB Standard	National Standards for Testing and Balancing Heating, Ventilating, and Air Conditioning Systems	Procedural Standards for Testing, Adjusting and Balancing of Environmental Systems	International Standards for Environmental Systems Balance
TAB Specialist	TAB Engineer	TAB Supervisor	TAB Supervisor

SIMILAR TERMS			
Contract Term	AABC Term	NEBB Term	TABB Term
Systems Readiness Check	Construction Phase Inspection	Field Readiness Check & Preliminary Field Procedures	Field Readiness Check & Prelim. Field Procedures

1.3 WORK DESCRIPTION

The work includes duct air leakage testing (DALT) and testing, adjusting, and balancing (TAB) of new heating, ventilating, and cooling (HVAC) air distribution systems including equipment and performance data, ducts, and piping which are located within, on, under, between, and adjacent to buildings.

Perform TAB in accordance with the requirements of the TAB procedural standard recommended by the TAB trade association that approved the TAB Firm's qualifications. Comply with requirements of AABC MN-1, NEBB PROCEDURAL STANDARDS, or SMACNA 1780 (TABB) as supplemented and modified by this specification section. All recommendations and suggested practices contained in the TAB procedural standards are considered mandatory.

Conduct DALT and TAB of the indicated existing systems and equipment and submit the specified DALT and TAB reports for approval. Conduct DALT testing in compliance with the requirements specified in SMACNA 1972 CD, except as supplemented and modified by this section. Conduct DALT and TAB work in accordance with the requirements of this section.

1.3.1 Air Distribution Systems

Test, adjust, and balance system (TAB) in compliance with this section. Obtain Contracting Officer's written approval before applying insulation to exterior of air distribution systems as specified under Section 23 07 00 THERMAL INSULATION FOR MECHANICAL SYSTEMS.

1.3.2 Water Distribution Systems

TAB system in compliance with this section. Obtain Contracting Officer's written approval before applying insulation to water distribution systems as specified under Section 23 07 00 THERMAL INSULATION FOR MECHANICAL SYSTEMS. At Contractor's option and with Contracting Officer's written approval, the piping systems may be insulated before systems are TAB'd.

Terminate piping insulation immediately adjacent to each flow control valve, automatic control valve, or device. Seal the ends of pipe insulation and the space between ends of pipe insulation and piping, with waterproof vapor barrier coating.

After completion of work under this section, insulate the flow control valves and devices as specified under Section 23 07 00 THERMAL INSULATION FOR MECHANICAL SYSTEMS.

1.3.3 TAB SCHEMATIC DRAWINGS

Show the following information on TAB Schematic Drawings:

1. A unique number or mark for each piece of equipment or terminal.

2. Air quantities at air terminals.

3. Air quantities and temperatures in air handling unit schedules.

4. Water quantities and temperatures in thermal energy transfer equipment schedules.

5. Water quantities and heads in pump schedules.

6. Water flow measurement fittings and balancing fittings.

7. Ductwork Construction and Leakage Testing Table that defines the DALT test requirements, including each applicable HVAC duct system ID or mark, duct pressure class, duct seal class, and duct leakage test pressure. This table is included in the file for Graphics for Unified Facilities Guide Specifications:

http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/forms-graphics-

Submit three copies of the TAB Schematic Drawings and Report Forms to the Contracting Officer, no later than 21 days prior to the start of TAB field measurements.

1.4 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

TAB Schematic Drawings and Report Forms

SD-03 Product Data

Equipment and Performance Data

SD-06 Test Reports

Completed Pre-Final DALT Report

Certified Final DALT Report

SD-07 Certificates

Independent TAB Agency and Personnel Qualifications

1.5 QUALITY ASSURANCE

1.5.1 Independent TAB Agency and Personnel Qualifications

To secure approval for the proposed agency, submit information certifying that the TAB agency is a first tier subcontractor who is not affiliated with any other company participating in work on this contract, including design, furnishing equipment, or construction. Further, submit the following, for the agency, to Contracting Officer for approval:

a. Independent AABC or NEBB or TABB TAB agency:

TAB agency: AABC registration number and expiration date of current certification; or NEBB certification number and expiration date of current certification; or TABB certification number and expiration date of current certification.

TAB team supervisor: Name and copy of AABC or NEBB or TABB TAB supervisor certificate and expiration date of current certification.

TAB team field leader: Name and documented evidence that the team field leader has satisfactorily performed full-time supervision of TAB work in the field for not less than 3 years immediately preceding this contract's bid opening date.

TAB team field technicians: Names and documented evidence that each field technician has satisfactorily assisted a TAB team field leader in performance of TAB work in the field for not less than one year immediately preceding this contract's bid opening date.

Current certificates: Registrations and certifications are current, and valid for the duration of this contract. Renew Certifications which expire prior to completion of the TAB work, in a timely manner so that there is no lapse in registration or certification. TAB agency or TAB team personnel without a current registration or current certification are not to perform TAB work on this contract.

b. TAB Team Members: TAB team approved to accomplish work on this contract are full-time employees of the TAB agency. No other personnel is allowed to do TAB work on this contract.

c. Replacement of TAB team members: Replacement of members may occur if each new member complies with the applicable personnel qualifications and each is approved by the Contracting Officer.

PART 2 PRODUCTS

Not Used

PART 3 EXECUTION

3.1 WORK DESCRIPTIONS OF PARTICIPANTS

Comply with requirements of this section.

3.2 PRE-DALT/TAB MEETING

Meet with the Contracting Officer's technical representative (COTR) to develop a mutual understanding relative to the details of the DALT work and TAB work requirements. Ensure that the TAB supervisor is present at this meeting. Requirements to be discussed include required submittals, work schedule, and field quality control.

3.3 DALT PROCEDURES

3.3.1 Instruments, Consumables and Personnel

Provide instruments, consumables and personnel required to accomplish the DALT field work. Follow the same basic procedure specified below for TAB Field Work, including maintenance and calibration of instruments, accuracy of measurements, preliminary procedures, field work, workmanship and treatment of deficiencies. Calibrate and maintain instruments in accordance with manufacturer's written procedures.

3.3.2

On completion of the installation of each duct system indicated to be DALT'd, notify the Contracting Officer in writing prior to the COTR's duct selection field visit.

3.3.3 Ductwork To Be DALT'd

From each duct system indicated as subject to DALT, the COTR will randomly select sections of each completed duct system for testing by the Contractor's TAB Firm. The sections selected will not exceed 20 percent of the total measured linear footage of duct systems indicated as subject to DALT. Sections of duct systems subject to DALT will include 20 percent of main ducts, branch main ducts, branch ducts and plenums for supply, return, exhaust, and plenum ductwork.

It is acceptable for an entire duct system to be DALT'd instead of disassembling that system in order to DALT only the 20 percent portion specified above.

3.3.4 DALT Testing

Perform DALT on the HVAC duct sections of each system as selected by the COTR. Use the duct class, seal class, leakage class and the leak test pressure data indicated on the drawings, to comply with the procedures specified in SMACNA 1972 CD.

In spite of specifications of SMACNA 1972 CD to the contrary, DALT ductwork of construction class of 3-inch water gauge static pressure and below if indicated to be DALT'd. Complete DALT work on the COTR selected ductwork within 48 hours after the particular ductwork was selected for DALT. Separately conduct DALT work for large duct systems to enable the DALT work to be completed in 48 hours.

3.3.5 Completed Pre-Final DALT Report

3.3.6 Quality Assurance - COTR DALT Field Acceptance Testing

In the presence of the COTR and TAB team field leader, verify for accuracy Pre-final DALT Report data selected by the COTR. For each duct system, this acceptance testing shall be conducted on a maximum of 50 percent of the duct sections DALT'd.

Further, if any data on the Pre-final DALT report form for a given duct section is out-of-tolerance, then field acceptance testing shall be conducted on data for one additional duct section, preferably in the same duct system, in the presence of the COTR.

3.3.7 Additional COTR Field Acceptance Testing

If any of the duct sections checked for a given system are determined to have a leakage rate measured that exceeds the leakage rate allowed by SMACNA Leak Test Manual for an indicated duct construction class and sealant class, terminate data checking for that section. The associated Pre-final DALT Report data for the given duct system will be disapproved. Make the necessary corrections and prepare a revised Pre-final DALT Report. Reschedule a field check of the revised report data with the COTR.

3.3.8 Certified Final DALT Report

After completion of the DALT work, prepare a Pre-final DALT Report meeting the additional requirements specified in Appendix B REPORTS - DALT and TAB. Data required by those data report forms shall be furnished by the TAB team. Prepare the report neatly and legibly; the Pre-final DALT report shall provide the basis for the Final DALT Report.

Supervisor shall review, approve and sign the Pre-Final DALT Report and submit this report within one day of completion of DALT field work. Verbally notify the COTR that the field check of the Pre-Final DALT Report data can commence.

3.3.9 Prerequisite for TAB Field Work

Do not commence TAB field work prior to the completion and approval, for all systems, of the Final DALT Report.

3.4 TAB PROCEDURES

3.4.1 TAB Field Work

Test, adjust, and balance the HVAC systems until measured flow rates (air and water flow) are within plus or minus 5 percent of the design flow rates as specified or indicated on the contract documents.

That is, comply with the the requirements of AABC MN-1 or SMACNA 1780 (TABB) and SMACNA 1858 (TABB),except as supplemented and modified by this section.

Provide instruments and consumables required to accomplish the TAB work. Calibrate and maintain instruments in accordance with manufacturer's written procedures.

Test, adjust, and balance the HVAC systems until measured flow rates (air and water flow) are within plus or minus 5 percent of the design flow rates as specified or indicated on the contract documents. Conduct TAB work, including measurement accuracy, and sound measurement work in conformance with the AABC MN-1 and AABC MN-4, or NEBB TABES and NEBB MASV, or SMACNA 1780 (used by TABB) and SMACNA 1858 sound measurement procedures, except as supplemented and modified by this section.

3.4.2 Preliminary Procedures

Use the approved pre-field engineering report as instructions and procedures for accomplishing TAB field work. TAB engineer is to locate, in the field, test ports required for testing. It is the responsibility of the sheet metal contractor to provide and install test ports as required by the TAB engineer.

3.4.3 TAB Air Distribution Systems

3.4.3.1 Units With Coils

Report heating and cooling performance capacity tests for hot water, chilled water, DX and steam coils for the purpose of verifying that the coils meet the indicated design capacity. Submit the following data and calculations with the coil test reports:

a. For air handlers with capacities greater than 7.5 tons (90,000 Btu) cooling, such as factory manufactured units, central built-up units and rooftop units, conduct capacity tests in accordance with AABC MN-4, procedure 3.5, "Coil Capacity Testing."

   Do not determine entering and leaving wet and dry bulb temperatures by single point measurement, but by the average of multiple readings in compliance with paragraph 3.5-5, "Procedures", (in subparagraph d.) of AABC MN-4, Procedure 3.5, "Coil Capacity Testing."

   Submit part-load coil performance data from the coil manufacturer converting test conditions to design conditions; use the data for the purpose of verifying that the coils meet the indicated design capacity in compliance with AABC MN-4, Procedure 3.5, "Coil Capacity Testing," paragraph 3.5.7, "Actual Capacity Vs. Design Capacity" (in subparagraph c.).

b. For units with capacities of 7.5 tons (90,000 Btu) or less, such as fan coil units, duct mounted reheat coils associated with VAV terminal units, and unitary units, such as through-the-wall heat pumps:

   Determine the apparent coil capacity by calculations using single point measurement of entering and leaving wet and dry bulb temperatures; submit the calculations with the coil reports.

3.4.3.2 Rooftop Air Conditioning

Rooftop air conditioning systems including fans, coils, ducts, plenums, and air distribution devices for supply air, return air, and outside air.

For refrigeration compressors/condensers/condensing units/evaporators, report data as required by NEBB, AABC, and TABB standard procedures, including refrigeration operational data.

3.4.3.3 Exhaust Fans

Exhaust fan systems including fans, ducts, plenums, grilles, and hoods for exhaust air.

3.4.4 TAB Work on Performance Tests Without Seasonal Limitations

3.4.4.1 Performance Tests

In addition to the TAB proportionate balancing work on the air distribution systems and the water distribution systems, accomplish TAB work on the HVAC systems which directly transfer thermal energy. TAB the operational performance of the heating systems and cooling systems.

3.4.4.2 Ambient Temperatures

On each tab report form used for recording data, record the outdoor and indoor ambient dry bulb temperature range and the outdoor and indoor ambient wet bulb temperature range within which the report form's data was recorded. Record these temperatures at beginning and at the end of data taking.

3.4.4.3 Sound Measurements

Comply with the paragraph SOUND MEASUREMENT WORK, specifically, the requirement that a room must be operating in its noisiest mode at the time of sound measurements in the room. The maximum noise level measurements could depend on seasonally related heat or cooling transfer equipment.

3.4.5 Workmanship

Conduct TAB work on the HVAC systems until measured flow rates are within plus or minus 5 percent of the design flow rates as specified or indicated on the contract documents. This TAB work includes adjustment of balancing valves, balancing dampers, and sheaves. Further, this TAB work includes changing out fan sheaves and pump impellers if required to obtain air and water flow rates specified or indicated. If, with these adjustments and equipment changes, the specified or indicated design flow rates cannot be attained, contact the Contracting Officer for direction.

3.4.6 Deficiencies

Strive to meet the intent of this section to maximize the performance of the equipment as designed and installed. However, if deficiencies in equipment design or installation prevent TAB work from being accomplished within the range of design values specified in the paragraph WORKMANSHIP, provide written notice as soon as possible to the Contractor and the Contracting Officer describing the deficiency and recommended correction.

Responsibility for correction of installation deficiencies is the Contractor's. If a deficiency is in equipment design, call the TAB team supervisor for technical assistance. Responsibility for reporting design deficiencies to Contractor is the TAB team supervisor's.

3.4.7 TAB Reports

3.4.8 Quality Assurance - COTR TAB Field Acceptance Testing

3.4.8.1 TAB Field Acceptance Testing

During the field acceptance testing, verify, in the presence of the COTR, random selections of data (water, air quantities, air motion,) recorded in the TAB Report. Points and areas for field acceptance testing are to be selected by the COTR. Measurement and test procedures are the same as approved for TAB work for the TAB Report.

Field acceptance testing includes verification of TAB Report data recorded for the following equipment groups:

Group 1: All chillers, boilers, return fans, computer room units, and air handling units (rooftop and central stations).

Group 2: 25 percent of the VAV terminal boxes and associated diffusers and registers.

Group 3: 25 percent of the supply diffusers, registers, grilles associated with constant volume air handling units.

Group 4: 25 percent of the return grilles, return registers, exhaust grilles and exhaust registers.

Group 5: 25 percent of the supply fans, exhaust fans, and pumps.

Further, if any data on the TAB Report for Groups 2 through 5 is found not to fall within the range of plus 5 to minus 5 percent of the TAB Report data, additional group data verification is required in the presence of the COTR. Verify TAB Report data for one additional piece of equipment in that group. Continue this additional group data verification until out-of-tolerance data ceases to be found.

3.4.8.2 Additional COTR TAB Field Acceptance Testing

If any of the acceptance testing measurements for a given equipment group is found not to fall within the range of plus 5 to minus 5 percent of the TAB Report data, terminate data verification for all affected data for that group. The affected data for the given group will be disapproved. Make the necessary corrections and prepare a revised TAB Report. Reschedule acceptance testing of the revised report data with the COTR.

3.4.8.3 Prerequisite for Approval

Compliance with the field acceptance testing requirements of this section is a prerequisite for the final Contracting Officer approval of the TAB Report submitted.

3.5 MARKING OF SETTINGS

Upon the final TAB work approval, permanently mark the settings of HVAC adjustment devices including valves, gauges, splitters, and dampers so that adjustment can be restored if disturbed at any time. Provide permanent markings clearly indicating the settings on the adjustment devices which result in the data reported on the submitted TAB report.

3.6 MARKING OF TEST PORTS

The TAB team is to permanently and legibly mark and identify the location points of the duct test ports. If the ducts have exterior insulation, make these markings on the exterior side of the duct insulation. Show the location of test ports on the as-built mechanical drawings with dimensions given where the test port is covered by exterior insulation.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 07 00

THERMAL INSULATION FOR MECHANICAL SYSTEMS

PART 1 GENERAL

1.1 REFERENCES
1.2 SYSTEM DESCRIPTION
1.2.1 General
1.3 SUBMITTALS
1.4 CERTIFICATIONS
1.4.1 Adhesives and Sealants
1.5 QUALITY ASSURANCE
1.5.1 Installer Qualification
1.6 DELIVERY, STORAGE, AND HANDLING

PART 2 PRODUCTS

2.1 STANDARD PRODUCTS
2.1.1 Insulation System
2.1.2 Surface Burning Characteristics
2.2 MATERIALS
2.2.1 Adhesives
2.2.1.1 Acoustical Lining Insulation Adhesive
2.2.1.2 Mineral Fiber Insulation Cement
2.2.1.3 Lagging Adhesive
2.2.1.4 Contact Adhesive
2.2.2 Caulking
2.2.3 Corner Angles
2.2.4 Fittings
2.2.5 Finishing Cement
2.2.6 Fibrous Glass Cloth and Glass Tape
2.2.7 Staples
2.2.8 Jackets
2.2.8.1 Aluminum Jackets
2.2.8.2 Polyvinyl Chloride (PVC) Jackets
2.2.8.3 Vapor Barrier/Weatherproofing Jacket
2.2.8.4 Vapor Barrier/Vapor Retarder
2.2.9 Vapor Retarder Required
2.2.9.1 White Vapor Retarder All Service Jacket (ASJ)
2.2.9.2 Vapor Retarder/Vapor Barrier Mastic Coatings
2.2.9.2.1 Vapor Barrier
2.2.9.2.2 Vapor Retarder
2.2.9.3 Laminated Film Vapor Retarder
2.2.9.4 Polyvinylidene Chloride (PVDC) Film Vapor Retarder
2.2.9.5 Polyvinylidene Chloride Vapor Retarder Adhesive Tape
2.2.9.6 Vapor Barrier/Weather Barrier
2.2.10 Vapor Retarder Not Required
2.2.11 Wire
2.2.12 Insulation Bands

2.2.13 Sealants
2.3 DUCT INSULATION SYSTEMS
2.3.1 Acoustical Duct Lining
2.3.1.1 General
2.3.1.2 Duct Liner
2.3.2 Duct Insulation Jackets
2.3.2.1 All-Purpose Jacket
2.3.2.2 Metal Jackets
2.3.2.2.1 Aluminum Jackets
2.3.2.2.2 Stainless Steel Jackets
2.3.2.3 Vapor Barrier/Weatherproofing Jacket
2.4 EQUIPMENT INSULATION SYSTEMS

PART 3 EXECUTION

3.1 APPLICATION - GENERAL
3.1.1 Display Samples
3.1.1.1 Pipe Insulation Display Sections
3.1.1.2 Duct Insulation Display Sections
3.1.2 Installation
3.1.3 Firestopping
3.1.4 Painting and Finishing
3.1.5 Installation of Flexible Elastomeric Cellular Insulation
3.1.5.1 Adhesive Application
3.1.5.2 Adhesive Safety Precautions
3.1.6 Welding
3.1.7 Pipes/Ducts/Equipment That Require Insulation
3.2 PIPE INSULATION SYSTEMS INSTALLATION
3.2.1 Pipe Insulation
3.2.1.1 General
3.2.1.2 Pipes Passing Through Walls, Roofs, and Floors
3.2.1.2.1 Penetrate Interior Walls
3.2.1.2.2 Penetrating Floors
3.2.1.2.3 Penetrating Waterproofed Floors
3.2.1.2.4 Penetrating Exterior Walls
3.2.1.2.5 Penetrating Roofs
3.2.1.2.6 Hot Water Pipes Supplying Lavatories or Other Similar Heated Service
3.2.1.2.7 Domestic Cold Water Pipes Supplying Lavatories or Other Similar Cooling Service
3.2.1.3 Pipes Passing Through Hangers
3.2.1.3.1 Horizontal Pipes Larger Than 2 Inches at 16 Degrees C 60 Degrees F and Above
3.2.1.3.2 Horizontal Pipes Larger Than 2 Inches and Below 16 Degrees C 60 Degrees F
3.2.1.3.3 Vertical Pipes
3.2.1.3.4 Inserts
3.2.1.4 Flexible Elastomeric Cellular Pipe Insulation
3.2.1.5 Pipes in high abuse areas.
3.2.1.6 Pipe Insulation Material and Thickness
3.2.2 Piping Exposed to Weather
3.2.2.1 Aluminum Jacket
3.2.2.2 Insulation for Fittings
3.2.2.3 PVC Jacket
3.2.2.4 Stainless Steel Jackets
3.3 DUCT INSULATION SYSTEMS INSTALLATION
3.3.1 Duct Insulation Minimum Thickness
3.3.2 Insulation and Vapor Retarder/Vapor Barrier for Cold Air Duct
3.3.2.1 Installation on Concealed Duct

3.3.2.2 Installation on Exposed Duct Work
3.3.3 Insulation for Warm Air Duct
3.3.3.1 Installation on Concealed Duct
3.3.3.2 Installation on Exposed Duct
3.3.4 Insulation for Evaporative Cooling Duct
3.3.5 Duct Test Holes
3.3.6 Duct Exposed to Weather
3.3.6.1 Installation
3.3.6.2 Round Duct
3.3.6.3 Fittings
3.3.6.4 Rectangular Ducts
3.4 EQUIPMENT INSULATION SYSTEMS INSTALLATION
3.4.1 Insulation for Hot Equipment
3.4.1.1 Other Equipment
3.4.2 Equipment Handling Dual Temperature Media
3.4.3 Equipment Exposed to Weather
3.4.3.1 Installation
3.4.3.2 Optional Panels

-- End of Section Table of Contents --

SECTION 23 07 00

THERMAL INSULATION FOR MECHANICAL SYSTEMS

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only. At the discretion of the Government, the manufacturer of any material supplied will be required to furnish test reports pertaining to any of the tests necessary to assure compliance with the standard or standards referenced in this specification.

ASTM INTERNATIONAL (ASTM)

ASTM A167	(2011) Standard Specification for Stainless and Heat-Resisting Chromium-Nickel Steel Plate, Sheet, and Strip
ASTM A240/A240M	(2020a) Standard Specification for Chromium and Chromium-Nickel Stainless Steel Plate, Sheet, and Strip for Pressure Vessels and for General Applications
ASTM A580/A580M	(2018) Standard Specification for Stainless Steel Wire
ASTM B209	(2014) Standard Specification for Aluminum and Aluminum-Alloy Sheet and Plate
ASTM C195	(2007; R 2013) Standard Specification for Mineral Fiber Thermal Insulating Cement
ASTM C450	(2008) Standard Practice for Fabrication of Thermal Insulating Fitting Covers for NPS Piping, and Vessel Lagging
ASTM C534/C534M	(2020a) Standard Specification for Preformed Flexible Elastomeric Cellular Thermal Insulation in Sheet and Tubular Form
ASTM C547	(2022) Standard Specification for Mineral Fiber Pipe Insulation
ASTM C552	(2022) Standard Specification for Cellular Glass Thermal Insulation
ASTM C647	(2008; R 2013) Properties and Tests of Mastics and Coating Finishes for Thermal Insulation
ASTM C755	(2019b) Standard Practice for Selection of

	Water Vapor Retarders for Thermal Insulation
ASTM C795	(2008; R 2018) Standard Specification for Thermal Insulation for Use in Contact with Austenitic Stainless Steel
ASTM C916	(2020) Standard Specification for Adhesives for Duct Thermal Insulation
ASTM C920	(2018) Standard Specification for Elastomeric Joint Sealants
ASTM C921	(2010; R 2015) Standard Practice for Determining the Properties of Jacketing Materials for Thermal Insulation
ASTM C1126	(2018) Standard Specification for Faced or Unfaced Rigid Cellular Phenolic Thermal Insulation
ASTM C1136	(2021) Standard Specification for Flexible, Low Permeance Vapor Retarders for Thermal Insulation
ASTM C1710	(2011) Standard Guide for Installation of Flexible Closed Cell Preformed Insulation in Tube and Sheet Form
ASTM D882	(2012) Tensile Properties of Thin Plastic Sheeting
ASTM D2863	(2019) Standard Test Method for Measuring the Minimum Oxygen Concentration to Support Candle-Like Combustion of Plastics (Oxygen Index)
ASTM D5590	(2000; R 2010; E 2012) Standard Test Method for Determining the Resistance of Paint Films and Related Coatings to Fungal Defacement by Accelerated Four-Week Agar Plate Assay
ASTM E84	(2020) Standard Test Method for Surface Burning Characteristics of Building Materials
ASTM E96/E96M	(2022) Standard Test Methods for Gravimetric Determination ofWater Vapor Transmission Rate of Materials
ASTM E2231	(2021) Standard Practice for Specimen Preparation and Mounting of Pipe and Duct Insulation Materials to Assess Surface Burning Characteristics

CALIFORNIA DEPARTMENT OF PUBLIC HEALTH (CDPH)

CDPH SECTION 01350	(2010; Version 1.1) Standard Method for

	the Testing and Evaluation of Volatile Organic Chemical Emissions from Indoor Sources using Environmental Chambers

FM GLOBAL (FM)

FM APP GUIDE	(updated on-line) Approval Guide http://www.approvalguide.com/

GREEN SEAL (GS)

GS-36	(2013) Adhesives for Commercial Use

MANUFACTURERS STANDARDIZATION SOCIETY OF THE VALVE AND FITTINGS INDUSTRY (MSS)

MSS SP-58	(2018) Pipe Hangers and Supports - Materials, Design and Manufacture, Selection, Application, and Installation

MIDWEST INSULATION CONTRACTORS ASSOCIATION (MICA)

MICA Insulation Stds	(8th Ed) National Commercial & Industrial Insulation Standards

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 90A	(2021) Standard for the Installation of Air Conditioning and Ventilating Systems
NFPA 90B	(2021) Standard for the Installation of Warm Air Heating and Air Conditioning Systems

SCIENTIFIC CERTIFICATION SYSTEMS (SCS)

SCS	SCS Global Services (SCS) Indoor Advantage

SOUTH COAST AIR QUALITY MANAGEMENT DISTRICT (SCAQMD)

SCAQMD Rule 1168	(2017) Adhesive and Sealant Applications

TECHNICAL ASSOCIATION OF THE PULP AND PAPER INDUSTRY (TAPPI)

TAPPI T403 OM	(2015) Bursting Strength of Paper

U.S. DEPARTMENT OF DEFENSE (DOD)

MIL-A-3316	(1987; Rev C; Am 2 1990) Adhesives, Fire-Resistant, Thermal Insulation
MIL-A-24179	(1969; Rev A; Am 2 1980; Notice 1 1987; Notice 2 2020) Adhesive, Flexible Unicellular-Plastic Thermal Insulation
MIL-PRF-19565	(1988; Rev C) Coating Compounds, Thermal Insulation, Fire- and Water-Resistant, Vapor-Barrier

UNDERWRITERS LABORATORIES (UL)

UL 94	(2013; Reprint Apr 2022) UL Standard for Safety Tests for Flammability of Plastic Materials for Parts in Devices and Appliances
UL 723	(2018) UL Standard for Safety Test for Surface Burning Characteristics of Building Materials
UL 2818	(2013) GREENGUARD Certification Program For Chemical Emissions For Building Materials, Finishes And Furnishings

1.2 SYSTEM DESCRIPTION

1.2.1 General

Provide field-applied insulation and accessories on mechanical systems as specified herein; factory-applied insulation is specified under the piping, duct or equipment to be insulated. Furnish and install field applied insulation materials required for use on Government-furnished items as listed in the SPECIAL CONTRACT REQUIREMENTS.

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

Submit the three SD types, SD-02 Shop Drawings, SD-03 Product Data, and SD-08 Manufacturer's Instructions at the same time for each system.

SD-02 Shop Drawings

Pipe Insulation Systems and Associated Accessories

Duct Insulation Systems and Associated Accessories

Equipment Insulation Systems and Associated Accessories

SD-03 Product Data

Pipe Insulation Systems

Duct Insulation Systems

Equipment Insulation Systems

SD-04 Samples

Thermal Insulation

Display Samples

SD-07 Certificates

Indoor air quality for adhesives

SD-08 Manufacturer's Instructions

Pipe Insulation Systems

Duct Insulation Systems

Equipment Insulation Systems

1.4 CERTIFICATIONS

1.4.1 Adhesives and Sealants

Provide products certified to meet indoor air quality requirements by UL 2818 (Greenguard) Gold, SCS Global Services Indoor Advantage Gold or provide certification or validation by other third-party programs that products meet the requirements of this Section. Provide current product certification documentation from certification body. When product does not have certification, provide validation that product meets the indoor air quality product requirements cited herein.

1.5 QUALITY ASSURANCE

1.5.1 Installer Qualification

Qualified installers will have successfully completed three or more similar type jobs within the last 5 years.

1.6 DELIVERY, STORAGE, AND HANDLING

Deliver materials in the manufacturer's unopened containers. Protect materials delivered and placed in storage from weather, humidity, dirt, dust and other contaminants. The Contracting Officer may reject insulation material and supplies that become dirty, dusty, wet, or contaminated by some other means. Attach manufacturer's stamp or label giving the name of the manufacturer and brand, and a description of the material, date codes, and approximate shelf life (if applicable) to packages or standard containers of insulation, jacket material, cements, adhesives, and coatings delivered for use, and samples required for approval. Insulation packages and containers must be asbestos free.

PART 2 PRODUCTS

2.1 STANDARD PRODUCTS

Provide materials which are the standard products of manufacturers regularly engaged in the manufacture of such products and that essentially duplicate items that have been in satisfactory use for at least 2 years prior to bid opening. Submit a complete list of materials, including manufacturer's descriptive technical literature, performance data, catalog cuts, and installation instructions. Include the product number, k-value, thickness and furnished accessories including adhesives, sealants and jackets for each mechanical system requiring insulation. The product data must be copyrighted, have an identifying or publication number, and have been published prior to the issuance date of this solicitation. Submit

materials furnished under this section together in a booklet.

2.1.1 Insulation System

Provide insulation systems in accordance with the approved MICA National Insulation Standards plates as supplemented by this specification. Provide field-applied insulation for heating, ventilating, and cooling (HVAC) air distribution systems and piping systems that are located within, on, under, and adjacent to buildings; and for plumbing systems. Provide CFC and HCFC free insulation.

2.1.2 Surface Burning Characteristics

Unless otherwise specified, insulation must have a maximum flame spread index of 25 and a maximum smoke developed index of 50 when tested in accordance with ASTM E84. Determine flame spread, and smoke developed indexes, by ASTM E84 or UL 723. Test insulation in the same density and installed thickness as the material to be used in the actual construction. Prepare and mount test specimens according to ASTM E2231.

2.2 MATERIALS

Provide insulation that meets or exceed the requirements of ASHRAE 90.1. Ensure insulation exterior is cleanable, grease resistant, non-flaking and non-peeling. Provide compatible materials that do not contribute to corrosion, soften, or otherwise attack surfaces to which applied in either wet or dry state. Use materials on stainless steel surfaces meeting ASTM C795 requirements. Do not use calcium silicate on chilled or cold water systems. Use asbestos free materials. Provide product recognized under UL 94 (if containing plastic) and listed in FM APP GUIDE.

2.2.1 Adhesives

Provide non-aerosol adhesive products used on the interior of the building (defined as inside of the weatherproofing system) that meet either emissions requirements of CDPH SECTION 01350 (limit requirements for either office or classroom spaces regardless of space type) or VOC content requirements of SCAQMD Rule 1168 (HVAC duct sealants must meet limit requirements of "Other" category within SCAQMD Rule 1168 sealants table). Provide aerosol adhesives used on the interior of the building that meet either emissions requirements of CDPH SECTION 01350 (use the office or classroom requirements, regardless of space type) or VOC content requirements of GS-36. Provide certification or validation of indoor air quality for adhesives.

2.2.1.1 Acoustical Lining Insulation Adhesive

Provide a nonflammable, fire-resistant adhesive conforming to ASTM C916, Type I.

2.2.1.2 Mineral Fiber Insulation Cement

Provide cement in accordance with ASTM C195.

2.2.1.3 Lagging Adhesive

Lagging is the material used for thermal insulation, especially around a cylindrical object. This may include the insulation as well as the cloth/material covering the insulation. To resist mold/mildew, use

lagging adhesive meeting ASTM D5590 with 0 growth rating. Provide nonflammable and fire-resistant lagging adhesives that have a maximum flame spread index of 25 and a maximum smoke developed index of 50 when tested in accordance with ASTM E84. Ensure adhesive is MIL-A-3316, Class 1, pigmented white and suitable for bonding fibrous glass cloth to faced and unfaced fibrous glass insulation board; for bonding cotton brattice cloth to faced and unfaced fibrous glass insulation board; for sealing edges of and bonding glass tape to joints of fibrous glass board; for bonding lagging cloth to thermal insulation; or Class 2 for attaching fibrous glass insulation to metal surfaces. Apply lagging adhesives in strict accordance with the manufacturer's recommendations for pipe and duct insulation.

2.2.1.4 Contact Adhesive

Adhesives may be any of, but not limited to, the neoprene based, rubber based, or elastomeric type that have a maximum flame spread index of 25 and a maximum smoke developed index of 50 when tested in accordance with ASTM E84. Ensure adhesive does not adversely affect, initially or in service, the insulation to which it is applied, nor cause any corrosive effect on metal to which it is applied. Ensure that any solvent dispersing medium or volatile component of the adhesive has no objectionable odor and does not contain any benzene or carbon tetrachloride. Ensure dried adhesive does not emit nauseous, irritating, or toxic volatile matters or aerosols when the adhesive is heated to any temperature up to 212 degrees F. The dried adhesive must be nonflammable and fire resistant. Flexible Elastomeric Adhesive: Comply with MIL-A-24179, Type II, Class I. Provide product listed in FM APP GUIDE.

2.2.2 Caulking

ASTM C920, Type S, Grade NS, Class 25, Use A.

2.2.3 Corner Angles

Nominal 0.016 inch aluminum 1 by 1 inch with factory applied kraft backing. Aluminum must be ASTM B209, Alloy 3003, 3105, or 5005.

2.2.4 Fittings

Fabricated Fittings are the prefabricated fittings for flexible elastomeric pipe insulation systems in accordance with ASTM C1710. Together with the flexible elastomeric tubes, they provide complete system integrity for retarding heat gain and controlling condensation drip from chilled-water and refrigeration systems. Flexible elastomeric, fabricated fittings provide thermal protection (0.25 k) and condensation resistance (0.05 Water Vapor Transmission factor). For satisfactory performance, use properly installed protective vapor retarder/barriers and vapor stops on high relative humidity and below ambient temperature applications to reduce movement of moisture through or around the insulation to the colder interior surface.

2.2.5 Finishing Cement

ASTM C450: Mineral fiber hydraulic-setting thermal insulating and finishing cement. All cements that may come in contact with Austenitic stainless steel must comply with ASTM C795.

2.2.6 Fibrous Glass Cloth and Glass Tape

Provide fibrous glass cloth, with 20X20 maximum mesh size, and glass tape with maximum flame spread index of 25 and a maximum smoke developed index of 50 when tested in accordance with ASTM E84. Provide tape consisting of 4 inch wide rolls. Provide Class 3 tape that is 4.5 ounces/square yard. Elastomeric Foam Tape: Black vapor-retarder foam tape with acrylic adhesive containing an anti-microbial additive.

2.2.7 Staples

Outward clinching type ASTM A167, Type 304 or 316 stainless steel.

2.2.8 Jackets

2.2.8.1 Aluminum Jackets

Provide aluminum jackets consisting of corrugated, embossed or smooth sheet, 0.016 inch nominal thickness; ASTM B209, Temper H14, Temper H16, Alloy 3003, 5005, or 3105. Do not use corrugated aluminum jacket outdoors. Aluminum jacket securing bands must be Type 304 stainless steel, 0.015 inch thick, 1/2 inch wide for pipe under 12 inch diameter and 3/4 inch wide for pipe over 12 inch and larger diameter. Aluminum jacket circumferential seam bands must be 2 by 0.016 inch aluminum matching jacket material. Ensure bands for insulation below ground are 3/4 by 0.020 inch thick stainless steel, or fiberglass reinforced tape. The jacket may, at the option of the Contractor, be provided with a factory fabricated Pittsburgh or "Z" type longitudinal joint. When the "Z" joint is used, use bands at the circumferential joints that are designed by the manufacturer to seal the joints and hold the jacket in place.

2.2.8.2 Polyvinyl Chloride (PVC) Jackets

Polyvinyl chloride (PVC) jacket and fitting covers must have high impact strength, ultraviolet (UV) resistant rating or treatment and moderate chemical resistance with minimum thickness 0.030 inch.

2.2.8.3 Vapor Barrier/Weatherproofing Jacket

Provide laminated self-adhesive vapor barrier/weatherproofing jacket, greater than 3 plies standard grade, silver, white, black and embossed or greater than 8 ply (minimum 2.9 mils adhesive); with 0.0000 permeability when tested in accordance with ASTM E96/E96M, using the water transmission rate test method; heavy duty, white or natural; and UV resistant. Flexible Elastomeric exterior foam with factory applied, UV Jacket made with a cold weather acrylic adhesive. Construction of laminate designed to provide UV resistance, high puncture, tear resistance and excellent Water Vapor Transmission (WVT) rate.

2.2.8.4 Vapor Barrier/Vapor Retarder

Apply the following criteria to determine which system is required.

a. On ducts, equip piping and equipment operating below 93.9 degrees F or located outside with a vapor barrier.

b. Install ducts, pipes and equipment that are located inside and that always operate above 93.9 degrees F with a vapor retarder where

required as stated in paragraph VAPOR RETARDER REQUIRED.

2.2.9 Vapor Retarder Required

ASTM C921, Type I, minimum puncture resistance 50 Beach units on all surfaces except concealed ductwork, where a minimum puncture resistance of 25 Beach units is acceptable. Minimum tensile strength, 35 pounds/inch width. ASTM C921, Type II, minimum puncture resistance 25 Beach units, tensile strength minimum 20 pounds/inch width. Use jackets on insulation exposed in finished areas that have white finish suitable for painting without sizing. Based on the application, insulation materials that require manufacturer or fabricator applied pipe insulation jackets are cellular glass, when all joints are sealed with a vapor barrier mastic, and mineral fiber. Ensure all non-metallic jackets have a maximum flame spread index of 25 and a maximum smoke developed index of 50 when tested in accordance with ASTM E84. Flexible elastomerics require (in addition to vapor barrier skin) vapor retarder jacketing for high relative humidity and below ambient temperature applications.

2.2.9.1 White Vapor Retarder All Service Jacket (ASJ)

ASJ is for use on hot/cold pipes, ducts, or equipment indoors or outdoors if covered by a suitable protective jacket. Provide product which meets all physical property and performance requirements of ASTM C1136, Type I, except a minimum burst strength of 85 psi. ASTM D2863 Limited Oxygen Index (LOI) is a minimum of 31.

In addition, do not use paper or other moisture-sensitive material for the outer exposed surface or the inner-most surface contacting the insulation. Ensure the outer exposed surface is white and has an emittance no less than 0.80. Ensure the outer exposed surface is paintable.

2.2.9.2 Vapor Retarder/Vapor Barrier Mastic Coatings

2.2.9.2.1 Vapor Barrier

The vapor barrier must be self adhesive (minimum 2 mils adhesive, 3 mils embossed) greater than 3 plies standard grade, silver, white, black and embossed white jacket for use on hot/cold pipes. Ensure permeability is less than 0.02 when tested in accordance with ASTM E96/E96M. Provide products meeting UL 723 or ASTM E84 flame and smoke requirements and that are UV resistant.

2.2.9.2.2 Vapor Retarder

Provide fire and water resistant vapor retarder coating appropriately selected for either outdoor or indoor service. Color must be white. Ensure the water vapor permeance of the compound is in accordance with ASTM C755, Section 7.2.2, Table 2, for insulation type and service conditions. Provide nonflammable, fire resistant coating. To resist mold/mildew, provide coating meeting ASTM D5590 with 0 growth rating. Ensure coating meets MIL-PRF-19565 Type II (if selected for indoor service) and is Qualified Products Database listed. Determine all other application and service properties pursuant to ASTM C647.

2.2.9.3 Laminated Film Vapor Retarder

ASTM C1136, Type I, maximum moisture vapor transmission 0.02 perms,

minimum puncture resistance 50 Beach units on all surfaces except concealed ductwork; where Type II, maximum moisture vapor transmission 0.02 perms, a minimum puncture resistance of 25 Beach units is acceptable. Provide vapor retarder with a maximum flame spread index of 25 and a maximum smoke developed index of 50 when tested in accordance with ASTM E84. Flexible Elastomeric exterior foam with factory applied UV Jacket. Construction of laminate designed to provide UV resistance, high puncture, tear resistance and an excellent WVT rate.

2.2.9.4 Polyvinylidene Chloride (PVDC) Film Vapor Retarder

Provide PVDC film vapor retarder with a maximum moisture vapor transmission of 0.02 perms, minimum puncture resistance of 150 Beach units, a minimum tensile strength in any direction of 30 lb/inch when tested in accordance with ASTM D882, and a maximum flame spread index of 25 and a maximum smoke developed index of 50 when tested in accordance with ASTM E84.

2.2.9.5 Polyvinylidene Chloride Vapor Retarder Adhesive Tape

Requirements must meet the same as specified for Laminated Film Vapor Retarder above.

2.2.9.6 Vapor Barrier/Weather Barrier

Ensure the vapor barrier is greater than 3 ply self adhesive laminate -white vapor barrier jacket- superior performance (less than 0.0000 permeability when tested in accordance with ASTM E96/E96M). Provide vapor barrier meeting UL 723 or ASTM E84 25 flame and 50 smoke requirements; and UV resistant. Minimum burst strength 185 psi in accordance with TAPPI T403 OM . Tensile strength 68 lb/inch width (PSTC-1000). Provide tape as specified for laminated film vapor barrier above.

2.2.10 Vapor Retarder Not Required

ASTM C921, Type II, Class D, minimum puncture resistance 50 Beach units on all surfaces except ductwork, where Type IV, maximum moisture vapor transmission 0.10, a minimum puncture resistance of 25 Beach units is acceptable. Provide jacket with a maximum flame spread index of 25 and a maximum smoke developed index of 50 when tested in accordance with ASTM E84.

2.2.11 Wire

Soft annealed ASTM A580/A580M Type 302, 304 or 316 stainless steel, 16 or 18 gauge.

2.2.12 Insulation Bands

Provide 1/2 inch wide; 26 gauge stainless steel insulation bands.

2.2.13 Sealants

Choose sealants from the butyl polymer type, the styrene-butadiene rubber type, or the butyl type of sealants. Provide sealants with a maximum permeance of 0.02 perms based on Procedure B for ASTM E96/E96M, and a maximum flame spread index of 25 and a maximum smoke developed index of 50 when tested in accordance with ASTM E84.

2.3 DUCT INSULATION SYSTEMS

2.3.1 Acoustical Duct Lining

2.3.1.1 General

For ductwork indicated or specified in Section 23 31 13.00 40 METAL DUCTS to be acoustically lined, provide external insulation in accordance with this specification section and in addition to the acoustical duct lining. Do not use acoustical lining in place of duct wrap or rigid board insulation (insulation on the exterior of the duct).

2.3.1.2 Duct Liner

Flexible Elastomeric Acoustical and Conformable Duct Liner Materials: Flexible Elastomeric Thermal, Acoustical and Conformable Insulation Compliance with ASTM C534/C534M Grade 1, Type II; and NFPA 90A or NFPA 90B as applicable.

2.3.2 Duct Insulation Jackets

2.3.2.1 All-Purpose Jacket

Provide insulation with insulation manufacturer's standard reinforced fire-retardant jacket with or without integral vapor barrier as required by the service. In exposed locations, provide jacket with a white surface suitable for field painting.

2.3.2.2 Metal Jackets

2.3.2.2.1 Aluminum Jackets

ASTM B209, Temper H14, minimum thickness of 27 gauge (0.016 inch), with factory-applied polyethylene and kraft paper moisture barrier on inside surface. Provide smooth surface jackets for jacket outside dimension 8 inches and larger. Provide corrugated surface jackets for jacket outside dimension 8 inches and larger. Provide stainless steel bands, minimum width of 1/2 inch.

2.3.2.2.2 Stainless Steel Jackets

ASTM A167 or ASTM A240/A240M; Type 304, minimum thickness of 33 gauge (0.010 inch), smooth surface with factory-applied polyethylene and kraft paper moisture barrier on inside surface. Provide stainless steel bands, minimum width of 1/2 inch.

2.3.2.3 Vapor Barrier/Weatherproofing Jacket

Provide vapor barrier/weatherproofing jacket that is laminated self-adhesive (minimum 2 mils adhesive, 3 mils embossed) less than 0.0000 permeability, (greater than 3 ply, standard grade, silver, white, black and embossed or greater than 8 ply (minimum 2.9 mils adhesive), heavy duty white or natural).

2.4 EQUIPMENT INSULATION SYSTEMS

Insulate equipment and accessories as specified in Tables 5 and 6. In outside locations, provide insulation 1/2 inch thicker than specified. Increase the specified insulation thickness for equipment where necessary

to equal the thickness of angles or other structural members to make a smooth, exterior surface. Submit a booklet containing manufacturer's published installation instructions for the insulation systems. The instructions must be copyrighted, have an identifying or publication number, and have been published prior to the issuance date of this solicitation. A booklet is also required by paragraphs titled: Pipe Insulation Systems and Duct Insulation Systems.

PART 3 EXECUTION

3.1 APPLICATION - GENERAL

Apply insulation to unheated and uncooled piping and equipment. Do not compress flexible elastomeric cellular insulation at joists, studs, columns, ducts, and hangers. The insulation must not pull apart after a one hour period; replace any insulation found to pull apart after one hour.

3.1.1 Display Samples

Submit and display, after approval of materials, actual sections of installed systems, properly insulated in accordance with the specification requirements. Such actual sections must remain accessible to inspection throughout the job and will be reviewed from time to time for controlling the quality of the work throughout the construction site. Identify each material used by indicating on an attached sheet the specification requirement for the material and the material by each manufacturer intended to meet the requirement. The Contracting Officer will inspect display sample sections at the jobsite. Keep approved display sample sections on display at the jobsite during the construction period. Upon completion of construction, the display sample sections will be closed and sealed.

3.1.1.1 Pipe Insulation Display Sections

Include as a minimum an elbow or tee, a valve, dielectric waterways and flanges, a hanger with protection shield and insulation insert, or dowel as required, at support point, method of fastening and sealing insulation at longitudinal lap, circumferential lap, butt joints at fittings and on pipe runs, and terminating points for each type of pipe insulation used on the job, and for hot pipelines and cold pipelines, both interior and exterior, even when the same type of insulation is used for these services.

3.1.1.2 Duct Insulation Display Sections

Display sample sections for rigid and flexible duct insulation used on the job. Use a temporary covering to enclose and protect display sections for duct insulation exposed to weather

3.1.2 Installation

Except as otherwise specified, install material in accordance with the manufacturer's written instructions. Do not apply insulation materials until tests specified in other sections of this specification are completed. Remove material such as rust, scale, dirt and moisture from surfaces to receive insulation. Keep insulaton clean and dry. Do not remove insulation from its shipping containers until the day it is ready to use and return to like containers or equally protect from dirt and moisture at the end of each workday. Thoroughly clean insulation that becomes dirty prior to use. If insulation becomes wet or if cleaning does

not restore the surfaces to like new condition, reject the insulation, and immediately remove from the jobsite. Stagger joints on multi layer insulation. Mix mineral fiber thermal insulating cement with demineralized water when used on stainless steel surfaces. Install insulation, jacketing and accessories in accordance with MICA Insulation Stds plates except where modified herein or on the drawings.

3.1.3 Firestopping

Where pipes and ducts pass through fire walls, fire partitions, above grade floors, and fire rated chase walls, seal the penetration with fire stopping materials as specified in Section 07 84 00 FIRESTOPPING. The protection of ducts at point of passage through firewalls must be in accordance with NFPA 90A and/or NFPA 90B. All other penetrations, such as piping, conduit, and wiring, through firewalls must be protected with a material or system of the same hourly rating that is listed by UL, FM, or a NRTL.

3.1.4 Painting and Finishing

Paint as specified in Section 09 90 00 PAINTS AND COATINGS.

3.1.5 Installation of Flexible Elastomeric Cellular Insulation

Install flexible elastomeric cellular insulation with seams and joints sealed with rubberized contact adhesive. Do not use flexible elastomeric cellular insulation on surfaces greater than 220 degrees F. Stagger seams when applying multiple layers of insulation. Protect insulation exposed to weather and not shown to have vapor barrier weatherproof jacketing with two coats of UV resistant finish or PVC or metal jacketing as recommended by the manufacturer after the adhesive is dry and cured.

3.1.5.1 Adhesive Application

Apply a brush coating of adhesive to both butt ends to be joined and to both slit surfaces to be sealed. Allow the adhesive to set until dry to touch but tacky under slight pressure before joining the surfaces. Ensure insulation seals at seams and joints are not capable of being pulled apart one hour after application. Replace insulation that can be pulled apart one hour after installation.

3.1.5.2 Adhesive Safety Precautions

Use natural cross-ventilation, local (mechanical) pickup, and/or general area (mechanical) ventilation to prevent an accumulation of solvent vapors, keeping in mind the ventilation pattern must remove any heavier-than-air solvent vapors from lower levels of the workspaces. Gloves and spectacle-type safety glasses are recommended in accordance with safe installation practices.

3.1.6 Welding

Welding is not permitted on piping, duct or equipment without written approval of the Contracting Officer. The capacitor discharge welding process may be used for securing metal fasteners to duct.

3.1.7 Pipes/Ducts/Equipment That Require Insulation

Insulation is required on all pipes, ducts, or equipment, except for omitted items as specified.

3.2 PIPE INSULATION SYSTEMS INSTALLATION

3.2.1 Pipe Insulation

3.2.1.1 General

Install pipe insulation on aboveground hot and cold pipeline systems as specified below to form a continuous thermal retarder/barrier, including straight runs, fittings and appurtenances unless specified otherwise. Install full length units of insulation using a single cut piece to complete a run. Do not use cut pieces or scraps abutting each other. Omit pipe insulation on the following:

a. Pipe used solely for fire protection.

b. Chromium plated pipe to plumbing fixtures. However, for fixtures used by the physically handicapped, insulate the hot water supply and drain, including the trap, where exposed.

c. Sanitary drain lines.

d. Air chambers.

e. Adjacent insulation.

f. ASME stamps.

g. Access plates of fan housings.

h. Cleanouts or handholes.

3.2.1.2 Pipes Passing Through Walls, Roofs, and Floors

Provide continuous pipe insulation through the sleeve.

Provide an aluminum jacket or vapor barrier/weatherproofing self adhesive jacket (minimum 2 mils adhesive, 3 mils embossed) less than 0.0000 permeability, greater than 3 ply standard grade, silver, white, black and embossed with factory applied moisture retarder over the insulation wherever penetrations require sealing.

3.2.1.2.1 Penetrate Interior Walls

Provide aluminum jacket or vapor barrier/weatherproofing - self adhesive jacket (minimum 2 mils adhesive, 3 mils embossed) less than 0.0000 permeability, greater than 3 plies standard grade, silver, white, black and embossed which extends 2 inches beyond either side of the wall and secure on each end with a band.

3.2.1.2.2 Penetrating Floors

Extend the aluminum jacket from a point below the backup material to a point 10 inches above the floor with one band at the floor and one not

more than 1 inch from the end of the aluminum jacket.

3.2.1.2.3 Penetrating Waterproofed Floors

Extend the aluminum jacket rom below the backup material to a point 2 inches above the flashing with a band 1 inch from the end of the aluminum jacket.

3.2.1.2.4 Penetrating Exterior Walls

Continue the aluminum jacket required for pipe exposed to weather through the sleeve to a point 2 inches beyond the interior surface of the wall.

3.2.1.2.5 Penetrating Roofs

Insulate pipe as required for interior service to a point flush with the top of the flashing and sealed with flashing sealant. Tightly butt the insulation for exterior application to the top of flashing and interior insulation. Extend the exterior aluminum jacket 2 inches down beyond the end of the insulation to form a counter flashing. Seal the flashing and counter flashing underneath with metal jacketing/flashing sealant.

3.2.1.2.6 Hot Water Pipes Supplying Lavatories or Other Similar Heated Service

Terminate the insulation on the backside of the finished wall. Protect the insulation termination with two coats of vapor barrier coating with a minimum total thickness of 1/16 inch applied with glass tape embedded between coats (if applicable). Extend the coating out onto the insulation 2 inches and seal the end of the insulation. Overlap glass tape seams 1 inch. Caulk the annular space between the pipe and wall penetration with approved fire stop material. Cover the pipe and wall penetration with a properly sized (well fitting) escutcheon plate. Ensure the escutcheon plate overlaps the wall penetration at least 3/8 inches.

3.2.1.2.7 Domestic Cold Water Pipes Supplying Lavatories or Other Similar Cooling Service

Terminate the insulation on the finished side of the wall (i.e., insulation must cover the pipe throughout the wall penetration). Protect the insulation with two coats of weather barrier mastic (breather emulsion type weatherproof mastic impermeable to water and permeable to air) with a minimum total thickness of 1/16 inch. Extend the mastic out onto the insulation 2 inches and seal the end of the insulation. The annular space between the outer surface of the pipe insulation and caulk the wall penetration with an approved fire stop material having vapor retarder properties. Cover the pipe and wall penetration with a properly sized (well fitting) escutcheon plate. Ensure the escutcheon plate overlaps the wall penetration by at least 3/8 inches.

3.2.1.3 Pipes Passing Through Hangers

Ensure insulation, whether hot or cold application, is continuous through hangers. Support all horizontal pipes 2 inches and smaller on hangers with the addition of a Type 40 protection shield to protect the insulation in accordance with MSS SP-58. Whenever insulation shows signs of being compressed, or when the insulation or jacket shows visible signs of distortion at or near the support shield, install insulation inserts as specified below for piping larger than 2 inches, or factory insulated

hangers (designed with a load bearing core) can be used.

3.2.1.3.1 Horizontal Pipes Larger Than 2 Inches at 60 Degrees F and Above

Supported on hangers in accordance with MSS SP-58, and Section 22 00 00 PLUMBING, GENERAL PURPOSE.

3.2.1.3.2 Horizontal Pipes Larger Than 2 Inches and Below 60 Degrees F

Supported on hangers with the addition of a Type 40 protection shield in accordance with MSS SP-58. Install an insulation insert of cellular glass, prefabricated insulation pipe hangers, or perlite above 80 degrees F above each shield. Ensure insert covers no less than the bottom 180-degree arc of the pipe. Provide inserts that are the same thickness as the insulation, and extend 2 inches on each end beyond the protection shield. When insulation inserts are required in accordance with the above, and the insulation thickness is less than 1 inch, wooden or cork dowels or blocks may be installed between the pipe and the shield to prevent the weight of the pipe from crushing the insulation, as an option to installing insulation inserts. Ensure the insulation jacket is continuous over the wooden dowel, wooden block, or insulation insert.

3.2.1.3.3 Vertical Pipes

Supported with either Type 8 or Type 42 riser clamps with the addition of two Type 40 protection shields in accordance with MSS SP-58 covering the 360-degree arc of the insulation. Install an insulation insert of cellular glass or calcium silicate between each shield and the pipe. Ensure the insert covers the 360-degree arc of the pipe. Provide inserts that are the same thickness as the insulation, and extend 2 inches on each end beyond the protection shield. When insulation inserts are required in accordance with the above, and the insulation thickness is less than 1 inch, wooden or cork dowels or blocks may be installed between the pipe and the shield to prevent the hanger from crushing the insulation, as an option instead of installing insulation inserts. Ensure the insulation jacket is continuous over the wooden dowel, wooden block, or insulation insert. Support the vertical weight of the pipe with hangers located in a horizontal section of the pipe. When the pipe riser is longer than 30 feet, support the weight of the pipe additionally with hangers in the vertical run of the pipe that are directly clamped to the pipe, penetrating the pipe insulation. Use insulated hangers and seal the insulation jacket as indicated herein for anchors in a similar service.

3.2.1.3.4 Inserts

Covered with a jacket material of the same appearance and quality as the adjoining pipe insulation jacket, overlap the adjoining pipe jacket 1-1/2 inches, and seal as required for the pipe jacket. Use jacket material to cover inserts in flexible elastomeric cellular insulation conforming to ASTM C1136, Type 1, and is allowed to be of a different material than the adjoining insulation material.

3.2.1.4 Flexible Elastomeric Cellular Pipe Insulation

Use tubular form flexible elastomeric cellular pipe insulation for pipe sizes 6 inches and less. Grade 1, Do not stretch Type II sheet insulation used on pipes larger than 6 inches around the pipe. On pipes larger than 12 inches, adhere the insulation directly to the pipe on the lower 1/3 of the pipe. Stagger seams when applying multiple layers of insulation.

Insulate sweat fittings with miter-cut pieces the same size as on adjacent piping. Insulate screwed fittings with sleeved fitting covers fabricated from miter-cut pieces and overlap and seal to the adjacent pipe insulation. Type II requires an additional exterior vapor retarder/barrier covering for high relative humidity and below ambient temperature applications.

3.2.1.5 Pipes in high abuse areas.

In high abuse areas such as janitor closets and traffic areas in equipment rooms, kitchens, and mechanical rooms, utilize stainless steel, aluminum or flexible laminate cladding (comprised of elastomeric, plastic or metal foil laminate) laminated self-adhesive (minimum 2 mils adhesive, 3 mils embossed) vapor barrier/weatherproofing jacket, - less than 0.0000 permeability; (greater than 3 ply, standard grade, silver, white, black and embossed) aluminum jackets. Protect pipe insulation to the 6 foot level.

3.2.1.6 Pipe Insulation Material and Thickness

Pipe insulation materials must be as listed in Table 1 and must meet or exceed the requirements of ASHRAE 90.1.

TABLE 1					
Insulation Material for Piping					
Service					
	Material	Specification	Type	Class	VR/VB Req'd
Cold Domestic Water Piping, Makeup Water & Drinking Fountain Drain Piping					
	Cellular Glass	ASTM C552	II	2	No
	Flexible Elastomeric Cellular	ASTM C534/C534M	I		No
Hot Domestic Water Supply & Recirculating Piping (Max 200 F)					
	Mineral Fiber	ASTM C547	I	1	No
	Cellular Glass	ASTM C552	II	2	No
	Flexible Elastomeric Cellular	ASTM C534/C534M	I		No
	Faced Phenolic Foam	ASTM C1126	III		Yes
Refrigerant Suction Piping (35 degrees F nominal)					
	Flexible Elastomeric Cellular	ASTM C534/C534M	I		No
	Cellular Glass	ASTM C552	II	1	Yes
Exposed Lavatory Drains, Exposed Domestic Water Piping & Drains to Areas for Handicapped Personnel					
	Flexible Elastomeric Cellular	ASTM C534/C534M	I		No
Horizontal Roof Drain Leaders (Including Underside of Roof Drain Fittings)					
	Flexible Elastomeric Cellular	ASTM C534/C534M	I		No

TABLE 1					
Insulation Material for Piping					
Service					
	Material	Specification	Type	Class	VR/VB Req'd
	Faced Phenolic Foam	ASTM C1126	III		Yes
	Cellular Glass	ASTM C552	III		Yes
Condensate Drain Located Inside Building					
	Cellular Glass	ASTM C552	II	2	No
	Flexible Elastomeric Cellular	ASTM C534/C534M	I		No
Note: VR/VB = Vapor Retarder/Vapor Barrier					

TABLE 2						
Piping Insulation Thickness (inch) Do not use integral wicking material in Chilled water applications exposed to outdoor ambient conditions in climatic zones 1 through 4.						
Service						
	Material	Tube And Pipe Size (inch)				
		<1	1-<1.5	1.5-<4	4-<8	> or = >8
Cold Domestic Water Piping, Makeup Water & Drinking Fountain Drain Piping						
	Cellular Glass	1.5	1.5	1.5	1.5	1.5
	Flexible Elastomeric Cellular	1	1	1	N/A	N/A
Hot Domestic Water Supply & Recirculating Piping (Max 200 F)						
	Mineral Fiber	1	1	1	1.5	1.5
	Cellular Glass	1.5	1.5	1.5	2	2
	Flexible Elastomeric Cellular	1	1	1	N/A	N/A
Refrigerant Suction Piping (35 degrees F nominal)						
	Flexible Elastomeric Cellular	1	1	1	N/A	N/A
	Cellular Glass	1.5	1.5	1.5	1.5	1.5

TABLE 2						
Piping Insulation Thickness (inch) Do not use integral wicking material in Chilled water applications exposed to outdoor ambient conditions in climatic zones 1 through 4.						
Service						
	Material	Tube And Pipe Size (inch)				
		<1	1-<1.5	1.5-<4	4-<8	> or = >8
Exposed Lavatory Drains, Exposed Domestic Water Piping & Drains to Areas for Handicapped Personnel						
	Flexible Elastomeric Cellular	0.5	0.5	0.5	0.5	0.5
Horizontal Roof Drain Leaders (Including Underside of Roof Drain Fittings)						
	Cellular Glass	1.5	1.5	1.5	1.5	1.5
	Flexible Elastomeric Cellular	1	1	1	N/A	N/A
	Faced Phenolic Foam	1	1	1	1	1
Condensate Drain Located Inside Building						
	Cellular Glass	1.5	1.5	1.5	1.5	1.5
	Flexible Elastomeric Cellular	1	1	1	N/A	N/A

3.2.2 Piping Exposed to Weather

Insulate and jacket piping exposed to weather as specified for the applicable service inside the building. After this procedure, apply a laminated self-adhesive (minimum 2 mils adhesive, 3 mils embossed) vapor barrier/weatherproofing jacket - less than 0.0000 permeability (greater than 3 ply, standard grade, silver, white, black and embossed aluminum jacket, stainless steel or PVC jacket.

PVC jacketing requires no factory-applied jacket beneath it, however apply an all service jacket if factory applied jacketing is not furnished. Treat flexible elastomeric cellular insulation exposed to weather in accordance with paragraph INSTALLATION OF FLEXIBLE ELASTOMERIC CELLULAR INSULATION in PART 3.

3.2.2.1 Aluminum Jacket

The jacket for hot piping may be factory applied. Overlap the jacket no less than 2 inches at longitudinal and circumferential joints and secure

with bands at no more than 12 inch centers. Overlap longitudinal joints down to shed water and locate at 4 or 8 o'clock positions. Seal joints on piping 60 degrees F and below with metal jacketing/flashing sealant while overlapping to prevent moisture penetration. Where jacketing on piping 60 degrees F and below abuts an un-insulated surface, caulk joints to prevent moisture penetration. Seal joints on piping above 60 degrees F with a moisture retarder.

3.2.2.2 Insulation for Fittings

Insulate and finish flanges, unions, valves, fittings, and accessories as specified for the applicable service. Apply two coats of breather emulsion type weatherproof mastic (impermeable to water, permeable to air) recommended by the insulation manufacturer with glass tape embedded between coats. Overlap tap no less than 1 inch and the adjoining aluminum jacket no less than 2 inches. Factory preformed aluminum jackets may be used in lieu of the above. Provide molded PVC fitting covers when PVC jackets are used for straight runs of pipe. Provide PVC fitting covers that have adhesive welded joints and are weatherproof laminated self-adhesive (minimum 2 mils adhesive, 3 mils embossed) vapor barrier/weatherproofing jacket - less than 0.0000 permeability, (greater than 3 ply, standard grade, silver, white, black and embossed, and UV resistant.

3.2.2.3 PVC Jacket

Provide ultraviolet resistant PVC jacket that is adhesive welded weather tight with manufacturer's recommended adhesive. Include provision for thermal expansion.

3.2.2.4 Stainless Steel Jackets

ASTM A167 or ASTM A240/A240M; Type 304, minimum thickness of 33 gauge (0.010 inch), smooth surface with factory-applied polyethylene and kraft paper moisture barrier on inside surface. Provide stainless steel bands, minimum width of 1/2 inch.

3.3 DUCT INSULATION SYSTEMS INSTALLATION

Except for oven hood exhaust duct insulation, install corner angles on external corners of insulation on ductwork in exposed finished spaces before covering with jacket. Air conditioned spaces are defined as those spaces directly supplied with cooled conditioned air (or provided with a cooling device such as a fan-coil unit) and heated conditioned air (or provided with a heating device such as a unit heater, radiator or convector).

3.3.1 Duct Insulation Minimum Thickness

Duct insulation minimum thickness in accordance with Table 4.

Table 4 - Minimum Duct Insulation (inches)	
Supply	1.5
Return/Relief	1.0

Table 4 - Minimum Duct Insulation (inches)	
Fresh Air Intake Ducts	2.0
Exterior Ducts	2.0

3.3.2 Insulation and Vapor Retarder/Vapor Barrier for Cold Air Duct

Provide insulation and vapor retarder/vapor barrier for the following cold air ducts and associated equipment.

a. Supply ducts.

b. Return air ducts.

c. Relief ducts.

d. Flexible run-outs (field-insulated).

e. Plenums.

f. Duct-mounted coil casings.

g. Coil headers and return bends.

h. Coil casings.

i. Fresh air intake ducts.

j. Filter boxes.

k. Mixing boxes (field-insulated).

l. Supply fans (field-insulated).

m. Site-erected air conditioner casings.

n. Ducts exposed to weather.

Use insulation for rectangular ducts that is flexible type where concealed, minimum density 3/4 pcf, and rigid type where exposed, minimum density 3 pcf. Provide insulation for both concealed or exposed round/oval ducts that is flexible type, minimum density 3/4 pcf or a semi rigid board, minimum density 3 pcf, formed or fabricated to a tight fit, edges beveled and joints tightly butted and staggered. Provide insulation for all exposed ducts with either a white, paint-able, factory-applied Type I jacket or a field applied vapor retarder/vapor barrier jacket coating finish as specified. Ensure the total field applied dry film thickness is approximately 1/16 inch. Provide insulation on all concealed duct with a factory-applied Type I or II vapor retarder/vapor barrier jacket. Continue duct insulation through sleeves and prepare openings except firewall penetrations. Duct insulation terminating at fire dampers, must be continuous over the damper collar and retaining angle of fire dampers, which are exposed to unconditioned air and which may be prone to condensate formation. Provide duct insulation and vapor retarder/vapor barrier to cover the collar, neck, and un-insulated surfaces of diffusers, registers and grills. Apply vapor retarder/vapor barrier materials to form a complete unbroken vapor seal over the

insulation. Seal sheet metal duct in accordance with Section 23 31 13.00 40 METAL DUCTS.

3.3.2.1 Installation on Concealed Duct

a. For rectangular, oval or round ducts, attach flexible insulation by applying adhesive around the entire perimeter of the duct in 6 inch wide strips on 12 inch centers.

b. For rectangular and oval ducts, 24 inches and larger, additionally secure insulation to bottom of ducts using mechanical fasteners. Space fasteners on 16 inch centers and no more than 16 inches from duct corners.

c. For rectangular, oval and round ducts, provide mechanical fasteners on sides of duct risers for all duct sizes. Space fasteners on 16 inch centers and no more than 16 inches from duct corners.

d. Impale insulation on the mechanical fasteners (self stick pins) where used and press thoroughly into the adhesive. Take care to ensure vapor retarder/vapor barrier jacket joints overlap 2 inches. Do not compress insulation to a thickness less than that specified. Carry insulation over standing seams and trapeze-type duct hangers.

e. Where mechanical fasteners are used, install self-locking washers and trim and bend the pin over.

f. Secure jacket overlaps with staples and tape as necessary to ensure a secure seal. Coat staples, tape and seams with a brush coat of vapor retarder coating or PVDC adhesive tape or greater than 3 ply laminate (minimum 2 mils adhesive, 3 mils embossed) - less than 0.0000 perm adhesive tape.

g. Cover breaks in the jacket material with patches of the same material as the vapor retarder jacket. Do not extend patches less than 2 inches beyond the break or penetration in all directions and secure with tape and staples. Seal staples and tape joints with a brush coat of vapor retarder coating or PVDC adhesive tape or greater than 3 ply laminate (minimum 2 mils adhesive, 3 mils embossed) - less than 0.0000 perm adhesive tape.

h. At jacket penetrations such as hangers, thermometers, and damper operating rods, fill voids in the insulation and seal the penetration with a brush coat of vapor retarder coating or PVDC adhesive tape greater than 3 ply laminate (minimum 2 mils adhesive, 3 mils embossed) - less than 0.0000 perm adhesive tape.

i. Seal insulation terminations and pin punctures and flash with a reinforced vapor retarder coating finish or tape with a brush coat of vapor retarder coating.. Ensure the coating overlaps the adjoining insulation and un-insulated surface 2 inches. Extend pin puncture coatings 2 inches from the puncture in all directions.

j. Where insulation standoff brackets occur, extend insulation under the bracket and terminate the jacket at the bracket.

3.3.2.2 Installation on Exposed Duct Work

a. For rectangular ducts, secure rigid insulation to the duct by

mechanical fasteners on all four sides of the duct, space no more than 12 inches apart and no more than 3 inches from the edges of the insulation joints. Provide a minimum of two rows of fasteners for each side of duct 12 inches and larger. Provide one row for each side of duct less than 12 inches. Provide mechanical fasteners that are corrosion resistant as G60 coated galvanized steel, and indefinitely sustain a 50 lb tensile dead load test perpendicular to the duct wall.

b. Form duct insulation with minimum jacket seams. Fasten each piece of rigid insulation to the duct using mechanical fasteners. When the height of projections is less than the insulation thickness, bring insulation up to standing seams, reinforcing, and other vertical projections and do not carry over. Continue vapor retarder/barrier jacket across seams, reinforcing, and projections. When height of projections is greater than the insulation thickness, carry over insulation and jacket . Apply insulation with joints tightly butted. Neatly bevel insulation around name plates and access plates and doors.

c. Impale insulation on the fasteners; install self-locking washers and trim and bend the pin over.

d. Seal joints in the insulation jacket with a 4 inch wide strip of tape. Seal taped seams with a brush coat of vapor retarder coating.

e. Cover breaks and ribs or standing seam penetrations in the jacket material with a patch of the same material as the jacket. Do not extend patches less than 2 inches beyond the break or penetration and secure with tape and staple. Seal staples and joints with a brush coat of vapor retarder coating.

f. At jacket penetrations such as hangers, thermometers, and damper operating rods, fill the voids in the insulation and seal the penetrations with a flashing sealant.

g. Seal and flash insulation terminations and pin punctures with a reinforced vapor retarder coating finish. Ensure coating overlaps the adjoining insulation and un-insulated surface 2 inches. Extend pin puncture coatings 2 inches from the puncture in all directions.

h. Insulate oval and round ducts, flexible type, with factory Type I jacket insulation with minimum density of 3/4 pcf, attach in accordance with MICA standards.

3.3.3 Insulation for Warm Air Duct

Provide insulation and vapor barrier for the following warm air ducts and associated equipment:.

a. Supply ducts.

b. Return air ducts.

c. Relief air ducts

d. Flexible run-outs (field insulated).

e. Plenums.

f. Duct-mounted coil casings.

g. Coil-headers and return bends.

h. Coil casings.

i. Fresh air intake ducts.

j. Filter boxes.

k. Mixing boxes.

l. Supply fans.

m. Site-erected air conditioner casings.

n. Ducts exposed to weather.

o. Exhaust ducts passing through concealed spaces exhausting conditioned air.

Provide insulation for rectangular ducts that is flexible type where concealed, and rigid type where exposed. Provide insulation on exposed ducts with a white, paint-able, factory-applied Type II jacket, or finish with adhesive finish. Use flexible type insulation for round ducts, with a factory-applied Type II jacket. Provide insulation on concealed duct with a factory-applied Type II jacket. Accomplish adhesive finish where indicated to be used by applying two coats of adhesive with a layer of glass cloth embedded between the coats. Ensure total dry film thickness is approximately 1/16 inch. Continue duct insulation through sleeves and prepare openings. Terminate duct insulation at fire dampers and flexible connections.

3.3.3.1 Installation on Concealed Duct

a. For rectangular, oval and round ducts, attach insulation by applying adhesive around the entire perimeter of the duct in 6 inch wide strips on 12 inch centers.

b. For rectangular and oval ducts 24 inches and larger, secure insulation to the bottom of ducts using mechanical fasteners. Space fasteners on 18 inch centers and no more than 18 inches from duct corner.

c. For rectangular, oval and round ducts, provide mechanical fasteners on sides of duct risers for all duct sizes. Space fasteners on 18 inch centers and no more than 18 inches from duct corners.

d. Impale insulation on the mechanical fasteners where used. Do not compress insulation to a thickness less than that specified. Carry insulation over standing seams and trapeze-type hangers.

e. Install self-locking washers where mechanical fasteners are used and trim and bend the pin over.

f. Do not overlap insulation jacket less than 2 inches at joints and secure the lap and staple on 4 inch centers.

3.3.3.2 Installation on Exposed Duct

a. For rectangular ducts, secure the rigid insulation to the duct using

mechanical fasteners on all four sides of the duct, space no more than 16 inches apart and no more than 6 inches from the edges of the insulation joints. Provide a minimum of two rows of fasteners for each side of duct 12 inches and larger and a minimum of one row for each side of duct less than 12 inches.

b. Form duct insulation with factory-applied jacket with minimum jacket seams, and fasten each piece of rigid insulation to the duct using mechanical fasteners. When the height of projection is less than the insulation thickness, bring insulation up to standing seams, reinforcing, and other vertical projections and do not carry over the projection. Continue jacket across seams, reinforcing, and projections. Where the height of projections is greater than the insulation thickness, carry insulation and jacket over the projection.

c. Impale insulation on the fasteners; install self-locking washers and trim and bend the pin over.

d. Seal joints on jacketed insulation with a 4 inch wide strip of tape and brush with vapor retarder coating.

e. Cover breaks and penetrations in the jacket material with a patch of the same material as the jacket. Extend patches no less than 2 inches beyond the break or penetration and secure with adhesive and staple.

f. Seal insulation terminations and pin punctures with tape and brush with vapor retarder coating.

g. Insulate oval and round ducts, flexible type, with factory Type I jacket insulation, minimum density of 3/4 pcf attach by staples spaced no more than 16 inches and no more than 6 inches from the degrees of joints. Seal joints in accordance with item "d." above.

3.3.4 Insulation for Evaporative Cooling Duct

Insulate evaporative cooling supply duct located in spaces not evaporatively cooled. Use material and installation requirements as specified for duct insulation for warm air duct.

3.3.5 Duct Test Holes

After duct systems have been tested, adjusted, and balanced, repair breaks in the insulation and jacket in accordance with the applicable section of this specification for the type of duct insulation to be repaired.

3.3.6 Duct Exposed to Weather

3.3.6.1 Installation

Insulate and finish ducts exposed to weather as specified for the applicable service for exposed duct inside the building. After the above is accomplished, further finish the insulation as detailed in the following subparagraphs.

3.3.6.2 Round Duct

Laminated self-adhesive (minimum 2 mils adhesive, 3 mils embossed) vapor barrier/weatherproofing jacket - Less than 0.0000 permeability, (greater than 3 ply, standard grade, silver, white, black and embossed or greater

than 8 ply, heavy duty, white and natural) membrane must be applied overlapping material by 3 inches no bands or caulking needed - see manufacturer's recommended installation instructions. Aluminum jacket with factory applied moisture retarder must be applied with the joints lapped no less than 3 inches and secured with bands located at circumferential laps and at no more than 12 inch intervals throughout. Lap horizontal joints down to shed water and located at 4 or 8 o'clock position. Seal joints with metal jacketing sealant to prevent moisture penetration. Where jacketing abuts an un-insulated surface, seal joints with metal jacketing sealant.

3.3.6.3 Fittings

Finish fittings and other irregular shapes as specified for rectangular ducts.

3.3.6.4 Rectangular Ducts

Apply two coats of weather barrier mastic reinforced with fabric or mesh for outdoor application to the entire surface. Ensure each coat of weatherproof mastic has a minimum thickness of 1/16 inch. Ensure exterior is a metal jacketing applied for mechanical abuse and weather protection, and secure with screws or vapor barrier/weatherproofing jacket less than 0.0000 permeability greater than 3 ply, standard grade, silver, white, black, and embossed or greater than 8 ply, heavy duty white and natural. Apply membrane overlapping material by 3 inches. No bands or caulking needed-see manufacturing recommend installation instructions.

3.4 EQUIPMENT INSULATION SYSTEMS INSTALLATION

3.4.1 Insulation for Hot Equipment

3.4.1.1 Other Equipment

a. Form or fabricate insulation to fit the equipment. To ensure a tight fit on round equipment, bevel edges and tightly butt and stagger joints.

b. Secure insulation in place with bands or wires at intervals as recommended by the manufacturer but no greater than 12 inch centers except adhere flexible elastomeric cellular. Protect insulation corners under wires and bands with suitable corner angles.

c. On high vibration equipment, set cellular glass insulation in a coating of bedding compound as recommended by the manufacturer, and seal joints with bedding compound. Fill mineral fiber joints with finishing cement.

d. Provide removable insulation on heads of heat exchangers. Fabricate the removable section joint using a male-female shiplap type joint. Finish the entire surface of the removable section as specified.

e. Protect exposed insulation corners with corner angles.

f. On equipment with ribs, such as boiler flue gas connection, draft fans, and fly ash or soot collectors, apply insulation over 6 by 6 inch by 12 gauge welded wire fabric which has been cinched in place, or if approved by the Contracting Officer, spot weld to the equipment over the ribs. Secure insulation to the fabric with J-hooks and 2 by 2 inch

washers or securely band or wire in place on 12 inch (maximum) centers.

g. Upon completion of installation of insulation, caulk penetrations. Apply two coats of adhesive over insulation, including removable sections, with a layer of glass cloth embedded between the coats. The total dry thickness of the finish must be 1/16 inch. Apply caulking to parting line between equipment and removable section insulation.

3.4.2 Equipment Handling Dual Temperature Media

Below and above 60 degrees F: insulate equipment handling dual temperature media as specified for cold equipment.

3.4.3 Equipment Exposed to Weather

3.4.3.1 Installation

Insulate equipment exposed to weather and finish in accordance with the requirements for ducts exposed to weather in paragraph DUCT INSULATION INSTALLATION.

3.4.3.2 Optional Panels

At the option of the Contractor, prefabricated metal insulation panels may be used in lieu of the insulation and finish previously specified. Thermal performance must be equal to or better than that specified for field applied insulation. Provide panels that are the standard catalog product of a manufacturer of metal insulation panels. Provide fastenings, flashing, and support system conforming to published recommendations of the manufacturer for weatherproof installation and that prevent moisture from entering the insulation. Design panels to accommodate thermal expansion and to support a 250 pound walking load without permanent deformation or permanent damage to the insulation. Exterior metal cover sheet must be aluminum and exposed fastenings must be stainless steel or aluminum.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 08 00.00 20

COMMISSIONING OF MECHANICAL AND PLUMBING SYSTEMS

PART 1 GENERAL

1.1 DEFINITIONS
1.2 SEQUENCING AND SCHEDULING
1.3 SUBMITTALS
1.4 ACCESSIBILITY REQUIREMENTS
1.5 COORDINATION
1.6 PIPE FLUSHING, TESTING, AND WATER TREATMENT REPORTS
1.7 CERTIFICATE OF READINESS DOCUMENTATION

PART 2 PRODUCTS

2.1 TEST EQUIPMENT
2.1.1 Proprietary Equipment
2.1.2 Calibration and Accuracy

PART 3 EXECUTION

3.1 MEETINGS
3.2 PREFUNCTIONAL CHECKS
3.3 STARTUP AND INITIAL CHECKOUT
3.4 COMMISSIONING TESTING
3.4.1 Preparation
3.4.2 Test Setup
3.4.3 Manufacturer's Representative
3.4.4 Sample Strategy
3.4.5 Simulating Conditions
3.4.6 Duct Air Leakage Test (DALT) Report Review
3.4.7 Duct Air Leakage Test (DALT) Report Verification
3.4.8 Testing, Adjusting, and Balancing (TAB) Report Review
3.4.9 Testing, Adjusting, and Balancing (TAB) Report Verification
3.4.10 HVAC Controls Test Procedures, Reports, and Trends Review
3.5 RETESTING REQUIREMENTS
3.6 SYSTEM ACCEPTANCE
3.7 SEASONAL TESTS
3.8 FULL-LOAD TESTS
3.9 TRAINING

-- End of Section Table of Contents --

SECTION 23 08 00.00 20

COMMISSIONING OF MECHANICAL AND PLUMBING SYSTEMS

PART 1 GENERAL

Total Building Commissioning (TBCx) is a systematic, quality-focused process for enhancing the delivery of a project that focuses on verifying and documenting that all of the commissioned systems and assemblies are planned, designed, installed, tested, operated, and maintained to meet the project requirements. The purpose is to reduce the cost and performance risks associated with delivering facilities projects, and to increase value to owners, occupants, and users.

1.1 DEFINITIONS

Commissioning Process (Cx) - a quality-focused process for enhancing the delivery of a project. Refer to ASHRAE 202 for a comprehensive description of the commissioning process.

Commissioning Provider (CxC)- The entity hired by the Government, who leads, plans, and coordinates the Commissioning Team. The terms Commissioning Provider, Commissioning Firm, Lead Commissioning Specialist, Commissioning Specialist, and Commissioning Authority (CA or CxA) when used by sustainable Third Party Certification (TPC) programs, are interchangeable.

Commissioning Authority - The Government retains the authority for oversight and assurance of the entire commissioning process, and final approval of all commissioning deliverables.

Government Acceptance Testing Representatives - Government Acceptance Testing Representatives perform the inherently Governmental function of technical oversight and quality assurance for critical systems, and is distinctly separate from the commissioning process. Government Acceptance Testing Representatives witness final testing of critical systems and report systems' acceptance to the COR. Submittals to be surveilled and approved by Government Acceptance Testing Representatives are identified in Section 01 33 00 SUBMITTAL PROCEDURES. Testing required to be witnessed by Government Acceptance Testing Representatives are indentified in system level sections.

1.2 SEQUENCING AND SCHEDULING

Complete functional performance testing prior to performance verification testing required by Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC. Complete the following prior to starting Functional Performance Tests of mechanical systems:

a. All equipment and systems completed, cleaned, flushed, disinfected, calibrated, tested, and operate in accordance with contract documents and construction plans and specifications

b. Final DALT Report submitted and approved in accordance with Section 23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC

c. Performance Verification Tests of the controls systems have been completed and the Performance Verification Test Report has been submitted and approved in accordance with Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC.

d. The Certificate of Readiness submitted and approved in accordance with Section 01 91 00.15 10 TOTAL BUILDING COMMISSIONING

e. Pre-final Testing, Adjusting, and Balancing Report submitted in accordance with Section 23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC

f. Air Leakage Test Reports and Diagnostic Test Reports submitted and approved in accordance with Section 07 27 10 BUILDING AIR BARRIER SYSTEM.

g. Tests, Flushing, and Disinfection in accordance with Section 22 00 00 PLUMBING, GENERAL PURPOSE

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-03 Product Data

Test Equipment; G

SD-06 Test Reports

Pipe Flushing, Testing, And Water Treatment Reports; G

Seasonal Test Report; G

Full-Load Test Report; G

1.4 ACCESSIBILITY REQUIREMENTS

Equipment, systems, and devices for commissioned systems must be accessible. Make necessary modifications if systems and devices are not accessible for inspections and testing.

Assist commissioning team in testing by removing equipment covers, opening access panels, and other required activities that assist with visual oversight. Furnish ladders, flashlights, meters, gauges, or other inspection equipment as necessary.

1.5 COORDINATION

Refer to Section 01 91 00.15 10 TOTAL BUILDING COMMISSIONING for requirements pertaining to coordination during the commissioning process. Coordinate with the Commissioning Provider in accordance with Section 01 91 00.15 10 and in accordance with the Commissioning Plan to schedule inspections as required to support the commissioning process. Furnish additional information requested by the Commissioning Provider. Coordinate scheduling of Functional Performance Testing with the commissioning team. Upload plans, reports, notes, and other documentation

to the Commissioning Provider's web-based commissioning software, or as specified in the commissioning plan, as it is completed.

1.6 PIPE FLUSHING, TESTING, AND WATER TREATMENT REPORTS

Test requirements are specified in Division 22 and 23 piping Sections. Prepare a pipe system cleaning, flushing, and hydrostatic testing log. Provide cleaning, flushing, testing, and water treatment log and final reports.

Include the following in the pipe system cleaning, flushing, and hydrostatic testing log:

a. Minimum flushing water velocity.

b. Water treatment reports.

c. Tracking checklist for managing and ensuring that all pipe sections have been cleaned, flushed, hydrostatically tested, and chemically treated.

1.7 CERTIFICATE OF READINESS DOCUMENTATION

Submit Certificate of Readiness documentation in accordance with Section 01 91 00.15 10 TOTAL BUILDING COMMISSIONING for all equipment and systems including start-up reports; completed Pre-Functional Checklists; Testing, Adjusting, and Balancing (TAB) Report; HVAC Controls Start-Up Reports. Do not schedule Functional Performance Tests for the system until the Certificate of Readiness for that system receives approval by the Contracting Officer. The Mechanical, Electrical, Controls, and TAB subcontractor representatives must sign and date the Certificate of Readiness.

PART 2 PRODUCTS

2.1 TEST EQUIPMENT

Provide all testing equipment required to perform testing for the systems to be commissioned, except for equipment specific to and used by TAB as required by Section 23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC. Provide a sufficient quantity of two-way radios for each subcontractor. Submit list of Test Equipment and instrumentation to be used for testing including equipment/instrument identification number, equipment application or planned use, manufacturer, make, model, and serial number, and calibration history with certificates. Also list special equipment and proprietary tools specific to a piece of equipment required for testing.

2.1.1 Proprietary Equipment

Provide manufacturer's proprietary test equipment and software required by any equipment manufacturer for programming and/or start-up, whether specified or not. Provide manufacturer test equipment, demonstrate its use, and assist in the commissioning process as needed. Provide data logging equipment and software required to test equipment.

2.1.2 Calibration and Accuracy

Comply with equipment manufacturer's test equipment calibration procedures

and intervals. Recalibrate test instruments immediately after instruments have been repaired resulting from being dropped or damaged. Affix calibration tags to test instruments. Furnish calibration records to Contracting Officer upon request.

Provide all testing equipment of sufficient quality and accuracy to test and/or measure system performance with the tolerances specified. Unless otherwise noted, the following minimum requirements apply: Provide temperature sensors and digital thermometers with a certified calibration within the past year to an accuracy of 0.5 degrees F and a resolution of plus or minus 0.1 degrees F. Provide pressure sensors with an accuracy of plus or minus 2.0 percent of the value range being measured (not full range of meter) and calibrated within the last year.

PART 3 EXECUTION

3.1 MEETINGS

Attend all meetings in accordance with Section 01 91 00.15 10 TOTAL BUILDING COMMISSIONING.

Provide timely updates on construction schedule changes so Commissioning Provider has scheduling information needed to execute commissioning process efficiently. Notify Contracting Officer of anticipated construction delays to commissioning activities not yet performed or not yet scheduled.

3.2 PREFUNCTIONAL CHECKS

Complete and sign Pre-Functional Checklists using the Commissioning Provider's web-based commissioning software, or as specified by the commissioning plan. Provide manufacturer's installation manual for each type of unit. Perform all work in accordance with the manufacturer's published diagrams, recommendations, and equipment warranty requirements.

3.3 STARTUP AND INITIAL CHECKOUT

Document start-up and initial testing procedures including:

a. Startup tests and factory testing reports.

b. Manufacturer's representative start-up, operating, troubleshooting and maintenance procedures.

c. Additional documentation necessary for third party certification programs.

d. Perform and clearly document system operational checks and quality control checks as they are completed, and providing a copy to the commissioning team.

e. Correct deficiencies and sign the Certificate of Readiness for each system before functional performance testing

3.4 COMMISSIONING TESTING

Conduct Functional Performance Testing in accordance with Section 01 91 00.15 10 01 91 00.15 20 TOTAL BUILDING COMMISSIONING and requirements in this section. Prior to Functional Performance Testing,

complete all prerequisites in accordance with paragraph SEQUENCING AND SCHEDULING.

3.4.1 Preparation

Put equipment and systems into operation and continue operation during each working day of commissioning, as required. Verify temperature and pressure taps in accordance with Contract Documents. Provide a pressure/temperature plug at each water sensor which is an input point to control system.

Perform minor adjustments to equipment and systems during Functional Performance Tests as deemed necessary by the commissioning team. Where calibrated DDC sensors cannot be used to record test data, provide measuring instruments, logging devices, and data acquisition equipment to record data for the complete range of test data for the required test period.

3.4.2 Test Setup

Perform each test under conditions that simulate actual conditions as close as is practically possible. Provide all necessary materials and system modifications to produce the necessary flows, pressures, temperatures, and other conditions necessary to execute the test according to the specified conditions. At completion of the test, return the affected building equipment and systems to their pre-test condition.

3.4.3 Manufacturer's Representative

Provide a factory trained representative authorized by the equipment manufacturer to perform Functional Performance Testing for the following equipment:

Packaged Direct-Expansion Refrigeration Equipment, including variable refrigerant flow (VRF) systems

Ensure the test representative reviews, approves, and signs the completed field test report. Include person's name with signatures.

3.4.4 Sample Strategy

Perform Functional Performance Tests using the sample strategy described in Section 01 91 00.15 10 TOTAL BUILDING COMMISSIONING. Prepare and complete a Functional Performance Test for each item of equipment or system to be tested. During testing, Government representatives may select the specific equipment or system to be tested for sample sizes less than 100 percent.

3.4.5 Simulating Conditions

Functional performance testing is conducted by simulating conditions at control devices to initiate a control system response. Before testing, calibrate all sensors, transducers and devices. Over-writing control input values through the control system is not acceptable unless approved by the Contracting Officer. Specific examples of simulating conditions are provided below. Do not simulate conditions when damage to the system or building may result.

a. When varying static pressures inside ductwork cannot be simulated

within the duct, and where a sensor signals the controls system to initiate sequences at various duct static pressures, it is acceptable to simulate the various pressures with a Pneumatic Squeeze-Bulb Type Signaling Device with gauge temporarily attached to the sensing tube leading to the transmitter. It is not acceptable to reset the various set-points, nor to simulate an electric analog signal (unless approved as noted above).

b. Dirty filter pressure drops can be simulated by partially blocking filter face.

c. Freeze-stat safeties can be simulated by packing portion of sensor with ice.

d. High outside air temperatures can be simulated with a hair blower.

e. Raising entering cooling coil temperatures by activating a heating/preheat coil can be used to simulate entering cooling coil conditions.

f. Do not use signal generators to simulate sensor signals unless approved by the Contracting Officer, as noted above, for special cases.

g. Control set points can be altered. For example, to see the air conditioning compressor lockout work at an outside air temperature below 55 degrees F, when the outside air temperature is above 55 degrees F, temporarily change the lockout set point to be 0 degrees F above the current outside air temperature. Caution: Set points are not to be raised or lowered to a point to cause damage to the components, systems, or the building structure and/or contents.

h. Test duct mounted smoke detectors in accordance with the manufacturer's recommendations. Perform the tests with air system at minimum airflow condition.

i. Test current sensing relays used for fan and pump status signals to control system to indicate unit failure and run status by resetting the set point on the relay to simulate a lost belt or unit failure while the unit is running. Confirm that the failure alarm was generated and received at the control system. After the test is conducted, return the set point to its original set-point or a set-point as indicated by the Contracting Officer.

3.4.6 Duct Air Leakage Test (DALT) Report Review

The Mechanical System Technical Commissioning Specialist must review the pre-final TAB Report required by Section 23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC. Identify any deficiencies to the Contracting Officer's Representative and the Contractor's Quality Control Personnel and include in the issues log. The Commissioning Specialist is responsible for reviewing the pre-final TAB Report required by Section 23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC and identifying any deficiencies to the Contracting Officer's Representative and the Contractor's Quality Control Personnel. All deficiencies must be resolved prior to DALT Report approval.

3.4.7 Duct Air Leakage Test (DALT) Report Verification

The Mechanical System Technical Commissioning Specialist must witness the

DALT Field Acceptance Testing specified by Section 23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC and identify any deficiencies to the Contracting Officer's Representative and the Contractor's Quality Control Personnel and include in the issues log. The Commissioning Specialist is responsible for witnessing the DALT Field Acceptance Testing specified by Section 23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC and identifying any deficiencies to the Contracting Officer's Representative and the Contractor's Quality Control Personnel. All deficiencies must be resolved prior to DALT Report approval.

3.4.8 Testing, Adjusting, and Balancing (TAB) Report Review

The Mechanical System Technical Commissioning Specialist must review the pre-final TAB Report required by Section 23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC and identify any deficiencies to the Contracting Officer's Representative and the Contractor's Quality Control Personnel and include in the issues log. The Commissioning Specialist is responsible for reviewing the pre-final TAB Report required by Section 23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC and identifying any deficiencies to the Contracting Officer's Representative and the Contractor's Quality Control Personnel. All deficiencies must be resolved prior to TAB Report approval.

3.4.9 Testing, Adjusting, and Balancing (TAB) Report Verification

The Mechanical System Technical Commissioning Specialist must witness the TAB Field Acceptance Testing specified by Section 23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC and identify any deficiencies to the Contracting Officer's Representative and the Contractor's Quality Control Personnel and include in the issues log. The Commissioning Specialist is responsible for witnessing the TAB Field Acceptance Testing specified by Section 23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC and identifying any deficiencies to the Contracting Officer's Representative and the Contractor's Quality Control Personnel. All deficiencies must be resolved prior to TAB Report approval.

3.4.10 HVAC Controls Test Procedures, Reports, and Trends Review

The Mechanical System Technical Commissioning Specialist must review the Start-Up Testing Report, PVT Procedures and PVT Reports including endurance testing trend submittals required by Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC. The Mechanical System Technical Commissioning Specialist must review each submittal and identify any deficiencies to the Contracting Officer's Representative and the Contractor's Quality Control Personnel and include in the issues log. The Commissioning Specialist is responsible for reviewing the Start-Up Testing Report, PVT Procedures and PVT Reports including endurance testing trend data required by Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC and identifying any deficiencies to the Contracting Officer's Representative and the Contractor's Quality Control Personnel. All deficiencies must be resolved prior to final acceptance.

3.5 RETESTING REQUIREMENTS

Abort tests if any deficiency prevents successful completion of the test or if any required commissioning team member is not present for the test. Re-test only after all deficiencies identified during the original tests have been corrected.

If sequence of operation in any of Functional Performance Tests fails, the Government's costs for witnessing further demonstration of that test procedure may be assigned to the Contractor as a deduct to their contracted price, including salary, travel costs, and per diem for Government commissioning team members. Correct deficiencies as identified by the commissioning team and retest the systems to be commissioned.

3.6 SYSTEM ACCEPTANCE

Systems may be partially accepted prior to seasonal testing if they comply with all construction contract and accepted design requirements that can be tested during initial Functional Performance Tests. All test procedures must be successful completed prior to full systems acceptance.

3.7 SEASONAL TESTS

Perform Initial Functional Performance Tests as soon as all contract work is completed, but prior to facility turnover, regardless of the season.

In addition to the Initial Functional Performance Tests, perform Functional Performance Tests of HVAC systems during season of maximum heating and cooling as defined by Section 23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC. Schedule Seasonal Functional Performance Tests in coordination with the Contracting Officer. Submit Seasonal Test Report within 14 days of test completion.

Execute seasonal functional performance testing, witnessed by the Contracting Officer. Correct deficiencies and make adjustments to O&M manuals and as-built drawings for applicable issues identified in any seasonal testing.

3.8 FULL-LOAD TESTS

Perform Initial Functional Performance Tests as soon as all contract work is completed, but prior to facility turnover. In addition to the Initial Functional Performance Tests, perform Functional Performance Tests of HVAC systems under full-load conditions. Schedule Full-Load Functional Performance Tests in coordination with the Contracting Officer. Submit Full-Load Test Report within 14 days of test completion.

Execute full-load functional performance testing, witnessed by the Contracting Officer. Correct deficiencies and make adjustments to O&M manuals and as-built drawings for applicable issues identified in any full load testing.

3.9 TRAINING

The Mechanical Systems Technical Commissioning Specialist must review the training plan required by Section 01 78 00 OPERATION AND MAINTENANCE DATA and identify any deficiencies to the Contracting Officer's Representative and the Contractor's Quality Control Personnel.

The Commissioning Provider is responsible for overseeing and approving the training plan required by Section 01 78 00 OPERATION AND MAINTENANCE DATA and identifying any deficiencies to the Contracting Officer's Representative and the Contractor's Quality Control Personnel.

Coordinate, schedule, and document all required training. At a minimum, include the following items in the training report for commissioned

systems:

a. Complete commissioning documentation

b. Complete O&M data

c. Complete Training

d. Purpose of equipment.

e. Principle of how the equipment works.

f. Important parts and assemblies.

g. How the equipment achieves its purpose and necessary operating conditions.

h. Most likely failure modes, causes and corrections.

i. On site demonstration.

j. Provide updates to O&M manuals based on field modifications.

k. Provide training of the post-occupancy operations and maintenance staff.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 09 00

INSTRUMENTATION AND CONTROL FOR HVAC

PART 1 GENERAL

1.1 SUMMARY
1.1.1 Proprietary Systems
1.1.1.1 Proprietary Systems Exempted From Open Protocol Requirements
1.1.1.2 Implementation of Proprietary Systems
1.1.1.3 Proprietary Multi-Split Engineering Tool Software
1.1.2 System Requirements
1.1.3 End to End Accuracy
1.1.4 Verification of Dimensions
1.1.5 Drawings
1.2 RELATED SECTIONS
1.3 REFERENCES
1.4 DEFINITIONS
1.4.1 Alarm Generation (All protocols)
1.4.2 Building Automation and Control Network (BACnet) (BACnet)
1.4.3 BACnet Advanced Application Controller (B-AAC) (BACnet)
1.4.4 BACnet Application Specific Controller (B-ASC) (BACnet)
1.4.5 BACnet Building Controller (B-BC) (BACnet)
1.4.6 BACnet Broadcast Management Device (BBMD) (BACnet)
1.4.7 BACnet/IP (BACnet)
1.4.8 BACnet Internetwork (BACnet)
1.4.9 BACnet Interoperability Building Blocks (BIBBs) (BACnet)
1.4.10 BACnet Network (BACnet)
1.4.11 BACnet Operator Display (B-OD) (BACnet)
1.4.12 BACnet Segment (BACnet)
1.4.13 BACnet Smart Actuator (B-SA) (BACnet)
1.4.14 BACnet Smart Sensor (B-SS) (BACnet)
1.4.15 BACnet Testing Laboratories (BTL) (BACnet)
1.4.16 BACnet Testing Laboratories (BTL) Listed (BACnet)
1.4.17 Binary (All protocols)
1.4.18 Broadcast (BACnet)
1.4.19 Building Control Network (BCN) (All protocols)
1.4.20 Building Point of Connection (BPOC) (All protocols)
1.4.21 Commandable (All protocols)
1.4.22 Commandable Objects (BACnet)
1.4.23 Configurable (All protocols)
1.4.24 Control Logic Diagram (All protocols)
1.4.25 Device (BACnet)
1.4.26 Device Object (BACnet)
1.4.27 Device Profile (BACnet)
1.4.28 Digital Controller (All protocols)
1.4.29 Direct Digital Control (DDC) (All protocols)
1.4.30 Field Point of Connection (FPOC) (All protocols)
1.4.31 Fox Protocol (Niagara Framework)

1.4.32 Gateway (All protocols)
1.4.33 IEEE 802.3 Ethernet (All protocols)
1.4.34 Internet Protocol (IP, TCP/IP, UDP/IP) (All protocols)
1.4.35 Input/Output (I/O) (All protocols)
1.4.36 I/O Expansion Unit (All protocols)
1.4.37 IP subnet (All protocols)
1.4.38 JACE (Niagara Framework)
1.4.39 Local-Area Network (LAN) (All protocols)
1.4.40 Local Display Panels (LDPs) (All protocols)
1.4.41 MAC Address (All protocols)
1.4.42 Master-Slave/Token-Passing (MS/TP) (BACnet)
1.4.43 Monitoring and Control (M&C) Software (All protocols)
1.4.44 Network Number (BACnet)
1.4.45 Niagara Framework (Niagara Framework)
1.4.46 Niagara Framework Supervisory Gateway (Niagara Framework)
1.4.47 Object (BACnet)
1.4.48 Object Identifier (BACnet)
1.4.49 Object Instance (BACnet)
1.4.50 Object Properties (BACnet)
1.4.51 Operator Configurable (All protocols)
1.4.52 Override (All protocols)
1.4.53 Packaged Equipment (All protocols)
1.4.54 Packaged Unit (All protocols)
1.4.55 Performance Verification Test (PVT) (All protocols)
1.4.56 Physical Segment (BACnet)
1.4.57 Polling (All protocols)
1.4.58 Points (All protocols)
1.4.59 Proportional, Integral, and Derivative (PID) Control Loop (All protocols)
1.4.60 Proprietary (BACnet)
1.4.61 Protocol Implementation Conformance Statement (PICS) (BACnet)
1.4.62 Repeater (All protocols)
1.4.63 Router (All protocols)
1.4.64 Segment (All protocols)
1.4.65 Standard BACnet Objects (BACnet)
1.4.66 Standard BACnet Properties (BACnet)
1.4.67 Standard BACnet Services (BACnet)
1.4.68 UMCS (All protocols)
1.4.69 UMCS Network (All protocols)
1.4.70 Writable Property (BACnet)
1.5 PROJECT SEQUENCING
1.6 SUBMITTALS
1.7 DATA PACKAGE AND SUBMITTAL REQUIREMENTS
1.8 SOFTWARE FOR DDC HARDWARE AND GATEWAYS
1.8.1 Configuration Software
1.8.2 Controller Configuration Settings
1.8.3 Programming Software
1.8.4 Controller Application Programs
1.8.5 Niagara Framework Supervisory Gateway Backups
1.8.6 Niagara Framework Engineering Tool(for all Niagara Framework system)
1.9 QUALITY CONTROL CHECKLISTS
1.9.1 Pre-Construction Quality Control (QC) Checklist
1.9.2 Post-Construction Quality Control (QC) Checklist
1.9.3 Closeout Quality Control (QC) Checklist

PART 2 PRODUCTS

2.1 GENERAL PRODUCT REQUIREMENTS

2.2 PRODUCT DATA
2.3 OPERATION ENVIRONMENT
2.4 WIRELESS CAPABILITY
2.5 ENCLOSURES
2.5.1 Outdoors
2.5.2 Mechanical and Electrical Rooms
2.5.3 Other Locations
2.6 WIRE AND CABLE
2.6.1 Terminal Blocks
2.6.2 Control Wiring for Binary Signals
2.6.3 Control Wiring for Analog Signals
2.6.4 Power Wiring for Control Devices
2.6.5 Transformers

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Dielectric Isolation
3.1.2 Penetrations in Building Exterior
3.1.3 Device Mounting Criteria
3.1.4 Labels and Tags
3.1.5 Surge Protection
3.1.5.1 Power-Line Surge Protection
3.1.5.2 Surge Protection for Transmitter and Control Wiring
3.1.6 Basic Cybersecurity Requirements
3.1.6.1 Passwords
3.1.6.2 Wireless Capability
3.1.6.3 IP Network Physical Security
3.2 DRAWINGS AND CALCULATIONS
3.2.1 Sample Drawings
3.2.2 Drawing Index and Legend
3.2.3 Thermostat and Occupancy Sensor Schedule
3.2.4 Damper Schedule
3.2.5 Project Summary Equipment Schedule
3.2.6 Equipment Schedule
3.2.7 Occupancy Schedule
3.2.8 DDC Hardware Schedule
3.2.8.1 DDC Hardware Identifier
3.2.8.2 HVAC System
3.2.8.3 BACnet Device Information
3.2.8.3.1 Device Object Identifier
3.2.8.3.2 Network Number
3.2.8.3.3 MAC Address
3.2.8.3.4 BTL Listing
3.2.8.3.5 Proprietary Services Information
3.2.8.3.6 Alarming Information
3.2.8.3.7 Scheduling Information
3.2.8.3.8 Trending Information
3.2.8.4 Niagara Station ID
3.2.9 Points Schedule
3.2.9.1 Point Name
3.2.9.2 Description
3.2.9.3 DDC Hardware Identifier
3.2.9.4 Settings
3.2.9.5 Range
3.2.9.6 Input or Output (I/O) Type
3.2.9.7 Object and Property Information
3.2.9.8 Niagara Station ID
3.2.9.9 Network Data Exchange Information (Gets Data From, Sends

Data To)
3.2.9.10 Override Information (Object Type and Instance Number)
3.2.9.11 Trend Object Information
3.2.9.12 Alarm Information
3.2.9.13 Configuration Information
3.2.10 Riser Diagram
3.2.11 Control System Schematics
3.2.12 Sequences of Operation
3.2.13 Controller, Motor Starter and Relay Wiring Diagram
3.3 CONTROLLER TUNING
3.4 START-UP
3.4.1 Start-Up Test
3.4.1.1 Systems Check
3.4.1.1.1 Step 1 - System Inspection
3.4.1.1.2 Step 2 - Calibration Accuracy Check
3.4.1.1.3 Step 3 - Actuator Range Check
3.4.1.2 Weather Dependent Test
3.4.2 Start-Up Testing Report
3.5 PERFORMANCE VERIFICATION TEST (PVT)
3.5.1 PVT Procedures
3.5.1.1 Sensor Accuracy Checks
3.5.1.2 Endurance Test
3.5.1.3 PVT Equipment List
3.5.2 PVT Execution
3.5.3 PVT Report
3.6 OPERATION AND MAINTENANCE (O&M) INSTRUCTIONS
3.7 TRAINING
3.7.1 Training Documentation
3.7.2 Training Course Content
3.7.3 Training Documentation Submittal Requirements

ATTACHMENTS:

QC Checklist for BACnet Systems

QC Checklist for Niagara Framework Based BACnet Systems

QC CHECKLIST FOR BACNET SYSTEMS

QC CHECKLIST FOR NIAGARA FRAMEWORK BASED BACNET SYSTEMS

-- End of Section Table of Contents --

SECTION 23 09 00

INSTRUMENTATION AND CONTROL FOR HVAC

PART 1 GENERAL

1.1 SUMMARY

Provide a complete Direct Digital Control (DDC) system suitable for the control of the heating, ventilating and air conditioning (HVAC) and other building-level systems as indicated and shown and in accordance with Section 23 09 13 INSTRUMENTATION AND CONTROL DEVICES FOR HVAC, Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS for BACnet or Niagara BACnet systems, and other referenced Sections.

1.1.1 Proprietary Systems

1.1.1.1 Proprietary Systems Exempted From Open Protocol Requirements

The following systems are specifically exempted from the open protocol requirements of Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS:

a. A simple split (DX) system consisting of a single indoor unit and a single outdoor unit from the same manufacturer.

1.1.1.2 Implementation of Proprietary Systems

For proprietary systems exempted from open protocol requirements, a proprietary network and DDC hardware communicating via proprietary protocol are permitted. For these systems a building control network meeting the requirements of Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS must also be provided, along with a gateway or interface to connect the proprietary system to the open building control network.

The proprietary system gateway or interface must provide the required functionaliality as shown on the points schedule. Scheduling, alarming, trending, overrides, network inputs, network outputs and other protocol related requirements must be met on the open protocol control system as specified in Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS.

1.1.1.3 Proprietary Multi-Split Engineering Tool Software

For each permitted proprietary systems in Table 1 shown as requiring Proprietary Multi-Split Engineering Tool Software, provide the software needed to replace a unit and configure the replacement. Submit hard copies of the software user manuals with the software submittal.

Submit Proprietary Multi-Split Engineering Tool Software on CD-ROM as a Technical Data Package. Submit 3 hard copies of the software user manual for each piece of software.

1.1.2 System Requirements

Provide systems meeting the requirements this Section and other Sections referenced by this Section, and which have the following characteristics:

a. The system implements the control sequences of operation shown in the Contract Drawings using DDC hardware to control mechanical and electrical equipment

b. The system meet the requirements of this specification as a stand-alone system and does not require connection to any other system.

c. Control sequences reside in DDC hardware in the building. The building control network is not dependent upon connection to a Utility Monitoring and Control System (UMCS) Front End or to any other system for performance of control sequences. To the greatest extent practical, the hardware performs control sequences without reliance on the building network, unless otherwise pre-approved by the Contracting Officer.

d. The hardware is installed such that individual control equipment can be replaced by similar control equipment from other equipment manufacturers with no loss of system functionality.

e. All necessary documentation, configuration information, programming tools, programs, drivers, and other software are licensed to and otherwise remain with the Government such that the Government or their agents are able to perform repair, replacement, upgrades, and expansions of the system without subsequent or future dependence on the Contractor, Vendor or Manufacturer.

f. Sufficient documentation and data, including rights to documentation and data, are provided such that the Government or their agents can execute work to perform repair, replacement, upgrades, and expansions of the system without subsequent or future dependence on the Contractor, Vendor or Manufacturer.

g. Hardware is installed and configured such that the Government or their agents are able to perform repair, replacement, and upgrades of individual hardware without further interaction with the Contractor, Vendor or Manufacturer.

h. All Niagara Framework components have an unrestricted interoperability license with a Niagara Compatibility Statement (NiCS) following the Tridium Open NiCS Specification and have a value of "ALL" for "Station Compatibility In", "Station Compatibility Out", "Tool Compatibility In" and "Tool Compatibility Out". Note that this will result in the following entries in the license file:

```
accept.station.in="*"
accept.station.out="*"
accept.wb.in="*"
accept.wb.out="*"
```

1.1.3 End to End Accuracy

Select products, install and configure the system such that the maximum error of a measured value as read from the DDC Hardware over the network is less than the maximum allowable error specified for the sensor or instrumentation.

1.1.4 Verification of Dimensions

After becoming familiar with all details of the work, verify all dimensions in the field, and advise the Contracting Officer of any discrepancy before performing any work.

1.1.5 Drawings

The Government will not indicate all offsets, fittings, and accessories that may be required on the drawings. Carefully investigate the mechanical, electrical, and finish conditions that could affect the work to be performed, arrange such work accordingly, and provide all work necessary to meet such conditions.

1.2 RELATED SECTIONS

Related work specified elsewhere:

a. Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS for BACnet systems with or without Niagara Framework.

b. Section 23 09 13 INSTRUMENTATION AND CONTROL DEVICES FOR HVAC

g. Section 01 91 00.15 10 TOTAL BUILDING COMMISSIONING

1.3 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS (ASHRAE)

ASHRAE 135	(2016) BACnet—A Data Communication Protocol for Building Automation and Control Networks
ASHRAE FUN IP	(2021) Fundamentals Handbook, I-P Edition

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE C62.41	(1991; R 1995) Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA 250	(2020) Enclosures for Electrical Equipment (1000 Volts Maximum)

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National Electrical Code
NFPA 90A	(2021) Standard for the Installation of

TRIDIUM, INC (TRIDIUM)

Niagara Framework	(2012) NiagaraAX User's Guide
Tridium Open NiCS	(2005) Understanding the NiagaraAX Compatibility Statement (NiCS)

UNDERWRITERS LABORATORIES (UL)

UL 5085-3	(2006; Reprint Jan 2022) UL Standard for Safety Low Voltage Transformers - Part 3: Class 2 and Class 3 Transformers

1.4 DEFINITIONS

The following list of definitions includes terms used in Sections referenced by this Section and are included here for completeness.The definitions contained in this Section may disagree with how terms are defined or used in other documents, including documents referenced by this Section. The definitions included here are the authoritative definitions for this Section and all Sections referenced by this Section.

After each term the protocol related to that term is included in parenthesis.

1.4.1 Alarm Generation (All protocols)

Alarm Generation is the monitoring of a value, comparison of the value to alarm conditions and the creation of an alarm when the conditions set for the alarm are met.

1.4.2 Building Automation and Control Network (BACnet) (BACnet)

The term BACnet is used in two ways. First meaning the BACnet Protocol Standard - the communication requirements as defined by ASHRAE 135 including all annexes and addenda. The second to refer to the overall technology related to the ASHRAE 135 protocol.

1.4.3 BACnet Advanced Application Controller (B-AAC) (BACnet)

A hardware device BTL Listed as a B-AAC, which is required to support BACnet Interoperability Building Blocks (BIBBs) for scheduling and alarming, but is not required to support as many BIBBs as a B-BC.

1.4.4 BACnet Application Specific Controller (B-ASC) (BACnet)

A hardware device BTL Listed as a B-ASC, with fewer BIBB requirements than a B-AAC. It is intended for use in a specific application.

1.4.5 BACnet Building Controller (B-BC) (BACnet)

A hardware device BTL Listed as a B-BC. A general-purpose, field-programmable device capable of carrying out a variety of building automation and control tasks including control and monitoring via direct digital control (DDC) of specific systems and data storage for trend information, time schedules, and alarm data. Like the other BTL Listed controller types (B-AAC, B-ASC etc.) a B-BC device is required to support

the server ("B") side of the ReadProperty and WriteProperty services, but unlike the other controller types it is also required to support the client ("A") side of these services. Communication between controllers requires that one of them support the client side and the other support the server side, so a B-BC is often used when communication between controllers is needed.

1.4.6 BACnet Broadcast Management Device (BBMD) (BACnet)

A communications device, typically combined with a BACnet router. A BBMD forwards BACnet broadcast messages to BACnet/IP devices and other BBMDs connected to the same BACnet/IP network. Each IP subnet that is part of a BACnet/IP network must have at least one BBMD. Note there are additional restrictions when multiple BBMDs share an IP subnet.

1.4.7 BACnet/IP (BACnet)

An extension of BACnet, Annex J, defines the use of a reserved UDP socket to transmit BACnet messages over IP networks. A BACnet/IP network is a collection of one or more IP subnets that share the same BACnet network number. See also paragraph BACNET BROADCAST MANAGEMENT DEVICE.

1.4.8 BACnet Internetwork (BACnet)

Two or more BACnet networks, connected with BACnet routers. In a BACnet Internetwork, there exists only one message path between devices.

1.4.9 BACnet Interoperability Building Blocks (BIBBs) (BACnet)

A BIBB is a collection of one or more ASHRAE 135 Services intended to define a higher level of interoperability. BIBBs are combined to build the BACnet functional requirements for a device in a specification. Some BIBBs define additional requirements (beyond requiring support for specific services) in order to achieve a level of interoperability. For example, the BIBB DS-V-A (Data Sharing-View-A), which would typically be used by a front-end, not only requires the client to support the ReadProperty Service, but also provides a list of data types (Object / Properties) which the client must be able to interpret and display for the user.

In the BIBB shorthand notation, -A is the client side and -B is the server side.

The following is a list of some BIBBs used by this or referenced Sections:	
DS-COV-A	Data Sharing-Change of Value (A side)
DS-COV-B	Data Sharing-Change of Value (B side)
NM-RC-B	Network Management-Router Configuration (B side)
DS-RP-A	Data Sharing-Read Property (A side)
DS-RP-B	Data Sharing-Read Property (B side)
DS-RPM-A	Data Sharing-Read Property Multiple (A Side)

The following is a list of some BIBBs used by this or referenced Sections:	
DS-RPM-B	Data Sharing-Read Property Multiple (B Side)
DS-WP-A	Data Sharing-Write Property (A Side)
DM-TS-B	Device Management-Time Synchronization (B Side)
DM-UTC-B	Device Management-UTC Time Synchronization (B Side)
DS-WP-B	Data Sharing-Write Property (B side)
SCHED-E-B	Scheduling-External (B side)
DM-OCD-B	Device Management-Object Creation and Deletion (B side)
AE-N-I-B	Alarm and Event-Notification Internal (B Side)
AE-N-E-B	Alarm and Event-Notification External (B Side)
T-VMT-I-B	Trending-Viewing and Modifying Trends Internal (B Side)
T-VMT-E-B	Trending-Viewing and Modifying Trends External (B Side)

1.4.10 BACnet Network (BACnet)

In BACnet, a portion of the control Internetwork consisting of one or more segments connected by repeaters. Networks are separated by routers.

1.4.11 BACnet Operator Display (B-OD) (BACnet)

A basic operator interface with limited capabilities relative to a B-OWS. It is not intended to perform direct digital control. A B-OD profile could be used for LCD devices, displays affixed to BACnet devices, handheld terminals or other very simple user interfaces.

1.4.12 BACnet Segment (BACnet)

One or more physical segments interconnected by repeaters (ASHRAE 135).

1.4.13 BACnet Smart Actuator (B-SA) (BACnet)

A simple actuator device with limited resources intended for specific applications.

1.4.14 BACnet Smart Sensor (B-SS) (BACnet)

A simple sensing device with limited resources.

1.4.15 BACnet Testing Laboratories (BTL) (BACnet)

Established by BACnet International to support compliance testing and interoperability testing activities and consists of BTL Manager and the BTL Working Group (BTL-WG). BTL also publishes Implementation Guidelines.

1.4.16 BACnet Testing Laboratories (BTL) Listed (BACnet)

A device that has been listed by BACnet Testing Laboratory. Devices may be certified to a specific device profile, in which case the listing indicates that the device supports the required capabilities for that profile, or may be listed as "other".

1.4.17 Binary (All protocols)

A two-state system where an "ON" condition is represented by a high signal level and an "OFF" condition is represented by a low signal level. 'Digital' is sometimes used interchangeably with 'binary'.

1.4.18 Broadcast (BACnet)

Unlike most messages, which are intended for a specific recipient device, a broadcast message is intended for all devices on the network.

1.4.19 Building Control Network (BCN) (All protocols)

The network connecting all DDC Hardware within a building (or specific group of buildings).

1.4.20 Building Point of Connection (BPOC) (All protocols)

A FPOC for a Building Control System. (This term is being phased out of use in preference for FPOC but is still used in some specifications and criteria. When it was used, it typically referred to a piece of control hardware. The current FPOC definition typically refers instead to IT hardware.)

1.4.21 Commandable (All protocols)

See Overridable.

1.4.22 Commandable Objects (BACnet)

Commandable Objects have a Commandable Property, Priority_Array, and Relinquish_Default Property as defined in ASHRAE 135, Clause 19.2, Command Prioritization.

1.4.23 Configurable (All protocols)

A property, setting, or value is configurable if it can be changed via hardware settings on the device, via the use of engineering software or over the control network from the front end, and is retained through (after) loss of power.

In a non-Niagara Framework BACnet system, a property, setting, or value is configurable if it can be changed via one or more of:

1) via BACnet services (including proprietary BACnet services)
2) via hardware settings on the device

In a Niagara Framework BACnet system, a property, setting, or value is configurable if it can be changed via one or more of:

1) via BACnet services (including proprietary BACnet services)
2) via hardware settings on the device
3) via the Niagara Framework

Note this is more stringent than the ASHRAE 135 definition.

1.4.24 Control Logic Diagram (All protocols)

A graphical representation of control logic for multiple processes that make up a system.

1.4.25 Device (BACnet)

A Digital Controller that contains a BACnet Device Object and uses BACnet to communicate with other devices.

1.4.26 Device Object (BACnet)

Every BACnet device requires one Device Object, whose properties represent the network visible properties of that device. Every Device Object requires a unique Object Identifier number on the BACnet Internetwork. This number is often referred to as the device instance or device ID.

1.4.27 Device Profile (BACnet)

A collection of BIBBs determining minimum BACnet capabilities of a device, defined in ASHRAE 135. Standard device profiles include BACnet Advanced Workstations (B-AWS), BACnet Building Controllers (B-BC), BACnet Advanced Application Controllers (B-AAC), BACnet Application Specific Controllers (B-ASC), BACnet Smart Actuator (B-SA), and BACnet Smart Sensor (B-SS).

1.4.28 Digital Controller (All protocols)

An electronic controller, usually with internal programming logic and digital and analog input/output capability, which performs control functions.

1.4.29 Direct Digital Control (DDC) (All protocols)

Digital controllers performing control logic. Usually the controller directly senses physical values, makes control decisions with internal programs, and outputs control signals to directly operate switches, valves, dampers, and motor controllers.

1.4.30 Field Point of Connection (FPOC) (All protocols)

The FPOC is the point of connection between the UMCS IP Network and the field control network (either an IP network, a non-IP network, or a combination of both). The hardware at this location which provides the connection is generally an IT device such as a switch, IP router, or firewall.

In general, the term "FPOC Location" means the place where this connection occurs, and "FPOC Hardware" means the device that provides the connection. Sometimes the term "FPOC" is used to mean either and its actual meaning (i.e. location or hardware) is determined by the context in which it is used.

1.4.31 Fox Protocol (Niagara Framework)

The protocol used for communication between components in the Niagara Framework. By default, Fox uses TCP port 1911.

1.4.32 Gateway (All protocols)

A device that translates from one protocol application data format to another. Devices that change only the transport mechanism of the protocol - "translating" from TP/FT-10 to Ethernet/IP or from BACnet MS/TP to BACnet over IP for example - are not gateways as the underlying data format does not change. Gateways are also called Communications Bridges or Protocol Translators.

A Niagara Framework Supervisory Gateway is one type of Gateway.

1.4.33 IEEE 802.3 Ethernet (All protocols)

A family of local-area-network technologies providing high-speed networking features over various media, typically Cat 5, 5e or Cat 6 twisted pair copper or fiber optic cable.

1.4.34 Internet Protocol (IP, TCP/IP, UDP/IP) (All protocols)

A communication method, the most common use is the World Wide Web. At the lowest level, it is based on Internet Protocol (IP), a method for conveying and routing packets of information over various LAN media. Two common protocols using IP are User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). UDP conveys information to well-known "sockets" without confirmation of receipt. TCP establishes connections, also known as "sessions", which have end-to-end confirmation and guaranteed sequence of delivery.

1.4.35 Input/Output (I/O) (All protocols)

Physical inputs and outputs to and from a device, although the term sometimes describes network or "virtual" inputs or outputs. See also "Points".

1.4.36 I/O Expansion Unit (All protocols)

An I/O expansion unit provides additional point capacity to a digital controller

1.4.37 IP subnet (All protocols)

A group of devices which share a defined range IP addresses. Devices on a common IP subnet can share data (including broadcasts) directly without the need for the traffic to traverse an IP router.

1.4.38 JACE (Niagara Framework)

Java Application Control Engine. See paragraph NIAGARA FRAMEWORK SUPERVISORY GATEWAY

1.4.39 Local-Area Network (LAN) (All protocols)

A communication network that spans a limited geographic area and uses the same basic communication technology throughout.

1.4.40 Local Display Panels (LDPs) (All protocols)

A DDC Hardware with a display and navigation buttons, and must provide display and adjustment of points as shown on the Points Schedule and as

indicated.

1.4.41 MAC Address (All protocols)

Media Access Control address. The physical device address that identifies a device on a Local Area Network.

1.4.42 Master-Slave/Token-Passing (MS/TP) (BACnet)

Data link protocol as defined by the BACnet standard. Multiple speeds (data rates) are permitted by the BACnet MS/TP standard.

1.4.43 Monitoring and Control (M&C) Software (All protocols)

The UMCS 'front end' software which performs supervisory functions such as alarm handling, scheduling and data logging and provides a user interface for monitoring the system and configuring these functions.

1.4.44 Network Number (BACnet)

A site-specific number assigned to each network. This network number must be unique throughout the BACnet Internetwork.

1.4.45 Niagara Framework (Niagara Framework)

A set of hardware and software specifications for building and utility control owned by Tridium Inc. and licensed to multiple vendors. The Framework consists of front end (M&C) software, web based clients, field level control hardware, and engineering tools. While the Niagara Framework is not adopted by a recognized standards body and does not use an open licensing model, it is sufficiently well-supported by multiple HVAC vendors to be considered a de-facto Open Standard.

1.4.46 Niagara Framework Supervisory Gateway (Niagara Framework)

DDC Hardware component of the Niagara Framework. A typical Niagara architecture has Niagara specific supervisory gateways at the IP level and other (non-Niagara specific) controllers on field networks (TP/FT-10, MS/TP, etc.) beneath the Niagara supervisory gateways. The Niagara specific controllers function as a gateway between the Niagara framework protocol (Fox) and the field network beneath. These supervisory gateways may also be used as general purpose controllers and also have the capability to provide a web-based user interface.

Note that different vendors refer to this component by different names. The most common name is "JACE"; other names include (but are not limited to)"EC-BOS", "FX-40", "TMN", "SLX" and "UNC".

1.4.47 Object (BACnet)

An ASHRAE 135 Object. The concept of organizing BACnet information into standard components with various associated Properties. Examples include Analog Input objects and Binary Output objects.

1.4.48 Object Identifier (BACnet)

A grouping of two Object properties: Object Type (e.g. Analog Value, Schedule, etc.) and Object Instance (in this case, a number). Object Identifiers must be unique within a device.

1.4.49 Object Instance (BACnet)

See paragraph OBJECT IDENTIFIER

1.4.50 Object Properties (BACnet)

Attributes of an object. Examples include present value and high limit properties of an analog input object. Properties are defined in ASHRAE 135; some are optional and some are required. Objects are controlled by reading from and writing to object properties.

1.4.51 Operator Configurable (All protocols)

Operator configurable values are values that can be changed from a single common front end user interface across multiple vendor systems.

For Niagara Framework Systems, a property, setting, or value is Operator Configurable when it is configurable from a Niagara Framework Front End.

For non Niagara-based BACnet systems, a property, setting, or value in a device is Operator Configurable when it is Configurable and is either:

a. a Writable Property of a Standard BACnet Object; or

b. a Property of a Standard BACnet Object that is Writable when Out_Of_Service is TRUE and Out_Of_Service is Writable.

1.4.52 Override (All protocols)

Changing the value of a point outside of the normal sequence of operation where the change has priority over the sequence and where there is a mechanism for releasing the change such that the point returns to the normal value. Overrides persist until released or overridden at the same or higher priority but are not required to persist through a loss of power. Overrides are often used by operators to change values, and generally originate at a user interface (workstation or local display panel).

1.4.53 Packaged Equipment (All protocols)

Packaged equipment is a single piece of equipment provided by a manufacturer in a substantially complete and operable condition, where the controls (DDC Hardware) are factory installed, and the equipment is sold and shipped from the manufacturer as a single entity. Disassembly and reassembly of a large piece of equipment for shipping does not prevent it from being packaged equipment. Package units may require field installation of remote sensors. Packaged equipment is also called a "packaged unit".

Note industry may use the term "Packaged System" to mean a collection of equipment that is designed to work together where each piece of equipment is packaged equipment and there is a network that connects the equipment together. A "packaged system" of this type is NOT packaged equipment; it is a collection of packaged equipment, and each piece of equipment must individually meet specification requirements.

1.4.54 Packaged Unit (All protocols)

See packaged equipment.

1.4.55 Performance Verification Test (PVT) (All protocols)

The procedure for determining if the installed BAS meets design criteria prior to final acceptance. The PVT is performed after installation, testing, and balancing of mechanical systems. Typically the PVT is performed by the Contractor in the presence of the Government.

1.4.56 Physical Segment (BACnet)

A single contiguous medium to which BACnet devices are attached (ASHRAE 135).

1.4.57 Polling (All protocols)

A device periodically requesting data from another device.

1.4.58 Points (All protocols)

Physical and virtual inputs and outputs. See also paragraph INPUT/OUTPUT (I/O).

1.4.59 Proportional, Integral, and Derivative (PID) Control Loop (All protocols)

Three parameters used to control modulating equipment to maintain a setpoint. Derivative control is often not required for HVAC systems (leaving "PI" control).

1.4.60 Proprietary (BACnet)

Within the context of BACnet, any extension of or addition to object types, properties, PrivateTransfer services, or enumerations specified in ASHRAE 135. Objects with Object_Type values of 128 and above are Proprietary Objects. Properties with Property_Identifier of 512 and above are proprietary Properties.

1.4.61 Protocol Implementation Conformance Statement (PICS) (BACnet)

A document, created by the manufacturer of a device, which describes which portions of the BACnet standard may be implemented by a given device. ASHRAE 135 requires that all ASHRAE 135 devices have a PICS, and also defines a minimum set of information that must be in it. A device as installed for a specific project may not implement everything in its PICS.

1.4.62 Repeater (All protocols)

A device that connects two control network segments and retransmits all information received on one side onto the other.

1.4.63 Router (All protocols)

A device that connects two ASHRAE 135 networks and controls traffic between the two by retransmitting signals received from one side onto the other based on the signal destination. Routers are used to subdivide a BACnet internetwork and to limit network traffic.

1.4.64 Segment (All protocols)

A 'single' section of a control network that contains no repeaters or routers. There is generally a limit on the number of devices on a segment, and this limit is dependent on the topology/media and device type.

1.4.65 Standard BACnet Objects (BACnet)

Objects with Object_Type values below 128 and specifically enumerated in Clause 21 of ASHRAE 135. Objects which are not proprietary. See paragraph PROPRIETARY.

1.4.66 Standard BACnet Properties (BACnet)

Properties with Property_Identifier values below 512 and specifically enumerated in Clause 21 of ASHRAE 135. Properties which are not proprietary. See Proprietary.

1.4.67 Standard BACnet Services (BACnet)

ASHRAE 135 services other than ConfirmedPrivateTransfer or UnconfirmedPrivateTransfer. See paragraph PROPRIETARY.

1.4.68 UMCS (All protocols)

UMCS stands for Utility Monitoring and Control System. The term refers to all components by which a project site monitors, manages, and controls real-time operation of HVAC and other building systems. These components include the UMCS "front-end" and all field building control systems connected to the front-end. The front-end consists of Monitoring and Control Software (user interface software), browser-based user interfaces and network infrastructure.

The network infrastructure (the "UMCS Network"), is an IP network connecting multiple building or facility control networks to the Monitoring and Control Software.

1.4.69 UMCS Network (All protocols)

The UMCS Network connects multiple building or facility control networks to the Monitoring and Control Software.

1.4.70 Writable Property (BACnet)

A Property is Writable when it can be changed through the use of one or more of the WriteProperty services defined in ASHRAE 135, Clause 15 regardless of the value of any other Property. Note that in the ASHRAE 135 standard, some Properties may be writable when the Out of Service Property is TRUE; for purposes of this Section, Properties that are only writable when the Out of Service Property is TRUE are not considered to be Writable.

1.5 PROJECT SEQUENCING

TABLE II: PROJECT SEQUENCING lists the sequencing of submittals as specified in paragraph SUBMITTALS (denoted by an 'S' in the 'TYPE' column) and activities as specified in PART 3 EXECUTION (denoted by an 'E' in the

'TYPE' column). TABLE II does not specify overall project milestone and completion dates; these dates are specified in the contract documents.

a. Sequencing for Submittals: The sequencing specified for submittals is the deadline by which the submittal must be initially submitted to the Government. Following submission there will be a Government review period as specified in Section 01 33 00 SUBMITTAL PROCEDURES. If the submittal is not accepted by the Government, revise the submittal and resubmit it to the Government within 14 days of notification that the submittal has been rejected. Upon resubmittal there will be an additional Government review period. If the submittal is not accepted the process repeats until the submittal is accepted by the Government.

b. Sequencing for Activities: The sequencing specified for activities indicates the earliest the activity may begin.

c. Abbreviations: In TABLE II the abbreviation AAO is used for 'after approval of' and 'ACO' is used for 'after completion of'.

TABLE II. PROJECT SEQUENCING

ITEM #	TYPE	DESCRIPTION	SEQUENCING (START OF ACTIVITY OR DEADLINE FOR SUBMITTAL)
1	S	Existing Conditions Report	
2	S	DDC Contractor Design Drawings	
3	S	Manufacturer's Product Data	
4	S	Pre-construction QC Checklist	
5	E	Install Building Control System	AAO #1 thru #4
6	E	Start-Up and Start-Up Testing	ACO #5
7	S	Post-Construction QC Checklist	ACO #6
8	S	Programming Software Configuration Software Niagara Framework Engineering Tool Niagara Framework Wizards	ACO #6
9	S	Draft As-Built Drawings	ACO #6
10	S	Start-Up Testing Report	ACO #6

TABLE II. PROJECT SEQUENCING			
ITEM #	TYPE	DESCRIPTION	SEQUENCING (START OF ACTIVITY OR DEADLINE FOR SUBMITTAL)
11	S	PVT Procedures	before schedule start of #12 and AAO #10
12	E	Execute PVT	AAO #9 and #11
13	S	PVT Report	7 days ACO #12
14	S	Controller Application Programs Controller Configuration Settings Niagara Framework Supervisory Gateway Backups	AAO #13
15	S	Final As-Built Drawings	AAO #13
16	S	O&M Instructions	AAO #15
17	S	Training Documentation	AAO #10 and before scheduled start of #18
18	E	Training	AAO #16 and #17
19	S	Closeout QC Checklist	ACO #18

1.6 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

DDC Contractor Design Drawings; G

Draft As-Built Drawings; G

Final As-Built Drawings; G

SD-03 Product Data

Programming Software; G

Controller Application Programs; G

Configuration Software; G

Controller Configuration Settings; G

Proprietary Multi-Split Engineering Tool Software; G

Manufacturer's Product Data; G

Niagara Framework Supervisory Gateway Backups; G

Niagara Framework Engineering Tool; G

SD-06 Test Reports

Pre-Construction Quality Control (QC) Checklist; G

Post-Construction Quality Control (QC) Checklist; G

Start-Up Testing Report; G

PVT Procedures; G

PVT Report; G

SD-10 Operation and Maintenance Data

Operation and Maintenance (O&M) Instructions; G

Training Documentation; G

SD-11 Closeout Submittals

Enclosure Keys; G

Password Summary Report; G

Closeout Quality Control (QC) Checklist; G

1.7 DATA PACKAGE AND SUBMITTAL REQUIREMENTS

Technical data packages consisting of technical data and computer software (meaning technical data which relates to computer software) which are specifically identified in this project and which may be defined/required in other specifications must be delivered strictly in accordance with the CONTRACT CLAUSES and in accordance with the Contract Data Requirements

List, DD Form 1423. Data delivered must be identified by reference to the particular specification paragraph against which it is furnished. All submittals not specified as technical data packages are considered 'shop drawings' under the Federal Acquisition Regulation Supplement (FARS) and must contain no proprietary information and be delivered with unrestricted rights.

1.8 SOFTWARE FOR DDC HARDWARE AND GATEWAYS

Provide all software related to the programming and configuration of DDC Hardware and Gateways as indicated. License all Software to the project site. The term "controller" as used in these requirements means both DDC Hardware and Gateways.

1.8.1 Configuration Software

For each type of controller, provide the configuration tool software in accordance with Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS. Submit hard copies of the software user manuals for each software with the software submittal.

Submit Configuration Software on CD-ROM as a Technical Data Package. Submit 3 hard copies of the software user manual for each piece of software.

1.8.2 Controller Configuration Settings

For each controller, provide copies of the installed configuration settings as source code compatible with the configuration tool software for that controller in accordance with Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS.

Submit Controller Configuration Settings on CD-ROM as a Technical Data Package. Include on the CD-ROM a list or table of contents clearly indicating which files are associated with each device. Submit 2 copies of the Controller Configuration Settings CD-ROM.

1.8.3 Programming Software

For each type of programmable controller, provide the programming software in accordance with Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS. Submit hard copies of software user manuals for each software with the software submittal.

Submit Programming Software on CD-ROM as a Technical Data Package. Submit 3 hard copies of the software user manual for each piece of software.

1.8.4 Controller Application Programs

For each programmable controller, provide copies of the application program as source code compatible with the programming software for that controller in accordance with Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS.

Submit Controller Application Programs on CD-ROM as a Technical Data Package. Include on the CD-ROM a list or table of contents clearly indicating which application program is associated with each device. Submit 2 copies of the Controller Application Programs CD-ROM.

1.8.5 Niagara Framework Supervisory Gateway Backups

For each Niagara Framework Supervisory Gateway, provide a backup of all software within the Niagara Framework Supervisory Gateway, including configuration settings. This backup must be sufficient to allow the restoration of the Niagara Framework Supervisory Gateway or the replacement of the Niagara Framework Supervisory Gateway.

Submit backups for each Niagara Framework Supervisory Gateway on CD-ROM as a Technical Data Package. Mark each backup indicating clearly the source Niagara Framework Supervisory Gateway.

1.8.6 Niagara Framework Engineering Tool(for all Niagara Framework system)

Provide a Niagara Framework Engineering Tool in accordance with Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS. Submit software user manuals with the Niagara Framework Engineering Tool submittal.

Submit the Niagara Framework Engineering Tool on CD-ROM as a Technical Data Package. Submit 2 hard copies of the software user manual for the Niagara Framework Engineering Tool.

1.9 QUALITY CONTROL CHECKLISTS

The QC Checklist for BACnet Systems in APPENDIX A of this Section must be completed by the Contractor's Chief Quality Control (QC) Representative and submitted as indicated.

The QC Checklist for Niagara Framework Based BACnet Systems in APPENDIX A of this Section must be completed by the Contractor's Chief Quality Control (QC) Representative and submitted as indicated.

The QC Representative must verify each item indicated and initial in the space provided to indicate that the requirement has been met. The QC Representative must sign and date the Checklist prior to submission to the Government.

1.9.1 Pre-Construction Quality Control (QC) Checklist

Complete items indicated as Pre-Construction QC Checklist items in the QC Checklist. Submit three copies of the Pre-Construction QC Checklist.

1.9.2 Post-Construction Quality Control (QC) Checklist

Complete items indicated as Post-Construction QC Checklist items in the QC Checklist. Submit three copies of the Post-Construction QC Checklist.

1.9.3 Closeout Quality Control (QC) Checklist

Complete items indicated as Closeout QC Checklist items in the QC Checklist. Submit three copies of the Closeout QC Checklist.

PART 2 PRODUCTS

Provide products meeting the requirements of Section 23 09 13 INSTRUMENTATION AND CONTROL DEVICES FOR HVAC, Section 23 09 23.02 BACNET

DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS for BACnet or Niagara BACnet systems, other referenced Sections, and this Section.

2.1 GENERAL PRODUCT REQUIREMENTS

Units of the same type of equipment must be products of a single manufacturer. Each major component of equipment must have the manufacturer's name and address, and the model and serial number in a conspicuous place. Materials and equipment must be standard products of a manufacturer regularly engaged in the manufacturing of these and similar products. The standard products must have been in a satisfactory commercial or industrial use for two years prior to use on this project. The two year use must include applications of equipment and materials under similar circumstances and of similar size. DDC Hardware not meeting the two-year field service requirement is acceptable provided it has been successfully used by the Contractor in a minimum of two previous projects. The equipment items must be supported by a service organization. Items of the same type and purpose must be identical, including equipment, assemblies, parts and components.

2.2 PRODUCT DATA

Provide manufacturer's product data sheets documenting compliance with product specifications for each product provided under Section 23 09 13 INSTRUMENTATION AND CONTROL DEVICES FOR HVAC, Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS, or this Section. Provide product data for all products in a single indexed compendium, organized by product type.

For all BACnet hardware: for each manufacturer, model and version (revision) of DDC Hardware provide the Protocol Implementation Conformance Statement (PICS) in accordance with Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS.

Submit Manufacturer's Product Data on CD-ROM.

2.3 OPERATION ENVIRONMENT

Unless otherwise specified, provide products rated for continuous operation under the following conditions:

a. Pressure: Pressure conditions normally encountered in the installed location.

b. Vibration: Vibration conditions normally encountered in the installed location.

c. Temperature:

(1) Products installed indoors: Ambient temperatures in the range of 32 to 112 degrees F and temperature conditions outside this range normally encountered at the installed location.

(2) Products installed outdoors or in unconditioned indoor spaces: Ambient temperatures in the range of -35 to +151 degrees F and temperature conditions outside this range normally encountered at the installed location.

d. Humidity: 10 to 95 percent relative humidity, noncondensing and humidity conditions outside this range normally encountered at the installed location.

2.4 WIRELESS CAPABILITY

For products incorporating any wireless capability (including but not limited to radio frequency (RF), infrared and optical), provide products for which wireless capability can be permanently disabled at the device. Optical and infrared capabilities may be disabled via a permanently affixed opaque cover plate.

2.5 ENCLOSURES

Enclosures supplied as an integral (pre-packaged) part of another product are acceptable. Provide two Enclosure Keys for each lockable enclosure on a single ring per enclosure with a tag identifying the enclosure the keys operate. Provide enclosures meeting the following minimum requirements:

2.5.1 Outdoors

For enclosures located outdoors, provide enclosures meeting NEMA 250 Type 4 requirements.

2.5.2 Mechanical and Electrical Rooms

For enclosures located in mechanical or electrical rooms, provide enclosures meeting NEMA 250 Type 2 requirements.

2.5.3 Other Locations

For enclosures in other locations including but not limited to occupied spaces, above ceilings, and in plenum returns, provide enclosures meeting NEMA 250 Type 1 requirements.

2.6 WIRE AND CABLE

Provide wire and cable meeting the requirements of NFPA 70 and NFPA 90A in addition to the requirements of this specification and referenced specifications.

2.6.1 Terminal Blocks

For terminal blocks which are not integral to other equipment, provide terminal blocks which are insulated, modular, feed-through, clamp style with recessed captive screw-type clamping mechanism, suitable for DIN rail mounting, and which have enclosed sides or end plates and partition plates for separation.

2.6.2 Control Wiring for Binary Signals

For Control Wiring for Binary Signals, provide 18 AWG copper or thicker wire rated for 300-volt service.

2.6.3 Control Wiring for Analog Signals

For Control Wiring for Analog Signals, provide 18 AWG or thicker, copper, single- or multiple-twisted wire meeting the following requirements:

a. minimum 2 inch lay of twist

b. 100 percent shielded pairs

c. at least 300-volt insulation

d. each pair has a 20 AWG tinned-copper drain wire and individual overall pair insulation

e. cables have an overall aluminum-polyester or tinned-copper cable-shield tape, overall 20 AWG tinned-copper cable drain wire, and overall cable insulation.

2.6.4 Power Wiring for Control Devices

For 24-volt circuits, provide insulated copper 18 AWG or thicker wire rated for 300 VAC service. For 120-volt circuits, provide 14 AWG or thicker stranded copper wire rated for 600-volt service.

2.6.5 Transformers

Provide UL 5085-3 approved transformers. Select transformers sized so that the connected load is no greater than 80 percent of the transformer rated capacity.

PART 3 EXECUTION

3.1 INSTALLATION

Fully install and test the control system in accordance Section 23 09 13 INSTRUMENTATION AND CONTROL DEVICES FOR HVAC, Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS for BACnet or Niagara BACnet systems, and this Section.

3.1.1 Dielectric Isolation

Provide dielectric isolation where dissimilar metals are used for connection and support. Install control system in a matter that provides clearance for control system maintenance by maintaining access space required to calibrate, remove, repair, or replace control system devices. Install control system such that it does not interfere with the clearance requirements for mechanical and electrical system maintenance.

3.1.2 Penetrations in Building Exterior

Make all penetrations through and mounting holes in the building exterior watertight.

3.1.3 Device Mounting Criteria

Install devices in accordance with the manufacturer's recommendations and as indicated and shown. Provide a weathershield for all devices installed outdoors. Provide clearance for control system maintenance by maintaining access space required to calibrate, remove, repair, or replace control system devices. Provide clearance for mechanical and electrical system maintenance; do not not interfere with the clearance requirements for mechanical and electrical system maintenance.

3.1.4 Labels and Tags

Key all labels and tags to the unique identifiers shown on the As-Built drawings. For labels exterior to protective enclosures provide engraved plastic labels mechanically attached to the enclosure or DDC Hardware. Labels inside protective enclosures may be attached using adhesive, but must not be hand written. For tags, provide plastic or metal tags mechanically attached directly to each device or attached by a metal chain or wire.

a. Label all Enclosures and DDC Hardware.

b. Tag Airflow measurement arrays (AFMA) with flow rate range for signal output range, duct size, and pitot tube AFMA flow coefficient.

c. Tag duct static pressure taps at the location of the pressure tap

3.1.5 Surge Protection

3.1.5.1 Power-Line Surge Protection

Protect equipment connected to AC circuits to withstand power-line surges in accordance with IEEE C62.41. Do not use fuses for surge protection.

3.1.5.2 Surge Protection for Transmitter and Control Wiring

Protect DDC hardware against or provided DDC hardware capable of withstanding surges induced on control and transmitter wiring installed outdoors and as shown. Protect equipment against the following two waveforms:

a. A waveform with a 10-microsecond rise time, a 1000-microsecond decay time and a peak current of 60 amps.

b. A waveform with an 8-microsecond rise time, a 20-microsecond decay time and a peak current of 500 amperes.

3.1.6 Basic Cybersecurity Requirements

3.1.6.1 Passwords

For all devices with a password, change the password from the default password. Do not use the same password for more than one device. Coordinate selection of passwords with user. Provide a Password Summary Report documenting the password for each device and describing the procedure to change the password for each device.

Provide two hardcopies of the Password Summary Report, each copy in its own sealed envelope.

3.1.6.2 Wireless Capability

Unless otherwise indicated, disable wireless capability (including but not limited to radio frequency (RF), infrared and optical) for all devices with wireless capability. Optical and infrared capabilities may be disabled via a permanently affixed opaque cover plate. Password protecting a wireless connections does not meet this requirement; the wireless capability must be disabled.

3.1.6.3 IP Network Physical Security

Install all IP Network media in conduit. Install all IP devices including but not limited to IP-enabled DDC hardware and IP Network Hardware in lockable enclosures.

3.2 DRAWINGS AND CALCULATIONS

Provide drawings in the form and arrangement indicated and shown. Use the same abbreviations, symbols, nomenclature and identifiers shown. Assign a unique identifier as shown to each control system element on a drawing. When packaging drawings, group schedules by system. When space allows, it is permissible to include multiple schedules for the same system on a single sheet. Except for drawings covering all systems, do not put information for different systems on the same sheet.

Submit hardcopy drawings on ISO A1 34 by 22 inches sheets, and electronic drawings in PDF and in AutoCAD format. In addition, submit electronic drawings in editable Excel format for all drawings that are tabular, including but not limited to the Point Schedule and Equipment Schedule.

a. Submit DDC Contractor Design Drawings consisting of each drawing indicated with pre-construction information depicting the intended control system design and plans. Submit DDC Contractor Design Drawings as a single complete package: 2 hard copies and 1 copies on CD-ROM.

b. Submit Draft As-Built Drawings consisting of each drawing indicated updated with as-built data for the system prior to PVT. Submit Draft As-Built Drawings as a single complete package: 2 hard copies and 1 copies on CD-ROM.

c. Submit Final As-Built Drawings consisting of each drawing indicated updated with all final as-built data. Final As-Built Drawings as a single complete package: 2 hard copies and 1 copies on CD-ROM.

3.2.1 Sample Drawings

Sample drawings in electronic format are available at the Whole Building Design Guide page for this section:
http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-23-09-00
These drawings may prove useful in demonstrating expected drawing formatting and example content and are provided for illustrative purposes only. Note that these drawings do not meet the content requirements of this Section and must be completed to meet project requirements.

3.2.2 Drawing Index and Legend

Provide an HVAC Control System Drawing Index showing the name and number of the building, military site, State or other similar designation, and Country. In the Drawing Index, list all Contractor Design Drawings, including the drawing number, sheet number, drawing title, and computer filename when used. In the Design Drawing Legend, show and describe all symbols, abbreviations and acronyms used on the Design Drawings. Provide a single Index and Legend for the entire drawing package.

3.2.3 Thermostat and Occupancy Sensor Schedule

Provide a thermostat and occupancy sensor schedule containing each

thermostat's unique identifier, room identifier and control features and functions as shown. Provide a single thermostat and occupancy sensor schedule for the entire project.

3.2.4 Damper Schedule

Provide a damper schedule containing each damper's unique identifier, type (opposed or parallel blade), nominal and actual sizes, orientation of axis and frame, direction of blade rotation, actuator size and spring ranges, operation rate, positive positioner range, location of actuators and damper end switches, arrangement of sections in multi-section dampers, and methods of connecting dampers, actuators, and linkages. Include the AMCA 511 maximum leakage rate at the operating static-pressure differential for each damper in the Damper Schedule. Provide a single damper schedule for the entire project.

3.2.5 Project Summary Equipment Schedule

Provide a project summary equipment schedule containing the manufacturer, model number, part number and descriptive name for each control device, hardware and component provided under this specification. Provide a single project equipment schedule for the entire project.

3.2.6 Equipment Schedule

Provide system equipment schedules containing the unique identifier, manufacturer, model number, part number and descriptive name for each control device, hardware and component provided under this specification. Provide a separate equipment schedule for each HVAC system.

3.2.7 Occupancy Schedule

Provide an occupancy schedule drawing containing the same fields as the occupancy schedule Contract Drawing with Contractor updated information. Provide a single occupancy schedule for the entire project.

3.2.8 DDC Hardware Schedule

Provide a single DDC Hardware Schedule for the entire project and including following information for each device.

3.2.8.1 DDC Hardware Identifier

The Unique DDC Hardware Identifier for the device.

3.2.8.2 HVAC System

The system "name" used to identify a specific system (the name used on the system schematic drawing for that system).

3.2.8.3 BACnet Device Information

3.2.8.3.1 Device Object Identifier

The Device Object Identifier: The Object_Identifier of the Device Object

3.2.8.3.2 Network Number

The Network Number for the device.

3.2.8.3.3 MAC Address

The MAC Address for the device

3.2.8.3.4 BTL Listing

The BTL Listing of the device. If the device is listed under multiple BTL Profiles, indicate the profile that matches the use and configuration of the device as installed.

3.2.8.3.5 Proprietary Services Information

If the device uses non-standard ASHRAE 135 services as defined and permitted in Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS, indicate that the device uses non-standard services and include a description of all non-standard services used. Describe usage and content such that a device from another vendor can interoperate with the device using the non-standard service. Provide descriptions with sufficient detail to allow a device from a different manufacturer to be programmed to both read and write the non-standard service request:

a. read: interpret the data contained in the non-standard service and;

b. write: given similar data, generate the appropriate non-standard service request.

3.2.8.3.6 Alarming Information

Indicate whether the device is used for alarm generation, and which types of alarm generation the device implements: intrinsic, local algorithmic, remote algorithmic.

3.2.8.3.7 Scheduling Information

Indicate whether the device is used for scheduling.

3.2.8.3.8 Trending Information

Indicate whether the device is used for trending, and indicate if the device is used to trend local values, remote values, or both.

3.2.8.4 Niagara Station ID

The Niagara Station ID for each Niagara Framework Supervisory Gateway

3.2.9 Points Schedule

Provide a Points Schedule in tabular form for each HVAC system, with the indicated columns and with each row representing a hardware point, network point or configuration point in the system.

a. When a Points Schedule was included in the Contract Drawing package, use the same fields as the Contract Drawing with updated information in addition to the indicated fields.

b. When Point Schedules are included in the contract package, items

requiring contractor verification or input have been shown in angle brackets ("<" and ">"), such as <___> for a required entry or <value> for a value requiring confirmation. Complete all items in brackets as well as any blank cells. Do not modify values which are not in brackets without approval.

Points Schedule Columns must include:

3.2.9.1 Point Name

The abbreviated name for the point using the indicated naming convention.

3.2.9.2 Description

A brief functional description of the point such as "Supply Air Temperature".

3.2.9.3 DDC Hardware Identifier

The Unique DDC Hardware Identifier shown on the DDC Hardware Schedule and used across all drawings for the DDC Hardware containing the point.

3.2.9.4 Settings

The value and units of any setpoints, configured setpoints, configuration parameters, and settings related to each point.

3.2.9.5 Range

The range of values, including units, associated with the point, including but not limited to a zone temperature setpoint adjustment range, a sensor measurement range, occupancy values for an occupancy input, or the status of a safety.

3.2.9.6 Input or Output (I/O) Type

The type of input or output signal associated with the point. Use the following abbreviations for entries in this column:

a. AI: The value comes from a hardware (physical) Analog Input

b. AO: The value is output as a hardware (physical) Analog Output

c. BI: The value comes from a hardware (physical) Binary Input

d. BO: The value is output as a hardware (physical) Binary Output

e. PULSE: The value comes from a hardware (physical) Pulse Accumulator Input

f. NET-IN: The value is provided from the network (generally from another device). Use this entry only when the value is received from another device as part of scheduling or as part of a sequence of operation, not when the value is received on the network for supervisory functions such as trending, alarming, override or display at a user interface.

g. NET-OUT: The value is provided to another controller over the network. Use this entry only when the value is transmitted to another

device as part of scheduling or as part of a sequence of operation, not when the value is transmitted on the network for supervisory functions such as trending, alarming, override or display at a user interface.

3.2.9.7 Object and Property Information

The Object Type and Instance Number for the Object associated with the point. If the value of the point is not in the Present_Value Property, then also provide the Property ID for the Property containing the value of the point. Any point that is displayed at the front end or on an LDP, is trended, is used by another device on the network, or has an alarm condition must be documented here.

3.2.9.8 Niagara Station ID

The Niagara Station ID of the Niagara Framework Supervisory Gateway the point is mapped into.

3.2.9.9 Network Data Exchange Information (Gets Data From, Sends Data To)

Provide the DDC Hardware Identifier of other DDC Hardware the point is shared with.

3.2.9.10 Override Information (Object Type and Instance Number)

For each point requiring an Override and not residing in a Niagara Framework Supervisory Gateway, indicate if the Object for the point is Commandable or, if the use of a separate Object was specifically approved by the Contracting Officer, provide the Object Type and Instance Number of the Object to be used in overriding the point.

3.2.9.11 Trend Object Information

For each point requiring a trend, indicate if the trend is Local or Remote, the trend Object type and the trend Object instance number. For remote trends provide the DDC Hardware Identifier for the device containing the trend Object in the Points Schedule notes.

3.2.9.12 Alarm Information

Indicate the Alarm Generation Type, Event Enrollment Object Instance Number, and Notification Class Object Instance Number for each point requiring an alarm. (Note that not all alarms will have Event Enrollment Objects.)

For Niagara BACnet systems: Indicate the Alarm Generation Type and Notification Class Object Instance Number for each point requiring an alarm. (Note that not all alarms will have a Notification Class Object.)

3.2.9.13 Configuration Information

Indicate the means of configuration associated with each point. For points in a Niagara Framework Supervisory Gateway, indicate the point within the Niagara Framework Supervisory Gateway used to configure the value. For other points:

a. For Operator Configurable Points indicate BACnet Object and Property

information (Name, Type, Identifiers) containing the configurable value. Indicate whether the property is writable always, or only when Out_Of_Service is TRUE.

b. For Configurable Points indicate the BACnet Object and Property information as for Operator Configurable points, or identification of the configurable settings from within the engineering software for the device or identification of the hardware settings on the device.

3.2.10 Riser Diagram

The Riser Diagram of the Building Control Network may be in tabular form, and must show all DDC Hardware and all Network Hardware, including network terminators. For each item, provide the unique identifier, common descriptive name, physical sequential order (previous and next device on the network), room identifier and location within room. A single riser diagram must be submitted for the entire system.

3.2.11 Control System Schematics

Provide control system schematics in the same form as the control system schematic Contract Drawing with Contractor updated information. Provide a control system schematic for each HVAC system.

3.2.12 Sequences of Operation

Provide HVAC control system sequence of operation and control logic diagrams in the same format as the Contract Drawings. Within these drawings, refer to devices by their unique identifiers. Submit sequences of operation and control logic diagrams for each HVAC system

3.2.13 Controller, Motor Starter and Relay Wiring Diagram

Provide controller wiring diagrams as functional wiring diagrams which show the interconnection of conductors and cables to each controller and to the identified terminals of input and output devices, starters and package equipment. Show necessary jumpers and ground connections and the labels of all conductors. Identify sources of power required for control systems and for packaged equipment control systems back to the panel board circuit breaker number, controller enclosures, magnetic starter, or packaged equipment control circuit. Show each power supply and transformer not integral to a controller, starter, or packaged equipment. Show the connected volt-ampere load and the power supply volt-ampere rating. Provide wiring diagrams for each HVAC system.

3.3 CONTROLLER TUNING

Tune each controller in a manner consistent with that described in the ASHRAE FUN IP and in the manufacturer's instruction manual. Tuning must consist of adjustment of the proportional, integral, and where applicable, the derivative (PID) settings to provide stable closed-loop control. Each loop must be tuned while the system or plant is operating at a high gain (worst case) condition, where high gain can generally be defined as a low-flow or low-load condition. Upon final adjustment of the PID settings, in response to a change in controller setpoint, the controlled variable must settle out at the new setpoint with no more than two (2) oscillations above and below setpoint. Upon settling out at the new setpoint the controller output must be steady. With the exception of

naturally slow processes such as zone temperature control, the controller must settle out at the new setpoint within five (5) minutes. Set the controller to its correct setpoint and record and submit the final PID configuration settings with the O&M Instructions and on the associated Points Schedule.

3.4 START-UP

3.4.1 Start-Up Test

Perform the following startup tests for each control system to ensure that the described control system components are installed and functioning per this specification.

Adjust, calibrate, measure, program, configure, set the time schedules, and otherwise perform all necessary actions to ensure that the systems function as indicated and shown in the sequence of operation and other contract documents.

3.4.1.1 Systems Check

An item-by-item check must be performed for each HVAC system

3.4.1.1.1 Step 1 - System Inspection

With the system in unoccupied mode and with fan hand-off-auto switches in the OFF position, verify that power and main air are available where required and that all output devices are in their failsafe and normal positions. Inspect each local display panel to verify that all displays indicate shutdown conditions.

3.4.1.1.2 Step 2 - Calibration Accuracy Check

Perform a two-point accuracy check of the calibration of each HVAC control system sensing element and transmitter by comparing the value from the test instrument to the network value provided by the DDC Hardware. Use digital indicating test instruments, such as digital thermometers, motor-driven psychrometers, and tachometers. Use test instruments with accuracy at least twice as accurate as the specified sensor accuracy and with calibration traceable to National Institute of Standards and Technology standards. Check one the first check point in the bottom one-third of the sensor range, and the second in the top one-third of the sensor range. Verify that the sensing element-to-DDC readout accuracies at two points are within the specified product accuracy tolerances, and if not recalibrate or replace the device and repeat the calibration check.

3.4.1.1.3 Step 3 - Actuator Range Check

With the system running, apply a signal to each actuator through the DDC Hardware controller. Verify proper operation of the actuators and positioners for all actuated devices and record the signal levels for the extreme positions of each device. Vary the signal over its full range, and verify that the actuators travel from zero stroke to full stroke within the signal range. Where applicable, verify that all sequenced actuators move from zero stroke to full stroke in the proper direction, and move the connected device in the proper direction from one extreme position to the other. For valve actuators and damper actuators, perform the actuator range check under normal system pressures.

3.4.1.2 Weather Dependent Test

Perform weather dependent test procedures in the appropriate climatic season.

3.4.2 Start-Up Testing Report

Submit 4 copies of the Start-Up Testing Report. The report may be submitted as a Technical Data Package documenting the results of the tests performed and certifying that the system is installed and functioning per this specification, and is ready for the Performance Verification Test (PVT).

3.5 PERFORMANCE VERIFICATION TEST (PVT)

3.5.1 PVT Procedures

Prepare PVT Procedures based on the steps listed below, the actions and expected results that will demonstrate that the control system performs in accordance with the sequences of operation, and other contract documents. Submit 4 copies of the PVT Procedures. The PVT Procedures may be submitted as a Technical Data Package.

3.5.1.1 Sensor Accuracy Checks

Include a one-point accuracy check of each sensor in the PVT procedures.

3.5.1.2 Endurance Test

Include a one-week endurance test as part of the PVT during which the system is operated continuously.

Use the building control system BACnet Trend Log or Trend Log Multiple Objects to trend all points shown as requiring a trend on the Point Schedule for the entire endurance test. If insufficient buffer capacity exists to trend the entire endurance test, upload trend logs during the course of the endurance test to ensure that no trend data is lost.

Use the building control system Niagara Trend Log Objects to trend all points shown as requiring a trend on the Point Schedule for the entire endurance test. If insufficient buffer capacity exists to trend the entire endurance test, upload trend logs during the course of the endurance test to ensure that no trend data is lost.

3.5.1.3 PVT Equipment List

Include in the PVT procedures a control system performance verification test equipment list that lists the equipment to be used during performance verification testing. For each piece of equipment, include manufacturer name, model number, equipment function, the date of the latest calibration, and the results of the latest calibration

3.5.2 PVT Execution

Demonstrate compliance of the control system with the contract documents. Using test plans and procedures approved by the Government, software capable of reading and writing COV Notification Subscriptions, Notification Class Recipient List Properties, event enrollments, demonstrate all physical and functional requirements of the project.

Show, step-by-step, the actions and results demonstrating that the control systems perform in accordance with the sequences of operation. Do not start the performance verification test until after receipt of written permission by the Government, based on Government approval of the PVT Plan and Draft As-Builts and completion of balancing. UNLESS GOVERNMENT WITNESSING OF A TEST IS SPECIFICALLY WAIVED BY THE GOVERNMENT, PERFORM ALL TESTS WITH A GOVERNMENT WITNESS. Do not conduct tests during scheduled seasonal off periods of base heating and cooling systems. If the system experiences any failures during the endurance test portion of the PVT, repair the system repeat the endurance test portion of the PVT until the system operates continuously and without failure for the specified endurance test period.

3.5.3 PVT Report

Prepare and submit a PVT report documenting all tests performed during the PVT and their results. Include all tests in the PVT procedures and any additional tests performed during PVT. Document test failures and repairs conducted with the test results.

Submit four copies of the PVT Report. The PVT Report may be submitted as a Technical Data Package.

3.6 OPERATION AND MAINTENANCE (O&M) INSTRUCTIONS

Provide HVAC control System Operation and Maintenance Instructions which include:

a. "Data Package 3" as indicated in Section 01 78 23 OPERATION AND MAINTENANCE DATA for each piece of control equipment.

b. "Data Package 4" as described in Section 01 78 23 OPERATION AND MAINTENANCE DATA for all air compressors.

c. HVAC control system sequences of operation formatted as indicated.

d. Procedures for the HVAC system start-up, operation and shut-down including the manufacturer's supplied procedures for each piece of equipment, and procedures for the overall HVAC system.

e. As-built HVAC control system detail drawings formatted as indicated.

f. Routine maintenance checklist. Provide the routine maintenance checklist arranged in a columnar format, where the first column lists all installed devices, the second column states the maintenance activity or that no maintenance required, the third column states the frequency of the maintenance activity, and the fourth column is used for additional comments or reference.

g. Qualified service organization list, including at a minimum company name, contact name and phone number.

h. Start-Up Testing Report.

i. Performance Verification Test (PVT) Procedures and Report.

Submit 2 copies of the Operation and Maintenance Instructions, indexed and in booklet form. The Operation and Maintenance Instructions may be

submitted as a Technical Data Package.

3.7 TRAINING

Conduct a training course for operating staff members designated by the Government in the maintenance and operation of the system, including specified hardware and software. Conduct 16 hours of training at the project site within 30 days after successful completion of the performance verification test. The Government reserves the right to make audio and visual recordings (using Government supplied equipment)of the training sessions for later use. Provide audiovisual equipment and other training materials and supplies required to conduct training. A training day is defined as 8 hours of classroom instruction, including two 15 minute breaks and excluding lunchtime, Monday through Friday, during the daytime shift in effect at the training facility.

3.7.1 Training Documentation

Prepare training documentation consisting of:

a. Course Attendee List: Develop the list of course attendees in coordination with and signed by the HVAC shop supervisor.

b. Training Manuals: Provide training manuals which include an agenda, defined objectives for each lesson, and a detailed description of the subject matter for each lesson. When presenting portions of the course material by audiovisuals, deliver copies of those audiovisuals as a part of the printed training manuals.

3.7.2 Training Course Content

For guidance in planning the required instruction, assume that attendees will have a high school education, and are familiar with HVAC systems. During the training course, cover all of the material contained in the Operating and Maintenance Instructions, the layout and location of each controller enclosure, the layout of one of each type of equipment and the locations of each, the location of each control device external to the panels, the location of the compressed air station, preventive maintenance, troubleshooting, diagnostics, calibration, adjustment, commissioning, tuning, and repair procedures. Typical systems and similar systems may be treated as a group, with instruction on the physical layout of one such system. Present the results of the performance verification test and the Start-Up Testing Report as benchmarks of HVAC control system performance by which to measure operation and maintenance effectiveness.

3.7.3 Training Documentation Submittal Requirements

Submit hardcopy training manuals and all training materials on CD-ROM. Provide one hardcopy manual for each trainee on the Course Attendee List and 2 additional copies for archive at the project site. Provide 2 copies of the Course Attendee List with the archival copies. Training Documentation may be submitted as a Technical Data Package.

APPENDIX A

QC CHECKLIST FOR BACNET SYSTEMS		
This checklist is not all-inclusive of the requirements of this specification and should not be interpreted as such. Instructions: Initial each item in the space provided (|____|) verifying that the requirement has been met.		
This checklist is for (circle one:) Pre-Construction QC Checklist Submittal Post-Construction QC Checklist Submittal Close-out QC Checklist Submittal		
Items verified for Pre-Construction, Post-Construction and Closeout QC Checklist Submittals:		
1	All DDC Hardware is numbered on Control System Schematic Drawings.	|____|
2	Signal lines on Control System Schematic are labeled with the signal type.	|____|
3	Local Display Panel (LDP) Locations are shown on Control System Schematic drawings.	|____|
Items verified for Post-Construction and Closeout QC Checklist Submittals:		
4	All sequences are performed as specified using DDC Hardware.	|____|
5	Training schedule and course attendee list has been developed and coordinated with shops and submitted.	|____|
Items verified for Closeout QC Checklist Submittal:		
6	Final As-built Drawings, including all Points Schedule drawings, accurately represent the final installed system.	|____|
7	Programming software has been submitted for all programmable controllers.	|____|
8	All software has been licensed to the Government.	

QC CHECKLIST FOR BACNET SYSTEMS		
9	O&M Instructions have been completed and submitted.	|____|
10	Training course has been completed.	|____|
11	All DDC Hardware is installed on a BACnet ASHRAE 135 network using either MS/TP in accordance with Clause 9 or IP in accordance with Annex J.	|____|
12	All DDC Hardware is BTL listed.	|____|
13	Communication between DDC Hardware is only via BACnet using standard services, except as specifically permitted by the specification. Non-standard services have been fully documented in the DDC Hardware Schedule.	|____|
14	Scheduling, Alarming, and Trending have been implemented using the standard BACnet Objects for these functions.	|____|
15	All Properties indicated as required to be Writable are Writable and Overrides have been provided as indicated	|____|
	_____ _____	
	(QC Representative Signature) (Date)	

QC CHECKLIST FOR NIAGARA FRAMEWORK BASED BACNET SYSTEMS
This checklist is not all-inclusive of the requirements of this specification and should not be interpreted as such. Instructions: Initial each item in the space provided (|____|) verifying that the requirement has been met.
This checklist is for (circle one:) Pre-Construction QC Checklist Submittal Post-Construction QC Checklist Submittal Close-out QC Checklist Submittal
Items verified for Pre-Construction, Post-Construction and Closeout QC Checklist Submittals:

1	All DDC Hardware is numbered on Control System Schematic Drawings.	|____|

QC CHECKLIST FOR NIAGARA FRAMEWORK BASED BACNET SYSTEMS		
2	Signal lines on Control System Schematic are labeled with the signal type.	|____|
3	Local Display Panel (LDP) Locations are shown on Control System Schematic drawings.	|____|
Items verified for Post-Construction and Closeout QC Checklist Submittals:		
4	All sequences are performed as specified using DDC Hardware.	|____|
5	Training schedule and course attendee list has been developed and coordinated with shops and submitted.	|____|
Items verified for Closeout QC Checklist Submittal:		
6	Final As-built Drawings, including all Points Schedule drawings, accurately represent the final installed system.	|____|
7	Programming software has been submitted for all programmable controllers.	|____|
8	All software has been licensed to the Government.	
9	O&M Instructions have been completed and submitted.	|____|
10	Training course has been completed.	|____|
11	All DDC Hardware is installed on a BACnet ASHRAE 135 network using either MS/TP in accordance with Clause 9 or IP in accordance with Annex J.	|____|
12	All DDC Hardware is BTL listed.	|____|
13	Communication between DDC Hardware is only via BACnet using standard services, except as specifically permitted by the specification. Non-standard services have been fully documented in the DDC Hardware Schedule.	|____|
14	Scheduling, Alarming, and Trending have been implemented using Niagara Framework objects and services, and BACnet Instrinsic Alarming as indicated.	|____|
15	All Properties indicated as required to be Writable are Writable and Overrides have been provided as indicated	|____|
_____ _____		
	(QC Representative Signature) (Date)	

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 09 13

INSTRUMENTATION AND CONTROL DEVICES FOR HVAC

PART 1 GENERAL

1.1 SUMMARY
1.1.1 Verification of Dimensions
1.1.2 Drawings
1.2 RELATED SECTIONS
1.3 REFERENCES
1.4 SUBMITTALS
1.5 DELIVERY AND STORAGE
1.6 INPUT MEASUREMENT ACCURACY
1.7 SUBCONTRACTOR SPECIAL REQUIREMENTS

PART 2 PRODUCTS

2.1 EQUIPMENT
2.1.1 General Requirements
2.1.2 Operation Environment Requirements
2.1.2.1 Pressure
2.1.2.2 Vibration
2.1.2.3 Temperature
2.1.2.4 Humidity
2.2 WEATHERSHIELDS
2.3 TUBING
2.3.1 Copper
2.3.2 Stainless Steel
2.3.3 Plastic
2.3.4 Polyethylene Tubing
2.4 WIRE AND CABLE
2.4.1 Terminal Blocks
2.4.2 Control Wiring for Binary Signals
2.4.3 Control Wiring for Analog Signals
2.4.4 Power Wiring for Control Devices
2.4.5 Transformers
2.5 DAMPERS
2.5.1 Damper Assembly
2.5.2 Operating Linkages
2.5.3 Damper Types
2.5.3.1 Flow Control Dampers
2.5.3.2 Mechanical Rooms and Other Utility Space Ventilation Dampers
2.5.3.3 Smoke Dampers
2.6 SENSORS AND INSTRUMENTATION
2.6.1 Analog and Binary Transmitters
2.6.2 Network Transmitters
2.6.3 Temperature Sensors
2.6.3.1 Sensor Accuracy and Stability of Control

2.6.3.1.1 Conditioned Space Temperature
2.6.3.1.2 Unconditioned Space Temperature
2.6.3.1.3 Duct Temperature
2.6.3.1.4 Outside Air Temperature
2.6.3.2 Transmitter Drift
2.6.3.3 Point Temperature Sensors
2.6.3.4 Temperature Sensor Details
2.6.3.4.1 Room Type
2.6.3.4.2 Duct Probe Type
2.6.3.4.3 Duct Averaging Type
2.6.3.4.4 Outside Air Type
2.6.4 Relative Humidity Sensor
2.6.5 Carbon Dioxide (CO2) Sensors
2.6.6 Differential Pressure Instrumentation
2.6.6.1 Differential Pressure Sensors
2.6.6.2 Differential Pressure Switch
2.6.7 Flow Sensors
2.6.7.1 Airflow Measurement Array (AFMA)
2.6.7.1.1 Airflow Straightener
2.6.7.1.2 Resistance to Airflow
2.6.7.1.3 Outside Air Temperature
2.6.7.1.4 Pitot Tube AFMA
2.6.7.1.5 Electronic AFMA
2.6.7.1.6 Fan Inlet Measurement Devices
2.6.7.2 Orifice Plate
2.6.7.3 Flow Nozzle
2.6.7.4 Venturi Tube
2.6.7.5 Annular Pitot Tube
2.6.8 Electrical Instruments
2.6.8.1 Current Transducers
2.6.8.2 Current Sensing Relays (CSRs)
2.6.8.3 Voltage Transducers
2.6.8.4 Energy Metering
2.6.8.4.1 Watt or Watthour Transducers
2.6.8.4.2 Watthour Revenue Meter (with and without Demand Register)
2.6.9 Occupancy Sensors
2.6.9.1 Passive Infrared (PIR) Occupancy Sensors
2.6.9.2 Ultrasonic Occupancy Sensors
2.6.9.3 Dual-Technology Occupancy Sensor (PIR and Ultrasonic)
2.6.10 Damper End Switches
2.6.11 Air Quality Sensors
2.7 INDICATING DEVICES
2.7.1 Thermometers
2.7.1.1 Air-Duct Thermometers
2.7.2 Pressure Gauges
2.7.3 Low Differential Pressure Gauges
2.8 OUTPUT DEVICES
2.8.1 Actuators
2.8.1.1 Damper Actuators
2.8.1.2 Positive Positioners
2.8.1.3 Electric Actuators
2.8.2 Relays
2.9 USER INPUT DEVICES
2.10 MULTIFUNCTION DEVICES
2.10.1 Current Sensing Relay Command Switch
2.10.2 Space Sensor Module

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 General Installation Requirements
3.1.1.1 Device Mounting Criteria
3.1.1.2 Labels and Tags
3.1.2 Weathershield
3.1.3 Room Instrument Mounting
3.1.4 Indication Devices Installed in Piping and Liquid Systems
3.1.5 Occupancy Sensors
3.1.6 Switches
3.1.6.1 Temperature Limit Switch
3.1.6.2 Hand-Off Auto Switches
3.1.7 Temperature Sensors
3.1.7.1 Room Temperature Sensors
3.1.7.2 Duct Temperature Sensors
3.1.7.2.1 Probe Type
3.1.7.2.2 Averaging Type
3.1.7.3 Immersion Temperature Sensors
3.1.7.4 Outside Air Temperature Sensors
3.1.8 Air Flow Measurement Arrays (AFMA)
3.1.9 Duct Static Pressure Sensors
3.1.10 Relative Humidity Sensors
3.1.11 Meters
3.1.11.1 Flowmeters
3.1.11.2 Energy Meters
3.1.12 Dampers
3.1.12.1 Damper Actuators
3.1.12.2 Damper Installation
3.1.13 Valves
3.1.13.1 Valve Actuators
3.1.14 Thermometers and Gauges
3.1.14.1 Local Gauges for Actuators
3.1.14.2 Thermometers
3.1.15 Wire and Cable
3.1.16 Copper Tubing
3.1.17 Plastic Tubing

-- End of Section Table of Contents --

SECTION 23 09 13

INSTRUMENTATION AND CONTROL DEVICES FOR HVAC

PART 1 GENERAL

1.1 SUMMARY

This section provides for the instrumentation control system components excluding direct digital controllers, network controllers, gateways etc. that are necessary for a completely functional automatic control system. When combined with a Direct Digital Control (DDC) system, the Instrumentation and Control Devices covered under this section must be a complete system suitable for the control of the heating, ventilating and air conditioning (HVAC) and other building-level systems as specified and indicated.

a. Install hardware to perform the control sequences as specified and indicated and to provide control of the equipment as specified and indicated.

b. Install hardware such that individual control equipment can be replaced by similar control equipment from other equipment manufacturers with no loss of system functionality.

c. Install and configure hardware such that the Government or their agents are able to perform repair, replacement, and upgrades of individual hardware without further interaction with the installing Contractor.

1.1.1 Verification of Dimensions

After becoming familiar with all details of the work, verify all dimensions in the field, and advise the Contracting Officer of any discrepancy before performing any work.

1.1.2 Drawings

The Government will not indicate all offsets, fittings, and accessories that may be required on the drawings. Carefully investigate the mechanical, electrical, and finish conditions that could affect the work to be performed, arrange such work accordingly, and provide all work necessary to meet such conditions.

1.2 RELATED SECTIONS

Related work specified elsewhere.

Section 01 30 00 ADMINISTRATIVE REQUIREMENTS

Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC

Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS

Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM

1.3 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AIR MOVEMENT AND CONTROL ASSOCIATION INTERNATIONAL, INC. (AMCA)

AMCA 500-D	(2018) Laboratory Methods of Testing Dampers for Rating
AMCA 511	(2010; R 2016) Certified Ratings Program for Air Control Devices

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

ANSI C12.1	(2014; Errata 2016) Electric Meters - Code for Electricity Metering

AMERICAN SOCIETY OF MECHANICAL ENGINEERS (ASME)

ASME B16.18	(2021) Cast Copper Alloy Solder Joint Pressure Fittings
ASME B16.22	(2021) Wrought Copper and Copper Alloy Solder Joint Pressure Fittings
ASME B16.26	(2018) Standard for Cast Copper Alloy Fittings for Flared Copper Tubes
ASME B40.100	(2013) Pressure Gauges and Gauge Attachments

ASTM INTERNATIONAL (ASTM)

ASTM A269/A269M	(2015; R 2019) Standard Specification for Seamless and Welded Austenitic Stainless Steel Tubing for General Service
ASTM B32	(2020) Standard Specification for Solder Metal
ASTM B75/B75M	(2020) Standard Specification for Seamless Copper Tube
ASTM B88	(2020) Standard Specification for Seamless Copper Water Tube
ASTM D635	(2018) Standard Test Method for Rate of Burning and/or Extent and Time of Burning of Plastics in a Horizontal Position
ASTM D638	(2014) Standard Test Method for Tensile Properties of Plastics
ASTM D792	(2013) Density and Specific Gravity (Relative Density) of Plastics by Displacement

ASTM D1238	(2013) Melt Flow Rates of Thermoplastics by Extrusion Plastometer
ASTM D1693	(2015) Standard Test Method for Environmental Stress-Cracking of Ethylene Plastics

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 142	(2007; Errata 2014) Recommended Practice for Grounding of Industrial and Commercial Power Systems - IEEE Green Book

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

ANSI C12.20	(2015; E 2018) Electricity Meters - 0.1, 0.2, and 0.5 Accuracy Classes
NEMA/ANSI C12.10	(2011; R 2021) Physical Aspects of Watthour Meters - Safety Standard

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National Electrical Code
NFPA 90A	(2021) Standard for the Installation of Air Conditioning and Ventilating Systems

UNDERWRITERS LABORATORIES (UL)

UL 94	(2013; Reprint Apr 2022) UL Standard for Safety Tests for Flammability of Plastic Materials for Parts in Devices and Appliances
UL 555	(2006; Reprint Aug 2016) UL Standard for Safety Fire Dampers
UL 555S	(2014; Reprint Oct 2020) UL Standard for Safety Smoke Dampers
UL 1820	(2004; Reprint May 2013) UL Standard for Safety Fire Test of Pneumatic Tubing for Flame and Smoke Characteristics
UL 5085-3	(2006; Reprint Jan 2022) UL Standard for Safety Low Voltage Transformers - Part 3: Class 2 and Class 3 Transformers

1.4 SUBMITTALS

Submittal requirements are specified in Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC.

1.5 DELIVERY AND STORAGE

Store and protect products from the weather, humidity, and temperature

variations, dirt and dust, and other contaminants, within the storage condition limits published by the equipment manufacturer.

1.6 INPUT MEASUREMENT ACCURACY

Select, install and configure sensors, transmitters and DDC Hardware such that the maximum error of the measured value at the input of the DDC hardware is less than the maximum allowable error specified for the sensor or instrumentation.

1.7 SUBCONTRACTOR SPECIAL REQUIREMENTS

Perform all work in this section in accordance with the paragraph entitled CONTRACTOR SPECIAL REQUIREMENTS in Section 01 30 00 ADMINISTRATIVE REQUIREMENTS.

PART 2 PRODUCTS

2.1 EQUIPMENT

2.1.1 General Requirements

All products used to meet this specification must meet the indicated requirements, but not all products specified here will be required by every project. All products must meet the requirements both Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC and this Section.

2.1.2 Operation Environment Requirements

Unless otherwise specified, provide products rated for continuous operation under the following conditions:

2.1.2.1 Pressure

Pressure conditions normally encountered in the installed location.

2.1.2.2 Vibration

Vibration conditions normally encountered in the installed location.

2.1.2.3 Temperature

a. Products installed indoors: Ambient temperatures in the range of 32 to 112 degrees F and temperature conditions outside this range normally encountered at the installed location.

b. Products installed outdoors or in unconditioned indoor spaces: Ambient temperatures in the range of -35 to +151 degrees F and temperature conditions outside this range normally encountered at the installed location.

2.1.2.4 Humidity

10 to 95 percent relative humidity, non-condensing and also humidity conditions outside this range normally encountered at the installed location.

2.2 WEATHERSHIELDS

Provide weathershields constructed of galvanized steel painted white, unpainted aluminum, aluminum painted white, or white PVC.

2.3 TUBING

2.3.1 Copper

Provide ASTM B75/B75M or ASTM B88 rated tubing meeting the following requirements:

a. For tubing 0.375 inch outside diameter and larger provide tubing with minimum wall thickness equal to ASTM B88, Type M

b. For tubing less than 0.375 inch outside diameter provide tubing with minimum wall thickness of 0.025 inch

c. For exposed tubing and tubing for working pressures greater than 30 psig provide hard copper tubing.

d. Provide fittings which are ASME B16.18 or ASME B16.22 solder type using ASTM B32 95-5 tin-antimony solder, or which are ASME B16.26 compression type.

2.3.2 Stainless Steel

For stainless steel tubing provide tubing conforming to ASTM A269/A269M

2.3.3 Plastic

Provide plastic tubing with the burning characteristics of linear low-density polyethylene tubing which is self-extinguishing when tested in accordance with ASTM D635, has UL 94 V-2 flammability classification or better, and which withstands stress cracking when tested in accordance with ASTM D1693. Provide plastic-tubing bundles with Mylar barrier and flame-retardant polyethylene jacket.

2.3.4 Polyethylene Tubing

Provide flame-resistant, multiple polyethylene tubing in flame-resistant protective sheath with mylar barrier, or unsheathed polyethylene tubing in rigid metal, intermediate metal, or electrical metallic tubing conduit for areas where tubing is exposed. Single, unsheathed, flame-resistant polyethylene tubing may be used where concealed in walls or above ceilings and within control panels. Do not provide polyethylene tubing for systems indicated as critical and smoke removal systems, or for systems with working pressures over 30 psig. Provide compression or brass barbed push-on type fittings. Provide extruded seamless polyethylene tubing conforming to the following:

a. Minimum Burst Pressure Requirements: 100 psig at 75 degrees F to 25 psig at 150 degrees F.

b. Stress Crack Resistance: ASTM D1693, 200 hours minimum.

c. Tensile Strength (Minimum): ASTM D638, 1100 psi.

d. Flow Rate (Average): ASTM D1238, 0.30 decigram per minute.

e. Density (Average): ASTM D792, 57.5 pounds per cubic feet.

f. Burn rate: ASTM D635

g. Flame Propagation: UL 1820, less than 5 feet ASTM D635

h. Average Optical Density: UL 1820, less than 0.15 ASTM D635

2.4 WIRE AND CABLE

Provide wire and cable meeting the requirements of NFPA 70 and NFPA 90A in addition to the requirements of this specification and referenced specifications.

2.4.1 Terminal Blocks

For terminal blocks which are not integral to other equipment, provide terminal blocks which are insulated, modular, feed-through, clamp style with recessed captive screw-type clamping mechanism, suitable for DIN rail mounting, and which have enclosed sides or end plates and partition plates for separation.

2.4.2 Control Wiring for Binary Signals

For Control Wiring for Binary Signals, provide 18 AWG copper or thicker wire rated for 300-volt service.

2.4.3 Control Wiring for Analog Signals

For Control Wiring for Analog Signals, provide 18 AWG or thicker, copper, single- or multiple-twisted wire meeting the following requirements:

a. minimum 2 inch lay of twist

b. 100 percent shielded pairs

c. at least 300-volt insulation

d. each pair has a 20 AWG tinned-copper drain wire and individual overall pair insulation

e. cables have an overall aluminum-polyester or tinned-copper cable-shield tape, overall 20 AWG tinned-copper cable drain wire, and overall cable insulation.

2.4.4 Power Wiring for Control Devices

For 24-volt circuits, provide insulated copper 18 AWG or thicker wire rated for 300 VAC service. For 120-volt circuits, provide 14 AWG or thicker stranded copper wire rated for 600-volt service.

2.4.5 Transformers

Provide UL 5085-3 approved transformers. Select transformers sized so that the connected load is no greater than 80 percent of the transformer rated capacity.

2.5 DAMPERS

2.5.1 Damper Assembly

Provide single damper sections with blades no longer than 48 inches and which are no higher than 72 inches and damper blade width of 8 inches or less. When larger sizes are required, combine damper sections. Provide dampers made of steel, or other materials where indicated and with assembly frames constructed of 0.07 inch minimum thickness galvanized steel channels with mitered and welded corners. Steel channel frames constructed of 0.06 inch minimum thickness are acceptable provided the corners are reinforced.

a. Flat blades must be made rigid by folding the edges. Blade-operating linkages must be within the frame so that blade-connecting devices within the same damper section must not be located directly in the air stream.

b. Damper axles must be 1/2 inch minimum, plated steel rods supported in the damper frame by stainless steel or bronze bearings. Blades mounted vertically must be supported by thrust bearings.

c. Provide dampers which do not exceed a pressure drop through the damper of 0.04 inches water gauge at 1000 ft/min in the wide-open position. Provide dampers with frames not less than 2 inch in width. Provide dampers which have been tested in accordance with AMCA 500-D.

2.5.2 Operating Linkages

For operating links external to dampers, such as crank arms, connecting rods, and line shafting for transmitting motion from damper actuators to dampers, provide links able to withstand a load equal to at least 300 percent of the maximum required damper-operating force without deforming. Rod lengths must be adjustable. Links must be brass, bronze, zinc-coated steel, or stainless steel. Working parts of joints and clevises must be brass, bronze, or stainless steel. Adjustments of crank arms must control the open and closed positions of dampers.

2.5.3 Damper Types

2.5.3.1 Flow Control Dampers

Provide parallel-blade or opposed blade type dampers for outside air, return air, relief air, exhaust, face and bypass dampers as indicated on the Damper Schedule. Blades must have interlocking edges. The channel frames of the dampers must be provided with jamb seals to minimize air leakage. Unless otherwise indicated, dampers must meet AMCA 511 Class 1A requirements. Outside air damper seals must be suitable for an operating temperature range of -40 to +167 degrees F. Dampers must be rated at not less than 2000 ft/min air velocity.

2.5.3.2 Mechanical Rooms and Other Utility Space Ventilation Dampers

Provide utility space ventilation dampers as indicated. Unless otherwise indicated provide AMCA 511 class 3 dampers. Provide dampers rated at not less than 1500 ft/min air velocity.

2.5.3.3 Smoke Dampers

Provide smoke-damper and actuator assemblies which meet the current requirements of NFPA 90A, UL 555, and UL 555S. For combination fire and smoke dampers provide dampers rated for 250 degrees F Class II leakage per UL 555S.

2.6 SENSORS AND INSTRUMENTATION

Unless otherwise specified, provide sensors and instrumentation which incorporate an integral transmitter. Sensors and instrumentation, including their transmitters, must meet the specified accuracy and drift requirements at the input of the connected DDC Hardware's analog-to-digital conversion.

2.6.1 Analog and Binary Transmitters

Provide transmitters which match the characteristics of the sensor. Transmitters providing analog values must produce a linear 4-20 mAdc, 0-10 Vdc signal corresponding to the required operating range and must have zero and span adjustment. Transmitters providing binary values must have dry contacts rated at 1A at 24 Volts AC.

2.6.2 Network Transmitters

Sensors and Instrumentation incorporating an integral network connection are considered DDC Hardware and must meet the DDC Hardware requirements of 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS when used in a BACnet network.

2.6.3 Temperature Sensors

Provide the same sensor type throughout the project. Temperature sensors may be provided without transmitters. Where transmitters are used, the range must be the smallest available from the manufacturer and suitable for the application such that the range encompasses the expected range of temperatures to be measured. The end to end accuracy includes the combined effect of sensitivity, hysteresis, linearity and repeatability between the measured variable and the end user interface (graphic presentation) including transmitters if used.

2.6.3.1 Sensor Accuracy and Stability of Control

2.6.3.1.1 Conditioned Space Temperature

Plus or minus 0.5 degree F over the operating range.

2.6.3.1.2 Unconditioned Space Temperature

a. Plus or minus 1 degree F over the range of 30 to 131 degrees F AND

b. Plus or minus 4 degrees F over the rest of the operating range.

2.6.3.1.3 Duct Temperature

Plus or minus 0.5 degree F

2.6.3.1.4 Outside Air Temperature

a. Plus or minus 2 degrees F over the range of -30 to +130 degrees F AND

b. Plus or minus 1 degree F over the range of 30 to 130 degrees F.

2.6.3.2 Transmitter Drift

The maximum allowable transmitter drift: 0.25 degrees F per year.

2.6.3.3 Point Temperature Sensors

Point Sensors must be encapsulated in epoxy, series 300 stainless steel, anodized aluminum, or copper.

2.6.3.4 Temperature Sensor Details

2.6.3.4.1 Room Type

Provide the sensing element components within a decorative protective cover suitable for surrounding decor.

2.6.3.4.2 Duct Probe Type

Ensure the probe is long enough to properly sense the air stream temperature.

2.6.3.4.3 Duct Averaging Type

Continuous averaging sensors must be one foot in length for each 1 square foot of duct cross-sectional area, and a minimum length of 5 feet.

2.6.3.4.4 Outside Air Type

Provide the sensing element rated for outdoor use

2.6.4 Relative Humidity Sensor

Relative humidity sensors must use bulk polymer resistive or thin film capacitive type non-saturating sensing elements capable of withstanding a saturated condition without permanently affecting calibration or sustaining damage. The sensors must include removable protective membrane filters. Where required for exterior installation, sensors must be capable of surviving below freezing temperatures and direct contact with moisture without affecting sensor calibration. When used indoors, the sensor must be capable of being exposed to a condensing air stream (100 percent relative humidity) with no adverse effect to the sensor's calibration or other harm to the instrument. The sensor must be of the wall-mounted or duct-mounted type, as required by the application, and must be provided with any required accessories. Sensors used in duct high-limit applications must have a bulk polymer resistive sensing element. Duct-mounted sensors must be provided with a duct probe designed to protect the sensing element from dust accumulation and mechanical damage. Relative humidity (RH) sensors must measure relative humidity over a range of 0 percent to 100 percent with an accuracy of plus or minus 2 percent. RH sensors must function over a temperature range of 40 to 135 degrees F and must not drift more than 1 percent per year.

2.6.5 Carbon Dioxide (CO2) Sensors

Provide photometric type CO2 sensors with integral transducers and linear output. Carbon dioxide (CO2) sensors must measure CO2 concentrations between 0 to 2000 parts per million (ppm) using non-dispersible infrared (NDIR) technology with an accuracy of plus or minus 50 ppm and a maximum response time of 1 minute. The sensor must be rated for operation at ambient air temperatures within the range of 32 to 122 degrees F and relative humidity within the range of 20 to 95 percent (non-condensing). The sensor must have a maximum drift of 2 percent per year. The sensor chamber must be manufactured with a non-corrosive material that does not affect carbon dioxide sample concentration. Duct mounted sensors must be provided with a duct probe designed to protect the sensing element from dust accumulation and mechanical damage. The sensor must have a calibration interval no less than 5 years.

2.6.6 Differential Pressure Instrumentation

2.6.6.1 Differential Pressure Sensors

Provide Differential Pressure Sensors with ranges as indicated or as required for the application. Pressure sensor ranges must not exceed the high end range indicated on the Points Schedule by more than 50 percent. The over pressure rating must be a minimum of 150 percent of the highest design pressure of either input to the sensor. The accuracy must be plus or minus 1 percent of full scale. The sensor must have a maximum drift of 2 percent per year

2.6.6.2 Differential Pressure Switch

Provide differential pressure switches with a user-adjustable setpoint which are sized for the application such that the setpoint is between 25 percent and 75 percent of the full range. The over pressure rating must be a minimum of 150 percent of the highest design pressure of either input to the sensor. The switch must have two sets of contacts and each contact must have a rating greater than it's connected load. Contacts must open or close upon rise of pressure above the setpoint or drop of pressure below the setpoint as indicated.

2.6.7 Flow Sensors

2.6.7.1 Airflow Measurement Array (AFMA)

2.6.7.1.1 Airflow Straightener

Provide AFMAs which contain an airflow straightener if required by the AFMA manufacturer's published installation instructions. The straightener must be contained inside a flanged sheet metal casing, with the AFMA located as specified according to the published recommendation of the AFMA manufacturer. In the absence of published documentation, provide airflow straighteners if there is any duct obstruction within 5 duct diameters upstream of the AFMA. Air-flow straighteners, where required, must be constructed of 0.125 inch aluminum honeycomb and the depth of the straightener must not be less than 1.5 inches.

2.6.7.1.2 Resistance to Airflow

The resistance to air flow through the AFMA, including the airflow straightener must not exceed 0.085 inch water gauge at an airflow of 2,000

fpm. AFMA construction must be suitable for operation at airflows of up to 5000 fpm over a temperature range of 40 to 120 degrees F.

2.6.7.1.3 Outside Air Temperature

In outside air measurement or in low-temperature air delivery applications, provide an AFMA certified by the manufacturer to be accurate as specified over a temperature range of -20 to +120 degrees F .

2.6.7.1.4 Pitot Tube AFMA

Each Pitot Tube AFMA must contain an array of velocity sensing elements. The velocity sensing elements must be of the multiple pitot tube type with averaging manifolds. The sensing elements must be distributed across the duct cross section in the quantity and pattern specified or recommended by the published installation instructions of the AFMA manufacturer.

a. Pitot Tube AFMAs for use in airflows over 600 fpm must have an accuracy of plus or minus 5 percent over a range of 500 to 2500 fpm.

b. Pitot Tube AFMAs for use in airflows under 600 fpm must have an accuracy of plus or minus 5 percent over a range of 125 to 2500 fpm.

2.6.7.1.5 Electronic AFMA

Each electronic AFMA must consist of an array of velocity sensing elements of the resistance temperature detector (RTD) or thermistor type. The sensing elements must be distributed across the duct cross section in the quantity and pattern specified or recommended by the published application data of the AFMA manufacturer. Electronic AFMAs must have an accuracy of plus or minus 5 percent over a range of 125 to 5,000 fpm and the output must be temperature compensated over a range of 32 to 212 degrees F.

2.6.7.1.6 Fan Inlet Measurement Devices

Fan inlet measurement devices cannot be used unless indicated on the drawings or schedules.

2.6.7.2 Orifice Plate

Orifice plate must be made of an austenitic stainless steel sheet of 0.125 inch nominal thickness with an accuracy of plus or minus 1 percent of full flow. The orifice plate must be flat within 0.002 inches. The orifice surface roughness must not exceed 20 micro-inches. The thickness of the cylindrical face of the orifice must not exceed 2 percent of the pipe inside diameter or 12.5 percent of the orifice diameter, whichever is smaller. The upstream edge of the orifice must be square and sharp. Where orifice plates are used, concentric orifice plates must be used in all applications except steam flow measurement in horizontal pipelines.

2.6.7.3 Flow Nozzle

Flow nozzle must be made of austenitic stainless steel with an accuracy of plus or minus 1 percent of full flow. The inlet nozzle form must be elliptical and the nozzle throat must be the quadrant of an ellipse. The thickness of the nozzle wall and flange must be such that distortion of the nozzle throat from strains caused by the pipeline temperature and pressure, flange bolting, or other methods of installing the nozzle in the pipeline must not cause the accuracy to degrade beyond the specified

limit. The outside diameter of the nozzle flange or the design of the flange facing must be such that the nozzle throat must be centered accurately in the pipe.

2.6.7.4 Venturi Tube

Venturi tube must be made of cast iron or cast steel and must have an accuracy of plus or minus 1 percent of full flow. The throat section must be lined with austenitic stainless steel. Thermal expansion characteristics of the lining must be the same as that of the throat casting material. The surface of the throat lining must be machined to a plus or minus 50 micro inch finish, including the short curvature leading from the converging entrance section into the throat.

2.6.7.5 Annular Pitot Tube

Annular pitot tube must be made of austenitic stainless steel with an accuracy of plus or minus 2 percent of full flow and a repeatability of plus or minus 0.5 percent of measured value. The unit must have at least one static port and no less than four total head pressure ports with an averaging manifold.

2.6.8 Electrical Instruments

Provide Electrical Instruments with an input range as indicated or sized for the application. Unless otherwise specified, AC instrumentation must be suitable for 60 Hz operation.

2.6.8.1 Current Transducers

Current transducers must accept an AC current input and must have an accuracy of plus or minus 0.5 percent of full scale. The device must have a means for calibration. Current transducers for variable frequency applications must be rated for variable frequency operation.

2.6.8.2 Current Sensing Relays (CSRs)

Current sensing relays (CSRs) must provide a normally-open contact with a voltage and amperage rating greater than its connected load. Current sensing relays must be of split-core design. The CSR must be rated for operation at 200 percent of the connected load. Voltage isolation must be a minimum of 600 volts. The CSR must auto-calibrate to the connected load or be adjustable and field calibrated. Current sensors for variable frequency applications must be rated for variable frequency operation.

2.6.8.3 Voltage Transducers

Voltage transducers must accept an AC voltage input and have an accuracy of plus or minus 0.25 percent of full scale. The device must have a means for calibration. Line side fuses for transducer protection must be provided.

2.6.8.4 Energy Metering

2.6.8.4.1 Watt or Watthour Transducers

Watt transducers must measure voltage and current and must output kW or kWh or both kW and kWh as indicated. kW outputs must have an accuracy of plus or minus 0.5 percent over a power factor range of 0.1 to 1. kWh

outputs must have an accuracy of plus or minus 0.5 percent over a power factor range of 0.1 to 1.

2.6.8.4.2 Watthour Revenue Meter (with and without Demand Register)

All Watthour revenue meters must measure voltage and current and must be in accordance with ANSI C12.1 with an ANSI C12.20 Accuracy class of 0.5 and must have pulse initiators for remote monitoring of Watthour consumption. Pulse initiators must consist of form C contacts with a current rating not to exceed two amperes and voltage not to exceed 500 V, with combinations of VA not to exceed 100 VA, and a life rating of one billion operations. Meter sockets must be in accordance with NEMA/ANSI C12.10. Watthour revenue meters with demand registers must output instantaneous demand in addition to the pulse initiators.

2.6.9 Occupancy Sensors

Occupancy sensors must have occupancy-sensing sensitivity adjustment and an adjustable off-delay timer with a setpoint of 15 minutes. Adjustments accessible from the face of the unit are preferred. Occupancy sensors must be rated for operation in ambient air temperatures ranging from 40 to 95 degrees F or temperatures normally encountered in the installed location. Sensors integral to wall mount on-off light switches must have an auto-off switch. Wall switch sensors must be decorator style and must fit behind a standard decorator type wall plate. All occupancy sensors, power packs, and slave packs must be UL listed. In addition to any outputs required for lighting control, the occupancy sensor must provide an output for the HVAC control system.

2.6.9.1 Passive Infrared (PIR) Occupancy Sensors

PIR occupancy sensors must have a multi-level, multi-segmented viewing lens and a conical field of view with a viewing angle of 180 degrees and a detection of at least 20 feet unless otherwise indicated or specified. PIR Sensors must provide field-adjustable background light-level adjustment with an adjustment range suitable to the light level in the sensed area, room or space. PIR sensors must be immune to false triggering from RFI and EMI.

2.6.9.2 Ultrasonic Occupancy Sensors

Ultrasonic sensors must operate at a minimum frequency 32 kHz and must be designed to not interfere with hearing aids.

2.6.9.3 Dual-Technology Occupancy Sensor (PIR and Ultrasonic)

Dual-Technology Occupancy Sensors must meet the requirements of both PIR and Ultrasonic Occupancy Sensors.

2.6.10 Damper End Switches

Each end switch must be a hermetically sealed switch with a trip lever and over-travel mechanism. The switch enclosure must be suitable for mounting on the duct exterior and must permit setting the position of the trip lever that actuates the switch. The trip lever must be aligned with the damper blade.

End switches integral to an electric damper actuator are allowed as long as at least one is adjustable over the travel of the actuator.

2.6.11 Air Quality Sensors

Provide full spectrum air quality sensors using a hot wire element based on the Taguchi principle. The sensor must monitor a wide range of gaseous volatile organic components common in indoor air contaminants like paint fumes, solvents, cigarette smoke, and vehicle exhaust. The sensor must automatically compensate for temperature and humidity, have span and calibration potentiometers, operate on 24 VDC power with output of 0-10 VDC, and have a service rating of 32 to 140 degrees F and 5 to 95 percent relative humidity.

2.7 INDICATING DEVICES

All indicating devices must display readings in English (inch-pound) units.

2.7.1 Thermometers

Provide bi-metal type thermometers at locations indicated. Thermometers must have either 9 inch long scales or 3.5 inch diameter dials, with insertion, immersion, or averaging elements. Provide matching thermowells for pipe-mounted installations. Select scale ranges suitable for the intended service, with the normal operating temperature near the scale's midpoint. The thermometer's accuracy must be plus or minus 2 percent of the scale range.

2.7.1.1 Air-Duct Thermometers

Air-duct thermometers must have perforated stem guards and 45-degree adjustable duct flanges with locking mechanism.

2.7.2 Pressure Gauges

Provide pipe-mounted pressure gauges at the locations indicated. Gauges must conform to ASME B40.100 and have a 4 inch diameter dial and shutoff cock. Select scale ranges suitable for the intended service, with the normal operating pressure near the scale's midpoint. The gauge's accuracy must be plus or minus 2 percent of the scale range.

Gauges must be suitable for field or panel mounting as required, must have black legend on white background, and must have a pointer traveling through a 270-degree arc. Gauge range must be suitable for the application with an upper end of the range not to exceed 150 percent of the design upper limit. Accuracy must be plus or minus 3 percent of scale range. Gauges must meet requirements of ASME B40.100.

2.7.3 Low Differential Pressure Gauges

Gauges for low differential pressure measurements must be a minimum of 3.5 inch (nominal) size with two sets of pressure taps, and must have a diaphragm-actuated pointer, white dial with black figures, and pointer zero adjustment. Gauge range must be suitable for the application with an upper end of the range not to exceed 150 percent of the design upper limit. Accuracy must be plus or minus two percent of scale range.

2.8 OUTPUT DEVICES

2.8.1 Actuators

Actuators must be electric (electronic) . All actuators must be normally open (NO), normally closed (NC) or fail-in-last-position (FILP) as indicated. Normally open and normally closed actuators must be of mechanical spring return type. Electric actuators must have an electronic cut off or other means to provide burnout protection if stalled. Actuators must have a visible position indicator. Electric actuators must provide position feedback to the controller as indicated. Actuators must smoothly and fully open or close the devices to which they are applied. Electric actuators must have a full stroke response time in both directions of 90 seconds or less at rated load. Electric actuators must be of the foot-mounted type with an oil-immersed gear train or the direct-coupled type. Where multiple electric actuators operate from a common signal, the actuators must provide an output signal identical to its input signal to the additional devices. All actuators must be rated for their operating environment. Actuators used outdoors must be designed and rated for outdoor use. Actuators under continuous exposure to water, such as those used in sumps, must be submersible.

Actuators incorporating an integral network connection are considered DDC Hardware and must meet the DDC Hardware requirements of Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS.

2.8.1.1 Damper Actuators

Damper actuators must provide the torque necessary per damper manufacturer's instructions to modulate the dampers smoothly over its full range of operation and torque must be at least 6 inch-pounds/1 square foot of damper area for opposed blade dampers and 9 inch-pounds/1 square foot of damper area for parallel blade dampers.

2.8.1.2 Positive Positioners

Positive positioners must be a pneumatic relay with a mechanical position feedback mechanism and an adjustable operating range and starting point.

2.8.1.3 Electric Actuators

Each actuator must have distinct markings indicating the full-open and full-closed position Each actuator must deliver the torque required for continuous uniform motion and must have internal end switches to limit the travel, or be capable of withstanding continuous stalling without damage. Actuators must function properly within 85 to 110 percent of rated line voltage. Provide actuators with hardened steel running shafts and gears of steel or copper alloy. Fiber or reinforced nylon gears may be used for torques less than 16 inch-pounds..

a. Two-position actuators must be single direction, spring return, or reversing type. Two position actuator signals may either be the control power voltage or line voltage as needed for torque or appropriate interlock circuits.

b. Modulating actuators must be capable of stopping at any point in the cycle, and starting in either direction from any point. Actuators must be equipped with a switch for reversing direction, and a button to disengage the clutch to allow manual adjustments. Provide the

actuator with a hand crank for manual adjustments, as applicable. Modulating actuator input signals can either be a 4 to 20 mAdc or a 0-10 VDC signal.

c. Floating or pulse width modulation actuators are acceptable for non-fail safe applications unless indicated otherwise provided that the floating point control (timed actuation) must have a scheduled re-calibration of span and position no more than once a day and no less than once a week. The schedule for the re-calibration should not affect occupied conditions and be staggered between equipment to prevent falsely loading or unloading central plant equipment.

2.8.2 Relays

Relays must have contacts rated for the intended application, indicator light, and dust proof enclosure. The indicator light must be lit when the coil is energized and off when coil is not energized.

Control relay contacts must have utilization category and ratings selected for the application. Each set of contacts must incorporate a normally open (NO), normally closed (NC) and common contact. Relays must be rated for a minimum life of one million operations.

2.9 USER INPUT DEVICES

User Input Devices, including potentiometers, switches and momentary contact push-buttons. Potentiometers must be of the thumb wheel or sliding bar type. Momentary Contact Push-Buttons may include an adjustable timer for their output. User input devices must be labeled for their function.

2.10 MULTIFUNCTION DEVICES

Multifunction devices are products which combine the functions of multiple sensor, user input or output devices into a single product. Unless otherwise specified, the multifunction device must meet all requirements of each component device. Where the requirements for the component devices conflict, the multifunction device must meet the most stringent of the requirements.

2.10.1 Current Sensing Relay Command Switch

The Current Sensing Relay portion must meet all requirements of the Current Sensing Relay input device. The Command Switch portion must meet all requirements of the Relay output device except that it must have at least one normally-open (NO) contact.

Current Sensing Relays used for Variable Frequency Drives must be rated for Variable Frequency applications unless installed on the source side of the drive. If used in this situation, the threshold for showing status must be set to allow for the VFD's control power when the drive is not enabled and provide indication of operation when the drive is enabled at minimum speed.

2.10.2 Space Sensor Module

Space Sensor Modules must be multifunction devices incorporating a temperature sensor and one or more of the following as specified and indicated on the Space Sensor Module Schedule:

a. A temperature indicating device.

b. A User Input Device which must adjust a temperature setpoint output.

c. A User Input Momentary Contact Button and an output to the control system indicating zone occupancy.

d. A three position User Input Switch labeled to indicate heating, cooling and off positions ('HEAT-COOL-OFF' switch) and providing corresponding outputs to the control system.

e. A two position User Input Switch labeled with 'AUTO' and 'ON' positions and providing corresponding output to the control system..

f. A multi-position User Input Switch with 'OFF' and at least two fan speed positions and providing corresponding outputs to the control system.

Space Sensor Modules cannot contain mercury (Hg).

PART 3 EXECUTION

3.1 INSTALLATION

3.1.1 General Installation Requirements

Perform the installation under the supervision of competent technicians regularly employed in the installation of DDC systems.

3.1.1.1 Device Mounting Criteria

All devices must be installed in accordance with manufacturer's recommendations and as specified and indicated. Control devices to be installed in piping and ductwork must be provided with required gaskets, flanges, thermal compounds, insulation, piping, fittings, and manual valves for shutoff, equalization, purging, and calibration. Strap-on temperature sensing elements must not be used except as specified. Spare thermowells must be installed adjacent to each thermowell containing a sensor and as indicated. Devices located outdoors must have a weathershield.

3.1.1.2 Labels and Tags

Match labels and tags to the unique identifiers indicated on the As-Built drawings. Label all enclosures and instrumentation. Tag all sensors and actuators in mechanical rooms. Tag airflow measurement arrays to show flow rate range for signal output range, duct size, and pitot tube AFMA flow coefficient. Tag duct static pressure taps at the location of the pressure tap. Provide plastic or metal tags, mechanically attached directly to each device or attached by a metal chain or wire. Labels exterior to protective enclosures must be engraved plastic and mechanically attached to the enclosure or instrumentation. Labels inside protective enclosures may attached using adhesive, but must not be hand written.

3.1.2 Weathershield

Provide weathershields for sensors located outdoors. Install

weathershields such that they prevent the sun from directly striking the sensor and prevent rain from directly striking or dripping onto the sensor. Install weather shields with adequate ventilation so that the sensing element responds to the ambient conditions of the surroundings. When installing weathershields near outside air intake ducts, install them such that normal outside air flow does not cause rainwater to strike the sensor.

3.1.3 Room Instrument Mounting

Mount room instruments, including but not limited to wall mounted non-adjustable space sensor modules and sensors located in occupied spaces, 48 inches above the floor unless otherwise indicated. Install adjustable devices to be ADA compliant unless otherwise indicated on the Room Sensor Schedule:

a. Space Sensor Modules for Fan Coil Units may be either unit or wall mounted but not mounted on an exterior wall.

b. Wall mount all other Space Sensor Modules.

3.1.4 Indication Devices Installed in Piping and Liquid Systems

Provide snubbers for gauges in piping systems subject to pulsation. For gauges for steam service use pigtail fittings with cock. Install thermometers and temperature sensing elements in liquid systems in thermowells. Provide spare Pressure/Temperature Ports (Pete's Plug) for all temperature and pressure sensing elements installed in liquid systems for calibration/testing.

3.1.5 Occupancy Sensors

Provide a sufficient quantity of occupancy sensors to provide complete coverage of the area (room or space). Occupancy sensors are to be ceiling mounted. Install occupancy sensors in accordance with NFPA 70 requirements and the manufacturer's instructions. Do not locate occupancy sensors within 6 feet of HVAC outlets or heating ducts, or where they can "see" beyond any doorway. Installation above doorway(s) is preferred. Do not use ultrasonic sensors in spaces containing ceiling fans. Install sensors to detect motion to within 2 feet of all room entrances and to not trigger due to motion outside the room. Set the off-delay timer to 15 minutes unless otherwise indicated. Adjust sensors prior to beneficial occupancy, but after installation of furniture systems, shelving, partitions, etc. For each controlled area, provide one hundred percent coverage capable of detecting small hand-motion movements, accommodating all occupancy habits of single or multiple occupants at any location within the controlled room.

3.1.6 Switches

3.1.6.1 Temperature Limit Switch

Provide a temperature limit switch (freezestat) to sense the temperature at the location indicated. Provide a sufficient number of temperature limit switches (freezestats) to provide complete coverage of the duct section but no less than 1 foot in length per square foot of cross sectional area. Install manual reset limit switches in approved, accessible locations where they can be reset easily. Install temperature limit switch (freezestat) sensing elements in a side-to-side (not

top-to-bottom) serpentine pattern with the relay section at the highest point and in accordance with the manufacturer's installation instructions.

3.1.6.2 Hand-Off Auto Switches

Wire safety controls such as smoke detectors and freeze protection thermostats to protect the equipment during both hand and auto operation.

3.1.7 Temperature Sensors

Install temperature sensors in locations that are accessible and provide a good representation of sensed media. Installations in dead spaces are not acceptable. Calibrate and install sensors according to manufacturer’s instructions. Select sensors only for intended application as designated or recommended by manufacturer.

3.1.7.1 Room Temperature Sensors

Mount the sensors on interior walls to sense the average room temperature at the locations indicated. Avoid locations near heat sources such as copy machines or locations by supply air outlet drafts. Mount the center of all user-adjustable sensors 48 inches above the floor to meet ADA requirements. Non user-adjustable sensors can be mounted as indicated in paragraph ROOM INSTRUMENT MOUNTING.

3.1.7.2 Duct Temperature Sensors

3.1.7.2.1 Probe Type

Place tip of the sensor in the middle of the airstream or in accordance with manufacturer's recommendations or instructions.Provide a gasket between the sensor housing and the duct wall. Seal the duct penetration air tight. When installed in insulated duct, provide enclosure or stand off fitting to accommodate the thickness of duct insulation to allow for maintenance or replacement of the sensor and wiring terminations. Seal the duct insulation penetration vapor tight.

3.1.7.2.2 Averaging Type

Weave the sensing element in a serpentine fashion from side to side perpendicular to the flow, across the duct or air handler cross-section, using durable non-metal supports in accordance with manufacturer's installation instructions. Avoid tight radius bends or kinking of the sensing element. Prevent contact between the sensing element and the duct or air handler internals. Provide a duct access door at the sensor location. The access door must be hinged on the side, factory insulated, have cam type locks, and be as large as the duct will permit, maximum 18 by 18 inches. For sensors inside air handlers, the sensors must be fully accessible through the air handler's access doors without removing any of the air handler's internals.

3.1.7.3 Immersion Temperature Sensors

Provide thermowells for sensors measuring piping, tank, or pressure vessel temperatures. Locate wells to sense continuous flow conditions. Do not install wells using extension couplings. When installed on insulated piping, provide stand enclosure or stand off fitting to accommodate the thickness of the pipe insulation and allow for maintenance or replacement of the sensor or wiring terminations. Where piping diameters are smaller

than the length of the wells, provide wells in piping at elbows to sense flow across entire area of well. Wells must not restrict flow area to less than 70 percent of pipe area. Increase piping size as required to avoid restriction. Provide the sensor well with a heat-sensitive transfer agent between the sensor and the well interior ensuring contact between the sensor and the well.

3.1.7.4 Outside Air Temperature Sensors

Provide outside air temperature sensors on the building's north side with a protective weather shade that does not inhibit free air flow across the sensing element, and protects the sensor from snow, ice, and rain. Location must not be near exhaust hoods and other areas such that it is not influenced by radiation or convection sources which may affect the reading. Provide a shield to shade the sensor from direct sunlight.

3.1.8 Air Flow Measurement Arrays (AFMA)

Locate Outside Air AFMAs downstream from the Outside Air filters.

Install AFMAs with the manufacturer's recommended minimum distances between upstream and downstream disturbances. Airflow straighteners may be used to reduce minimum distances as recommended by the AFMA manufacturer.

3.1.9 Duct Static Pressure Sensors

Locate the duct static pressure sensing tap at 75 percent of the distance between the first and last air terminal units as indicated on the design documents. If the transmitter output is a 0-10Vdc signal, locate the transmitter in the same enclosure as the air handling unit (AHU) controller for the AHU serving the terminal units. If a remote duct static pressure sensor is to be used, run the signal wire back to the controller for the air handling unit.

3.1.10 Relative Humidity Sensors

Install relative humidity sensors in supply air ducts at least 10 feet downstream of humidity injection elements.

3.1.11 Meters

3.1.11.1 Flowmeters

Install flowmeters to ensure minimum straight unobstructed piping for at least 10 pipe diameters upstream and at least 5 pipe diameters downstream of the flowmeter, and in accordance with the manufacturer's installation instructions.

3.1.11.2 Energy Meters

Locate energy meters as indicated. Connect each meter output to the DDC system, to measure both instantaneous demand/energy and other variables as indicated.

3.1.12 Dampers

3.1.12.1 Damper Actuators

Provide spring return actuators which fail to a position that protects the served equipment and space on all control dampers related to freeze protection or force protection. For all outside, makeup and relief dampers provide dampers which fail closed. Terminal fan coil units, terminal VAV units, convectors, and unit heaters nay be non-spring return unless indicated otherwise. Do not mount actuators in the air stream. Do not connect multiple actuators to a common drive shaft. Install actuators so that their action seal the damper to the extent required to maintain leakage at or below the specified rate and so that they move the blades smoothly throughout the full range of motion.

3.1.12.2 Damper Installation

Install dampers straight and true, level in all planes, and square in all dimensions. Dampers must move freely without undue stress due to twisting, racking (parallelogramming), bowing, or other installation error. External linkages must operate smoothly over the entire range of motion, without deformation or slipping of any connecting rods, joints or brackets that will prevent a return to it's normal position. Blades must close completely and leakage must not exceed that specified at the rated static pressure. Provide structural support for multi-section dampers. Acceptable methods of structural support include but are not limited to U-channel, angle iron, corner angles and bolts, bent galvanized steel stiffeners, sleeve attachments, braces, and building structure. Where multi-section dampers are installed in ducts or sleeves, they must not sag due to lack of support. Do not use jackshafts to link more than three damper sections. Do not use blade to blade linkages. Install outside and return air dampers such that their blades direct their respective air streams towards each other to provide for maximum mixing of air streams.

3.1.13 Valves

Install the valves in accordance with the manufacturer's instructions.

3.1.13.1 Valve Actuators

Provide spring return actuators on all control valves where freeze protection is required. Spring return actuators for terminal fan coil units, terminal VAV units, convectors, and unit heaters are not required unless indicated otherwise.

3.1.14 Thermometers and Gauges

3.1.14.1 Local Gauges for Actuators

Provide a pressure gauge at each pneumatic control input and output. Pneumatic actuators must have an accessible and visible pressure gauge installed in the tubing lines at the actuator as indicated.

3.1.14.2 Thermometers

Mount devices to allow reading while standing on the floor or ground, as applicable.

3.1.15 Wire and Cable

Provide complete electrical wiring for the Control System, including wiring to transformer primaries. Wire and Cable must be installed without splices between control devices and in accordance with NFPA 70 and NFPA 90A. Instrumentation grounding must be installed per the device manufacturer's instructions and as necessary to prevent ground loops, noise, and surges from adversely affecting operation of the system. Test installed ground rods as specified in IEEE 142. Cables and conductor wires must be tagged at both ends, with the identifier indicated on the shop drawings. Electrical work must be as specified in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM and as indicated. Wiring external to enclosures must be run in raceways

Install control circuit wiring not in raceways in a neat and safe manner. Wiring must not use the suspended ceiling system (including tiles, frames or hangers) for support. Where conduit or raceways are required, control circuit wiring must not run in the same conduit/raceway as power wiring over 50 volts. Run all circuits over 50 volts in conduit, metallic tubing, covered metal raceways, or armored cable.

3.1.16 Copper Tubing

Provide hard-drawn copper tubing in exposed areas and either hard-drawn or annealed copper tubing in concealed areas. Use only tool-made bends. Use only brass or copper solder joint type fittings, except for connections to apparatus. For connections to apparatus use brass compression type fittings.

3.1.17 Plastic Tubing

Install plastic tubing within covered raceways or conduit except when otherwise specified. Do not use plastic tubing for applications where the tubing could be subjected to a temperature exceeding 130 degrees F. For fittings, use brass or acetal resin of the compression or barbed push-on type for instrument service. Except in walls and exposed locations, plastic multitube instrument tubing bundle without conduit or raceway protection may be used where a number of air lines run to the same points, provided the multitube bundle is enclosed in a protective sheath, is run parallel to the building lines and is adequately supported as specified.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 09 23.02

BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS

PART 1 GENERAL

1.1 SUMMARY
1.1.1 System Requirements
1.1.2 Verification of Specification Requirements
1.1.3 Exisiting Basewide System
1.2 REFERENCES
1.3 DEFINITIONS
1.4 SUBMITTALS

PART 2 PRODUCTS

2.1 NETWORK HARDWARE
2.1.1 BACnet Router
2.1.2 BACnet Gateways
2.1.3 Ethernet Switch
2.2 CONTROL NETWORK WIRING
2.3 DIRECT DIGITAL CONTROL (DDC) HARDWARE
2.3.1 General Requirements
2.3.2 Hardware Input-Output (I/O) Functions
2.3.2.1 Analog Inputs
2.3.2.2 Analog Outputs
2.3.2.3 Binary Inputs
2.3.2.4 Binary Outputs
2.3.2.4.1 Relay Contact Closures
2.3.2.4.2 Triac Outputs
2.3.2.5 Pulse Accumulator
2.3.2.6 ASHRAE 135 Objects for Hardware Inputs and Outputs
2.3.2.7 Integrated H-O-A Switches
2.3.3 Local Display Panel (LDP)
2.3.4 Expansion Modules and Tethered Hardware
2.3.5 Supervisory Control Requirements
2.3.5.1 Alarm Generation Hardware
2.3.6 Niagara Framework Supervisory Gateway
2.4 NIAGARA FRAMEWORK ENGINEERING TOOL

PART 3 EXECUTION

3.1 CONTROL SYSTEM INSTALLATION
3.1.1 Niagara Framework Engineering Tool
3.1.2 Building Control Network (BCN)
3.1.2.1 Building Control Network IP Backbone
3.1.2.2 Building Control Network (BCN) Installation
3.1.3 DDC Hardware
3.1.3.1 Device Identifiers, Network Addresses, and IP addresses
3.1.3.2 ASHRAE 135 Object Name Property and Object Description

Property
3.1.3.3 Niagara Framework Point Names and Descriptions
3.1.3.4 Niagara Station IDs
3.1.3.5 Hand-Off-Auto (H-O-A) Switches
3.1.3.6 Local Display Panels
3.1.3.7 MS/TP Slave Devices
3.1.3.8 Change of Value (COV) and Read Property
3.1.3.9 Engineering Units
3.1.3.10 Occupancy Modes
3.1.3.11 Use of BACnet Objects
3.1.3.11.1 Niagara Framework Objects
3.1.3.12 Use of Standard BACnet Services
3.1.3.13 Device Application Configuration
3.1.3.14 Niagara Framework Engineering Tool
3.1.3.15 Graphics and Web Pages
3.1.4 Scheduling, Alarming, Trending, and Overrides
3.1.4.1 Scheduling
3.1.4.2 Alarm Configuration
3.1.4.3 Configuration of ASHRAE 135 Intrinsic Alarm Generation
3.1.4.4 Trending
3.1.4.5 Overrides
3.1.5 BACnet Gateways
3.1.5.1 General Gateway Requirements

-- End of Section Table of Contents --

SECTION 23 09 23.02

BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS

PART 1 GENERAL

1.1 SUMMARY

Provide a complete Direct Digital Control (DDC) system suitable for the control of the heating, ventilating and air conditioning (HVAC) and other building-level systems as specified and shown and in accordance with Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC.

1.1.1 System Requirements

Provide a system meeting the requirements of both Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC and this Section and with the following characteristics:

a. Except for Gateways, the control system must be an open implementation of BACnet technology using ASHRAE 135 and Fox as the communications protocols. The system must use standard ASHRAE 135 Objects and Properties and the Niagara Framework. The system must use standard ASHRAE 135 Services and the Niagara Framework exclusively for communication over the network. Gateways to packaged units must communicate with other DDC hardware using ASHRAE 135 or the Fox protocol exclusively and may communicate with packaged equipment using other protocols. The control system must be installed such that any two ASHRAE 135 devices on the Internetwork can communicate using standard ASHRAE 135 Services.

b. Install and configure control hardware to provide ASHRAE 135 Objects and Properties or Niagara Framework Objectsas indicated and as needed to meet the requirements of this specification.

c. Use Niagara Framework hardware and software exclusively for scheduling, trending, and communication with a front end (UMCS). Use Niagara Framework or standard BACnet Objects and services for alarming. Use the Fox protocol for all communication between Niagara Framework Supervisory Gateways; use the ASHRAE 135 protocol for all other building communication. Niagara Framework Supervisory Gateway must serve web pages as specified.

d. Use Niagara Framework Version 4.0 or later.

1.1.2 Verification of Specification Requirements

Review all specifications related to the control system installation and advise the Contracting Officer of any discrepancies before performing any work. If Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC or any other Section referenced in this specification is not included in the project specifications advise the Contracting Officer and either obtain the missing Section or obtain Contracting Officer approval before performing any work.

1.1.3 Exisiting Basewide System

Existing basewide BAS system is Honeywell Alerton. New DDC system and all control devices shall be fully compatible with the existing system.

1.2 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS (ASHRAE)

ASHRAE 135	(2020; Interpretation 1-8 2021; Errata 1-2 2021; Addenda CD 2021; Addenda BY-CE 2022; Interpretation 9-10 2022) BACnet—A Data Communication Protocol for Building Automation and Control Networks

BACNET INTERNATIONAL (BTL)

BTL Guide	(v.49; 2017) BACnet Testing Laboratory Implementation Guidelines

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 802.3	(2022) Ethernet

TRIDIUM, INC (TRIDIUM)

Niagara Framework	(2012) NiagaraAX User's Guide
Tridium Open NiCS	(2005) Understanding the NiagaraAX Compatibility Statement (NiCS)

U.S. FEDERAL COMMUNICATIONS COMMISSION (FCC)

FCC Part 15	Radio Frequency Devices (47 CFR 15)

UNDERWRITERS LABORATORIES (UL)

UL 916	(2015; Reprint Oct 2021) UL Standard for Safety Energy Management Equipment

1.3 DEFINITIONS

For definitions related to this section, see Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC.

1.4 SUBMITTALS

Submittal requirements related to this Section are specified in Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC.

PART 2 PRODUCTS

All products used to meet this specification must meet the indicated requirements, but not all products specified here will be required by

every project. All products must meet the requirements both Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC and this Section.

2.1 NETWORK HARDWARE

2.1.1 BACnet Router

All BACnet Routers must be BACnet/IP Routers and must perform layer 3 routing of ASHRAE 135 packets over an IP network in accordance with ASHRAE 135 Annex J and Clause 6. The router must provide the appropriate connection to the IP network and connections to one or more ASHRAE 135 MS/TP networks. Devices used as BACnet Routers must meet the requirements for DDC Hardware, and except for Niagara Framework Supervisory Gateways, devices used as BACnet routers must support the NM-RC-B BIBB.

2.1.2 BACnet Gateways

In addition to the requirements for DDC Hardware, the BACnet Gateway must be a Niagara Framework Supervisory Gateway or must meet the following requirements:

a. It must perform bi-directional protocol translation from one non-ASHRAE 135 protocol to ASHRAE 135. BACnet Gateways must incorporate a network connection to an ASHRAE 135 network (either BACnet over IP in accordance with Annex J or MS/TP) and a separate connection appropriate for the non-ASHRAE 135 protocol and media.

b. It must retain its configuration after a power loss of an indefinite time, and must automatically return to their pre-power loss state once power is restored.

c. It must allow bi-directional mapping of data between the non-ASHRAE 135 protocol and Standard Objects as defined in ASHRAE 135. It must support the DS-RP-B BIBB for Objects requiring read access and the DS-WP-B BIBB for Objects requiring write access.

d. It must support the DS-COV-B BIBB.

Although Gateways must meet DDC Hardware requirements , except for Niagara Framework Supervisory Gateways, they are not DDC Hardware and must not be used when DDC Hardware is required. (Niagara Framework Supervisory Gateways are both Gateways and DDC Hardware.)

2.1.3 Ethernet Switch

Ethernet Switches must autoconfigure between 10,100 and 1000 megabits per second (MBPS).

2.2 CONTROL NETWORK WIRING

a. BACnet MS/TP communications wiring must be in accordance with ASHRAE 135. The wiring must use shielded, three wire (twisted-pair with reference) cable with characteristic impedance between 100 and 120 ohms. Distributed capacitance between conductors must be less than 30 pF per foot.

b. Building Control Network Backbone IP Network must use Ethernet media. Ethernet cables must be CAT-5e at a minimum and meet all requirements

of IEEE 802.3 .

2.3 DIRECT DIGITAL CONTROL (DDC) HARDWARE

2.3.1 General Requirements

All DDC Hardware must meet the following requirements:

a. It must be locally powered and must incorporate a light to indicate the device is receiving power.

b. It must conform to the BTL Guide

c. It must be BACnet Testing Laboratory (BTL) Listed.

d. The Manufacturer's Product Data submittal for each piece of DDC Hardware must include the Protocol Implementation Conformance Statement (PICS) for that hardware as specified in Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC.

e. It must communicate and be interoperable in accordance with ASHRAE 135 and have connections for BACnet IP or MS/TP control network wiring.

f. Other than devices controlling terminal units or functioning solely as a BACnet Router, it must support DS-COV-B, DS-RPM-A and DS-RPM-B BIBBs.

g. Devices supporting the DS-RP-A BIBB must also support the DS-COV-A BIBB.

h. Application programs, configuration settings and communication information must be stored in a manner such that they persist through loss of power:

   (1) Application programs must persist regardless of the length of time power is lost.

   (2) Configured settings must persist for any loss of power less than 2,500 hours.

   (3) Communication information, including but not limited to COV subscriptions, event reporting destinations, Notification Class Object settings, and internal communication settings, must persist for any loss of power less than 2,500 hours.

i. Internal Clocks:

   (1) Clocks in DDC Hardware incorporating a Clock must continue to function for 120 hours upon loss of power to the DDC Hardware.

   (2) DDC Hardware incorporating a Clock must support the DM-TS-B or DM-UTC-B BIBB.

j. It must have all functionality indicated and required to support the application (Sequence of Operation or portion thereof) in which it is used, including but not limited to providing Objects or Niagara Framework Points as specified and as indicated on the Points Schedule.

k. In addition to these general requirements and the DDC Hardware Input-Output (I/O) Function requirements, all DDC Hardware must also

meet any additional requirements for the application in which it is used (e.g. scheduling, alarming, trending, etc.).

l. It must meet FCC Part 15 requirements and have UL 916 or equivalent safety listing.

m. Except for Niagara Framework Supervisory Gateways, Device must support Commandable Objects to support Override requirements as detailed in PART 3 EXECUTION

n. User interfaces which allow for modification of Properties or settings must be password-protected.

o. Devices communicating BACnet MS/TP must meet the following requirements:

(1) Must have a configurable Max_Master Property.

(2) DDC Hardware other than hardware controlling a single terminal unit must have a configurable Max_Info_Frames Property.

(3) Must respond to any valid request within 50 msec with either the appropriate response or with a response of "Reply Postponed".

(4) Must use twisted pair with reference and shield (3-wire media) wiring.

p. Devices communicating BACnet/IP must use UDP Port 0xBAC0. Devices with configurable UDP Ports must default to 0xBAC0.

q. All Device IDs, Network Numbers, and BACnet MAC addresses of devices must be fully configurable without limitation, except MS/TP MAC addresses may be limited by ASHRAE 135 requirements.

r. Except for Niagara Framework Supervisory Gateways, DDC Hardware controlling a single terminal unit must have:

(1) Objects (including the Device Object) with an Object Name Property of at least 8 characters in length.

(2) A configurable Device Object Name.

(3) A configurable Device Object Description Property at least 16 characters in length.

s. Except for Objects in either Niagara Framework Supervisory Gateways or DDC Hardware controlling a single terminal unit, all Objects (including Device Objects) must:

(1) Have a configurable Object Name Property of at least 12 characters in length.

(2) Have a configurable Object Description Property of at least 24 characters in length.

t. For programmable DDC Hardware, provide and license to the project site all programming software required to program the Hardware in accordance with Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC.

u. For programmable DDC Hardware, provide copies of the installed application programs (all software that is not common to every controller of the same manufacturer and model) as source code compatible with the supplied programming software in accordance with Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC. The submitted application program must be the complete application necessary for controller to function as installed and be sufficient to allow replacement of the installed controller with another controller of the same type.

2.3.2 Hardware Input-Output (I/O) Functions

DDC Hardware incorporating hardware input-output (I/O) functions must meet the following requirements:

2.3.2.1 Analog Inputs

DC Hardware analog inputs (AIs) must be implemented using ASHRAE 135 Analog Input Objects and perform analog to digital (A-to-D) conversion with a minimum resolution of 8 bits plus sign or better as needed to meet the accuracy requirements specified in Section 23 09 00. Signal conditioning including transient rejection must be provided for each analog input. Analog inputs must be capable of being individually calibrated for zero and span. Calibration via software scaling performed as part of point configuration is acceptable. The AI must incorporate common mode noise rejection of at least 50 dB from 0 to 100 Hz for differential inputs, and normal mode noise rejection of at least 20 dB at 60 Hz from a source impedance of 10,000 ohms.

2.3.2.2 Analog Outputs

DDC Hardware analog outputs (AOs) must be implemented using ASHRAE 135 Analog Output Objects and perform digital to analog (D-to-A) conversion with a minimum resolution of 8 bits plus sign, and output a signal with a range of 4-20 mAdc or 0-10 Vdc. Analog outputs must be capable of being individually calibrated for zero and span. Calibration via software scaling performed as part of point configuration is acceptable. DDC Hardware with Hand-Off-Auto (H-O-A) switches for analog outputs must provide for overriding the output through the range of 0 percent to 100 percent

2.3.2.3 Binary Inputs

DDC Hardware binary inputs (BIs) must be implemented using ASHRAE 135 Binary Input Objects and accept contact closures and must ignore transients of less than 5 milli-second duration. Protection against a transient 50VAC must be provided.

2.3.2.4 Binary Outputs

DDC Hardware binary outputs (BOs) must be implemented using ASHRAE 135 Binary Output Objects and provide relay contact closures or triac outputs for momentary and maintained operation of output devices. DDC Hardware with H-O-A switches for binary outputs must provide for overriding the output open or closed.

2.3.2.4.1 Relay Contact Closures

Closures must have a minimum duration of 0.1 second. Relays must provide

at least 180V of isolation. Electromagnetic interference suppression must be provided on all output lines to limit transients to 50 Vac. Minimum contact rating must be 0.5 amperes at 24 Vac.

2.3.2.4.2 Triac Outputs

Triac outputs must provide at least 180 V of isolation. Minimum contact rating must be 0.5 amperes at 24 Vac.

2.3.2.5 Pulse Accumulator

DDC Hardware pulse accumulators must be implemented using either an ASHRAE 135 Accumulator Object or an ASHRAE 135 Analog Value Object where the Present_Value is the totalized pulse count. Pulse accumulators must accept contact closures, ignore transients less than 5 msec duration, protect against
transients of 50 VAC, and accept rates of at least 20 pulses per second.

2.3.2.6 ASHRAE 135 Objects for Hardware Inputs and Outputs

The requirements for use of ASHRAE 135 objects for hardware input and outputs includes devices where the hardware sensor or actuator is integral to the controller (e.g. a VAV box with integral damper actuator, a smart sensor, a VFD, etc.)

2.3.2.7 Integrated H-O-A Switches

Where integrated H-O-A switches are provided on hardware outputs, controller must provide means of monitoring position or status of H-O-A switch. This feedback may be provided via the Niagara Framework or via any valid BACnet method, including the use of proprietary Objects, Properties, or Services.

2.3.3 Local Display Panel (LDP)

The Local Display Panels (LDPs) must be DDC Hardware with a display and navigation buttons or a touch screen display, and must provide display and adjustment of Niagara Framework points or ASHRAE 135 Properties as indicated on the Points Schedule and as specified. LDPs must be either BTL Listed as a B-OD, B-OWS, B-AWS, or be an integral part of another piece of DDC Hardware listed as a B-BC. For LDPs listed as B-OWS or B-AWS, the hardware must be BTL listed and the product must come factory installed with all applications necessary for the device to function as an LDP.

The adjustment of values using display and navigation buttons must be password protected.

2.3.4 Expansion Modules and Tethered Hardware

A single piece of DDC Hardware may consist of a base unit and also:

a. An unlimited number of hardware expansion modules, where the individual hardware expansion modules are designed to directly connect, both mechanically and electrically, to the base unit hardware. The expansion modules must be commercially available as an optional add-on to the base unit.

b. A single piece of hardware connected (tethered) to a base unit by a single cable where the cable carries a proprietary protocol between the base unit and tethered hardware. The tethered hardware must not contain control logic and be commercially available as an optional add-on to the base unit as a single package.

   Note that this restriction on tethered hardware does not apply to sensors or actuators using standard binary or analog signals (not a communications protocol); sensors or actuators using standard binary or analog signals are not considered part of the DDC Hardware.

Hardware capable of being installed stand-alone, or without a separate base unit, is DDC Hardware and must not be used as expansion modules or tethered hardware.

2.3.5 Supervisory Control Requirements

2.3.5.1 Alarm Generation Hardware

Non-Niagara Framework DDC Hardware used for alarm generation must meet the following requirements:

a. Device must support the AE-N-I-B BIBB

b. The Recipient_List Property must be Writable for all Notification Class Objects used for alarm generation.

c. For all Objects implementing Intrinsic Alarming, the following Properties must be Writable:

   (1) Time_Delay
   (2) High_Limit
   (3) Low_Limit
   (4) Deadband
   (5) Event_Enable
   (6) If the issue date of this project specification is after 1 January 2016, Time_Delay_Normal must be writable.

d. It is preferred, but not required, that devices support the DM-OCD-B BIBB on all Notification Class Objects. It is also preferred, but not required that devices supporting the DM-OCD-B BIBB accept any valid value as an initial value for properties of Notification Class Objects.

2.3.6 Niagara Framework Supervisory Gateway

Any device implementing the Niagara Framework is a Niagara Framework Supervisory Gateway and must meet these requirements. In addition to the general requirements for all DDC Hardware, Niagara Framework Supervisory Gateway Hardware must:

a. Be direct digital control hardware.

b. Have an unrestricted interoperability license and its Niagara Compatibility Statement (NiCS) must follow the Tridium Open NiCS Specification.

c. Manage communications between a field control network and the Niagara Framework Monitoring and Control Software, and between itself and other Niagara Framework Supervisory Gateways. Niagara Framework

Supervisory Gateway Hardware must use Fox protocol for communication with other Niagara Framework Components, regardless of the manufacturer of the other components.

d. Be fully programmable using the Niagara Framework Engineering Tool and must support the following:

(1) Time synchronization, Calendar, and Scheduling using Niagara Scheduling Objects

(2) Alarm generation and routing using the Niagara Alarm Service

(3) Trending using the Niagara History Service and Niagara Trend Log Objects

(4) Integration of field control networks using the Niagara Framework Engineering Tool

(5) Configuration of integrated field control system using the Niagara Framework Engineering Tool when supported by the field control system

e. Meet the following minimum hardware requirements:

(1) One 10/100 Mbps Ethernet Port

(2) One or more MS/TP ports.

f. Provide access to field control network data and supervisory functions via web interface and support a minimum of 16 simultaneous users. Note: implementation of this capability may not be required on all projects.

g. Submit a backup of each Niagara Framework Supervisory Gateway as specified in Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC. The backup must be sufficient to restore a Niagara Framework Supervisory Gateway to the final as-built condition such that a new Niagara Framework Supervisory Gateway loaded with the backup is indistinguishable in functionality from the original.

2.4 NIAGARA FRAMEWORK ENGINEERING TOOL

The Niagara Framework Engineering Tool must be Niagara Workbench or an equivalent Niagara Framework engineering tool software must:

a. Have an unrestricted interoperability license and its Niagara Compatibility Statement (NiCS) must follow the Tridium Open NiCS Specification.

b. Be capable of performing network configuration for Niagara Framework Supervisory Gateways and Niagara Framework Monitoring and Control Software.

c. Be capable of programming and configuring of Niagara Framework Supervisory Gateways and Niagara Framework Monitoring and Control Software.

d. Be capable of discovery of Niagara Framework Supervisory Gateways and all points mapped into each Niagara Framework Supervisory Gateway and

making these points accessible to Niagara Framework Monitoring and Control Software.

PART 3 EXECUTION

3.1 CONTROL SYSTEM INSTALLATION3.1.1 Niagara Framework Engineering Tool

Provide a Niagara Framework Engineering Tool.

3.1.2 Building Control Network (BCN)

Install the Building Control Network (BCN) as a single BACnet Internetwork consisting of a single IP network as the BCN Backbone and zero or more BACnet MS/TP networks. Note that in some cases there may only be a single device on the BCN Backbone.

Except for the IP Network and as permitted for the non-BACnet side of Gateways, use exclusively ASHRAE 135 networks.

3.1.2.1 Building Control Network IP Backbone

Install IP Network Cabling in conduit. Install Ethernet Switches in lockable enclosures. Install the Building Control Network (BCN) IP Backbone such that it is available at the Facility Point of Connection (FPOC) location as indicated. When the FPOC location is a room number, provide sufficient additional media to ensure that the Building Control Network (BCN) IP Backbone can be extended to any location in the room.

Use UDP port 0xBAC0 for all BACnet traffic on the IP network. (Note that in a Niagara Framework system there may not be BACnet traffic on the IP Network)

3.1.2.2 Building Control Network (BCN) Installation

Provide a building control network meeting the following requirements:

a. Install all DDC Hardware connected to the Building Control Network.

b. Where multiple pieces of DDC Hardware are used to execute one sequence, install all DDC Hardware executing that sequence on a single MS/TP network dedicated to that sequence.

c. Traffic between BACnet networks must be exclusively via BACnet routers.

d. Use the Fox protocol for all traffic both originating and terminating at Niagara Framework components. Use the Fox protocol for all traffic originating or terminating at a Niagara Framework UMCS (including traffic to or from a future UMCS). All other traffic, including traffic between ASHRAE 135 devices and traffic between Niagara Framework Supervisory Gateways and ASHRAE 135 devices must be in accordance with ASHRAE 135.

3.1.3 DDC Hardware

Install all DDC Hardware that connects to an IP network in lockable enclosure. Install other DDC Hardware that is not in suspended ceilings in lockable enclosures. For all DDC hardware with a user interface, coordinate with site to determine proper passwords and configure passwords into device.

a. Except for zone sensors (thermostats), install all Tethered Hardware within 6 feet of its base unit.

b. Install and configure all BTL-Listed devices in a manner consistent with their BTL Listing such that the device as provided still meets all requirements necessary for its BTL Listing.

c. Install and configure all BTL-Listed devices in a manner consistent with the BTL Device Implementation Guidelines such that the device as provided meets all those Guidelines.

3.1.3.1 Device Identifiers, Network Addresses, and IP addresses

a. Do not use any Device Identifier or Network Number already used by another BACnet system at the project site. .

b. Coordinate device IP addresses with installation. The installation POC is .

3.1.3.2 ASHRAE 135 Object Name Property and Object Description Property

Configure the Object_Names and Object_Descriptions properties of all ASHRAE 135 Objects (including Device Objects) as indicated on the Points Schedule (Point Name and Point Description) and as specified. At a minimum:

a. Except for DDC Hardware controlling a single terminal unit, configure the Object_Name and Object_Description properties of all Objects (including Device Objects) as indicated on the Points Schedule and as specified.

b. In DDC Hardware controlling a single terminal unit, configure the Device Object_Name and Device Object_Description as indicated on the Points Schedule and as specified.

When Points Schedule entries exceed the length limitations in the device, notify the user and provide recommended alternatives for approval.

3.1.3.3 Niagara Framework Point Names and Descriptions

Configure the names and descriptions of all Points in Niagara Framework Supervisory Gateways as indicated on the Points Schedule and as specified.

3.1.3.4 Niagara Station IDs

Ensure that Niagara Station IDs of new Niagara Framework Supervisory Gateways are maintained as unique within UMCS front-end, including ensuring they do not conflict with any existing Niagara Station ID.

3.1.3.5 Hand-Off-Auto (H-O-A) Switches

Provide Hand-Off-Auto (H-O-A) switches as specified and as indicated on the Points Schedule. Provide H-O-A switches that are integral to the controller hardware, an external device co-located with (in the same enclosure as) the controller, integral to the controlled equipment, or an external device co-located with (in the same enclosure as) the controlled equipment.

a. For H-O-A switches integral to DDC Hardware, meet the requirements specified in paragraph DIRECT DIGITAL CONTROL (DDC) HARDWARE.

b. For external H-O-A switches used for binary outputs, provide for overriding the output open or closed.

c. For eternal H-O-A switches used for analog outputs, provide for overriding through the range of 0 percent to 100 percent.

3.1.3.6 Local Display Panels

Provide LDPs to display and override values of points in a Niagara Framework Supervisory Gateway or ASHRAE 135 Object Properties as indicated on the Points Schedule. Install LDPs displaying points for anything other than a terminal unit in the same room as the equipment. Install LDPs displaying points for only terminal units in a mechanical room central to the group of terminal units it serves. For LDPs using WriteProperty to commandable objects to implement an override, write values with priority 9.

3.1.3.7 MS/TP Slave Devices

Configure all MS/TP devices as Master devices. Do not configure any devices to act as slave devices.

3.1.3.8 Change of Value (COV) and Read Property

a. To the greatest extent possible, configure all devices to support the SubscribeCOV service (the DS-COV-B BIBB). At a minimum, all devices supporting the DS-RP-B BIBB, other than devices controlling only a single terminal unit, must be configured to support the DS-COV-B BIBB.

b. Whenever supported by the server side, configure client devices to use the DS-COV-A BIBB.

3.1.3.9 Engineering Units

Configure devices to use English (Inch-Pound) engineering units as follows:

a. Temperature in degrees F

b. Air or natural gas flows in cubic feet per minute (CFM)

c. Water in gallons per minute (GPM)

d. Differential Air pressures in inches of water column (IWC)

e. Enthalpy in BTU/lb

f. Heating and cooling energy in MBTU (1MBTU = 1,000,000 BTU))

g. Cooling load in tons (1 ton = 12,000 BTU/hour)

h. Heating load in MBTU/hour (1MBTU = 1,000,000 BTU)

i. Electrical Power: kilowatts (kW)

j. Electrical Energy: kilowatt-hours (kWh)

3.1.3.10 Occupancy Modes

Use the following correspondence between value and occupancy mode whenever an occupancy state or value is required:

a. OCCUPIED mode: a value of one
b. UNOCCUPIED mode: a value of two
c. WARM-UP/COOL-DOWN (PRE-OCCUPANCY) mode: a value of three

Note that elsewhere in this Section the Schedule Object is required to also support a value of four, which is reserved for future use. Also note that the behavior of a system in each of these occupancy modes is indicated in the sequence of operation for the system.

3.1.3.11 Use of BACnet Objects

Except as specifically indicated for Niagara Framework Objects, Use only standard non-proprietary ASHRAE 135 Objects and services to accomplish the project scope of work as follows:

a. Use Analog Input or Analog Output Objects for all analog hardware I/O. Do not use Analog Value Object for analog hardware I/O) .

b. Use Binary Input or Binary Output Objects for all binary hardware I/O. Do not use Binary Value Objects for binary hardware I/O.

c. Use Analog Value Objects for analog setpoints.

d. Use Accumulator Objects or Analog Value Objects for pulse inputs.

e. For occupancy modes, use Multistate Value Objects and the correspondence between value and occupancy mode specified in paragraph OCCUPANCY MODES.

f. Use a combination of Niagara Framework Alarm Extensions and Alarm Services, Intrinsic Alarming, and Notification Class Objects for alarm generation.

g. For all other points shown on the Points Schedule as requiring an ASHRAE 135 Object, use the Object type shown on the Points Schedule or, if no Object Type is shown, use a standard Object appropriate to the point.

3.1.3.11.1 Niagara Framework Objects

Points in the Niagara Framework Supervisory Gateway, even if used in a sequence or are shown on the Points Schedule, are not required to be exposed as BACnet Objects unless they are required to be available on the network by another device or sequence of operation (i.e. there is some other reason they are needed).

Use a Niagara Framework Supervisory Gateway as specified for all scheduling and trending. Use a Niagara Framework Supervisory Gateway as specified for all alarming except for intrinsic alarming.

3.1.3.12 Use of Standard BACnet Services

Except as noted in this paragraph, for all DDC Hardware (including Niagara Frameworks Supervisory Gateways when communicating with non-Niagara

Framework DDC Hardware) use Standard BACnet Services as defined in this specification (which excludes some ASHRAE 135 services) exclusively for application control functionality and communication.

DDC Hardware that cannot meet this requirement may use non-standard services provided they can provide identical functionality using Standard BACnet Services when communicating with BACnet devices from a different vendor. When implementing non-standard services, document all non-standard services in the DDC Hardware Schedule as specified and as specified in Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC.

3.1.3.13 Device Application Configuration

a. For every property, setting or value shown on the Points Schedule or otherwise indicated as Configurable, provide a value that is retained through loss of power and can be changed via one or more of:

(1) BACnet services (including proprietary services)

(2) Hardware settings on the device

(3) The Niagara Framework

b. For every property, setting or value in non-Niagara Framework Hardware shown on the Points Schedule or otherwise indicated as Operator Configurable, provide a value that is retained through loss of power and can be changed via one or more of:

(1) A Writable Property of a standard BACnet Object

(2) A Property of a standard BACnet Object that is Writable when Out_Of_Service is TRUE and Out_Of_Service is Writable.

(3) Using some other method supported by a Niagara Framework Supervisory Gateway

c. Configure Niagara Framework Supervisory Gateways such that the property, setting or value is configurable from a Niagara Framework Front End.

d. For every property, setting or value in a Niagara Framework Supervisory Gateway which is shown on the Points Schedule or otherwise indicated as Operator Configurable, configure the value to be configurable from within the Niagara Framework such that it can be configured from a system graphic page at a Niagara Framework Front End.

3.1.3.14 Niagara Framework Engineering Tool

Use the Niagara Framework Engineering Tool to fully discover the field control system and make all field control system information available to the Niagara Framework Supervisory Gateway. Ensure that all points on the points schedule are available to the front end via the Fox protocol.

3.1.3.15 Graphics and Web Pages

Configure Niagara Framework Supervisory Gateways to use web pages to provide a graphical user interface including System Displays using the project site sample displays, including overrides, as indicated on the Points Schedule and as specified. Label all points on displays with the point description as indicated on the Points Schedule. Configure user

permissions for access to and executions of action using graphic pages. Coordinate user permissions with the Controls shop supervisor. Configure the web server to use HTTPS based on the Transport Layer Security (TLS) protocol in accordance with RFC 5246 using a Government furnished certificate.

3.1.4 Scheduling, Alarming, Trending, and Overrides

3.1.4.1 Scheduling

Configure schedules in Niagara Framework Supervisory Gateway using Niagara Schedule Objects as indicated on the Points Schedule and as specified. When the schedule is controlling occupancy modes in DDC Hardware other than a Niagara Framework Supervisory Gateway use the indicated correspondence between value and occupancy mode.

Provide a separate schedule for each AHU including it's associated Terminal Units and for each stand-alone Terminal Unit (those not dependent upon AHU service) or group of stand-alone Terminal Units acting according to a common schedule as indicated.

3.1.4.2 Alarm Configuration

Configure alarm generation and management as indicated on the Points Schedule and as specified. Configure alarm generation in Niagara Framework Supervisory Gateways using Niagara Framework Alarm Extensions and Alarm Services or in other DDC Hardware (not Niagara Framework Supervisory Gateways) using ASHRAE 135 Intrinsic Alarming. Configure alarm management and routing for all alarms, including those generated via intrinsic alarming in other devices, in the Niagara Framework Supervisory Gateway such that the alarms are able to be accessed from the Niagara Framework Front End.

Where Intrinsic Alarming is used, configure intrinsic alarming as specified in paragraph "Configuration of ASHRAE 135 Intrinsic Alarm Generation". Configure a Niagara Framework Supervisory Gateway to provide a means to configure the intrinsic alarm parameters such that the Intrinsic Alarm is configurable from the front end via the Niagara Framework.

3.1.4.3 Configuration of ASHRAE 135 Intrinsic Alarm Generation

Intrinsic alarm generation must meet the following requirements:

Configure alarm generation as indicated on the Points Schedule and as specified using Intrinsic Alarming in accordance with ASHRAE 135 or Algorithmic Alarming in accordance with ASHRAE 135. Alarm generation must meet the following requirements:

a. Send alarm events as Alarms (not Events).

b. Use the ConfirmedNotification Service for alarm events.

c. For alarm generation, support two priority levels for alarms: critical and non-critical. Configure the Priority of Notification Class Objects to use Priority 112 for critical and 224 for non-critical alarms.

d. Number of Notification Class Objects for Alarm Generation:

(1) If the device implements non-critical alarms, or if any Object in the device supports Intrinsic Alarms, then provide a single Notification Class Object specifically for (shared by) all non-critical alarms.

(2) If the device implements critical alarms, provide a single Notification Class Object specifically for (shared by) all critical alarms.

(3) If the device implements both critical and non-critical alarms, provide both Notification Class Objects (one for critical, one for non-critical).

(4) If the device controls equipment other than a single terminal unit, provide both Notification Class Objects (one for critical, one for non-critical) even if no alarm generation is required at time of installation.

e. For all intrinsic alarms configure the Limit_Enable Property to set both HighLimitEnable and LowLimitEnable to TRUE. If the specified alarm conditions are for a single-sided alarm (only High_Limit used or only Low_Limit used) assign a value to the unused limit such that the unused alarm condition will not occur.

f. For all objects supporting intrinsic alarming, even if no alarm generation is required during installation, configure the following Properties as follows:

(1) Notification_Class to point to the non-Critical Notification Class Object in that device.

(2) Limit_Enable to enable both the HighLimitEnable and LowLimitEnable

(3) Notify_Type to Alarm

g. Configure the Recipient_List Property of the Notification Class Object to point to the Niagara Framework Supervisory Gateway managing the alarm.

3.1.4.4 Trending

Perform all trending using a Niagara Framework Supervisory Gateway using Niagara Framework History Extensions and Niagara Framework History Service exclusively.

3.1.4.5 Overrides

Provide an override for each point shown on the Points Schedule as requiring an override. Use the Niagara Framework for all overrides to points in Niagara Framework Supervisory Gateways. For overrides to other points, provide an override to a point in a Niagara Framework Supervisory Gateway via the Niagara Framework where the Niagara Framework Supervisory Gateway overrides the other point as specified.

Unless otherwise approved, provide Commandable Objects to support all Overrides in non-Niagara Framework Supervisory Gateway DDC Hardware. With specific approval from the Contracting Officer, Overrides for points which are not hardware outputs and which are in DDC hardware controlling a

single terminal unit may support overrides via an additional Object provided for the override. No other means of implementing Overrides may be used.

a. Where Commandable Objects are used, ensure that WriteProperty service requests with a Priority of 10 or less take precedence over the SEQUENCE VALUE and that WriteProperty service request with a priority of 11 or more have a lower precedence than the SEQUENCE VALUE.

b. For devices implementing overrides via additional Objects, provide Objects which are NOT Written to as part of the normal Sequence of Operations and are Writable when Out_Of_Service is TRUE and Out_Of_Service is Writable. Use this point as an Override of the normal value when Out_Of_Service is TRUE and the normal value otherwise. Note these Objects may be modified as part of the sequence via local processes, but must not be modified by local processes when Out_Of_Service is TRUE.

3.1.5 BACnet Gateways

The requirements in this paragraph do not themselves permit the installation of hardware not meeting the other requirements of this section. Except for proprietary systems specifically indicated in Section 23 09 00, all control hardware installed under this project must meet the requirements of this specification, including the control hardware providing the network interface for a package unit or split system specified under another section. Only use gateways to connect to pre-existing control devices, and to proprietary systems specifically permitted by Section 23 09 00.

3.1.5.1 General Gateway Requirements

Provide BACnet Gateways to connect non-BACnet control hardware in accordance with the following:

a. Configure gateways to map writable data points in the controlled equipment to Writable Properties of Standard Objects, or to Niagara Framework points, as indicated in the Points Schedule and as specified.

b. Configure gateway to map readable data points in the controlled equipment to Readable Properties of Standard Objects, or to Niagara Framework points, as indicated in the Points Schedule and as specified.

c. Configure gateway to support the DS-COV-B BIBB for all points mapped to BACnet Objects.

d. Do not use non-BACnet control hardware for controlling built-up units or any other equipment that was not furnished with factory-installed controls. (Note: A Niagara Framework Supervisory Gateway is BACnet control hardware.)

e. Do not use non-BACnet control hardware for system scheduling functions.

f. Each gateway must communicate with and perform protocol translation for non-BACnet control hardware controlling one and only one package unit or a single non-BACnet system specifically permitted by Section 23 09 00.

g. Connect one network port on the gateway to the Building Control

Backbone IP Network or to a BACnet MS/TP network and the other port to the single piece of controlled equipment or the non-BACnet system specifically permitted by Section 23 09 00..

h. For gateways to existing package units or simple split systems, non-BACnet network wiring connecting the gateway to the package unit must not exceed 10 feet in length and must connect to exactly two devices: the controlled equipment (packaged unit) or split system interface and the gateway.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 23 00

REFRIGERANT PIPING

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 QUALITY ASSURANCE
1.3.1 Qualifications
1.3.2 Contract Drawings
1.4 DELIVERY, STORAGE, AND HANDLING
1.5 MAINTENANCE
1.5.1 General
1.5.2 Extra Materials

PART 2 PRODUCTS

2.1 STANDARD COMMERCIAL PRODUCTS
2.2 ELECTRICAL WORK
2.3 REFRIGERANT PIPING SYSTEM
2.4 PIPE, FITTINGS AND END CONNECTIONS (JOINTS)
2.4.1 Copper Tubing
2.4.2 Solder
2.4.3 Brazing Filler Metal
2.4.4 Brazing Flux
2.4.5 Press Fittings
2.5 VALVES
2.5.1 Refrigerant Stop Valves
2.5.2 Check Valves
2.5.3 Liquid Solenoid Valves
2.5.4 Expansion Valves
2.5.5 Electronic Expansion Valves
2.5.6 Safety Relief Valves
2.5.7 Evaporator Pressure Regulators, Direct-Acting
2.5.8 Refrigerant Access Valves
2.6 PIPING ACCESSORIES
2.6.1 Filter Driers
2.6.2 Sight Glass and Liquid Level Indicator
2.6.2.1 Assembly and Components
2.6.2.2 Gauge Glass
2.6.2.3 Bull's-Eye and Inline Sight Glass Reflex Lens
2.6.2.4 Moisture Indicator
2.6.3 Vibration Dampeners
2.6.4 Flexible Pipe Connectors
2.6.5 Strainers
2.6.6 Pressure and Vacuum Gauges
2.6.7 Temperature Gauges
2.6.7.1 Stem Cased-Glass
2.6.7.2 Bimetallic Dial

2.6.7.3 Liquid-, Solid-, and Vapor-Filled Dial
2.6.7.4 Thermowell
2.6.8 Pipe Hangers, Inserts, and Supports
2.6.9 Escutcheons
2.7 FABRICATION
2.7.1 Factory Applied Insulation

PART 3 EXECUTION

3.1 EXAMINATION
3.2 INSTALLATION
3.2.1 Directional Changes
3.2.2 Functional Requirements
3.2.3 Fittings and End Connections
3.2.3.1 Threaded Connections
3.2.3.2 Brazed Connections
3.2.3.3 Welded Connections
3.2.3.4 Flared Connections
3.2.3.5 Flanged Connections
3.2.4 Valves
3.2.4.1 General
3.2.4.2 Expansion Valves
3.2.4.3 Valve Identification
3.2.5 Vibration Dampers
3.2.6 Strainers
3.2.7 Filter Dryer
3.2.8 Sight Glass
3.2.9 Discharge Line Oil Separator
3.2.10 Accumulator
3.2.11 Flexible Pipe Connectors
3.2.12 Temperature Gauges
3.2.13 Pipe Hangers, Inserts, and Supports
3.2.13.1 Hangers
3.2.13.2 Inserts
3.2.13.3 C-Clamps
3.2.13.4 Angle Attachments
3.2.13.5 Saddles and Shields
3.2.13.6 Horizontal Pipe Supports
3.2.13.7 Vertical Pipe Supports
3.2.13.8 Pipe Guides
3.2.13.9 Steel Slides
3.2.13.10 High Temperature Guides with Cradles
3.2.13.11 Multiple Pipe Runs
3.2.13.12 Seismic Requirements
3.2.13.13 Structural Attachments
3.2.14 Pipe Alignment Guides
3.2.15 Pipe Anchors
3.2.16 Building Surface Penetrations
3.2.16.1 Refrigerated Space
3.2.16.2 General Service Areas
3.2.16.3 Waterproof Penetrations
3.2.16.3.1 Waterproofing Clamping Flange
3.2.16.3.2 Modular Mechanical Type Sealing Assembly
3.2.16.4 Fire-Rated Penetrations
3.2.16.5 Escutcheons
3.2.17 Access Panels
3.2.18 Field Applied Insulation
3.2.19 Field Painting
3.2.19.1 Color Coding

3.2.19.2 Color Coding Scheme
3.2.20 Identification Tags
3.3 CLEANING AND ADJUSTING
3.4 REFRIGERANT PIPING TESTS
3.4.1 Preliminary Procedures
3.4.2 Pneumatic Test
3.4.3 Evacuation Test
3.4.4 System Charging and Startup Test
3.4.5 Refrigerant Leakage
3.4.6 Contractor's Responsibility

-- End of Section Table of Contents --

SECTION 23 23 00

REFRIGERANT PIPING

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AIR-CONDITIONING, HEATING AND REFRIGERATION INSTITUTE (AHRI)

AHRI 710 I-P	(2009) Performance Rating of Liquid-Line Driers
AHRI 720	(2002) Refrigerant Access Valves and Hose Connectors
AHRI 750 I-P	(2016) Performance Rating of Thermostatic Refrigerant Expansion Valves
AHRI 760 I-P	(2014) Performance Rating of Solenoid Valves for Use with Volatile Refrigerants
AHRI 1370 I-P	(2017) Performance Rating of Electronic Expansion Valves

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS (ASHRAE)

ASHRAE 15 & 34	(2013) ASHRAE Standard 34-2016 Safety Standard for Refrigeration Systems/ASHRAE Standard 34-2016 Designation and Safety Classification of Refrigerants-ASHRAE Standard 34-2016
ASHRAE 17	(2015) Method of Testing Capacity of Thermostatic Refrigerant Expansion Valves
ASHRAE 90.1 - IP	(2019; Errata 1 2019; Errata 2-5 2020; Addenda BY-CP 2020; Addenda AF-DB 2020; Addenda A-G 2020; Addenda F-Y 2021; Errata 6-8 2021; Interpretation 1-4 2020; Interpretation 5-8 2021 Addenda AS-AQ 2022) Energy Standard for Buildings Except Low-Rise Residential Buildings

AMERICAN SOCIETY OF MECHANICAL ENGINEERS (ASME)

ASME B16.22	(2021) Wrought Copper and Copper Alloy Solder Joint Pressure Fittings
ASME B16.26	(2018) Standard for Cast Copper Alloy Fittings for Flared Copper Tubes

ASME B31.1	(2020) Power Piping
ASME B31.5	(2020) Refrigeration Piping and Heat Transfer Components
ASME B40.100	(2013) Pressure Gauges and Gauge Attachments

AMERICAN WELDING SOCIETY (AWS)

AWS A5.8/A5.8M	(2019) Specification for Filler Metals for Brazing and Braze Welding
AWS A5.31/A5.31M	(2012) Specification for Fluxes for Brazing and Braze Welding
AWS BRH	(2007; 5th Ed) Brazing Handbook
AWS D1.1/D1.1M	(2020; Errata 1 2021) Structural Welding Code - Steel
AWS Z49.1	(2021) Safety in Welding and Cutting and Allied Processes

ASTM INTERNATIONAL (ASTM)

ASTM A53/A53M	(2022) Standard Specification for Pipe, Steel, Black and Hot-Dipped, Zinc-Coated, Welded and Seamless
ASTM A653/A653M	(2020) Standard Specification for Steel Sheet, Zinc-Coated (Galvanized) or Zinc-Iron Alloy-Coated (Galvannealed) by the Hot-Dip Process
ASTM B32	(2020) Standard Specification for Solder Metal
ASTM B62	(2017) Standard Specification for Composition Bronze or Ounce Metal Castings
ASTM B75/B75M	(2020) Standard Specification for Seamless Copper Tube
ASTM B280	(2020) Standard Specification for Seamless Copper Tube for Air Conditioning and Refrigeration Field Service
ASTM B813	(2016) Standard Specification for Liquid and Paste Fluxes for Soldering of Copper and Copper Alloy Tube
ASTM D3308	(2012; R 2017) Standard Specification for PTFE Resin Skived Tape
ASTM E84	(2020) Standard Test Method for Surface Burning Characteristics of Building Materials

MANUFACTURERS STANDARDIZATION SOCIETY OF THE VALVE AND FITTINGS INDUSTRY (MSS)

MSS SP-58	(2018) Pipe Hangers and Supports - Materials, Design and Manufacture, Selection, Application, and Installation

U.S. DEPARTMENT OF DEFENSE (DOD)

UFC 3-301-01	(2019, with Change 1, 2022) Structural Engineering

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Refrigerant Piping System

SD-03 Product Data

Refrigerant Piping System

Spare Parts

Qualifications

Refrigerant Piping Tests

Verification of Dimensions

SD-06 Test Reports

Refrigerant Piping Tests

SD-07 Certificates

Service Organization

SD-10 Operation and Maintenance Data

Maintenance; G

1.3 QUALITY ASSURANCE

1.3.1 Qualifications

Submit 3 copies of qualified procedures, and list of names and identification symbols of qualified welders and welding operators, prior to non-factory welding operations.

1.3.2 Contract Drawings

Because of the small scale of the drawings, it is not possible to indicate all offsets, fittings, and accessories that may be required. Carefully investigate the plumbing, fire protection, electrical, structural and finish conditions that would affect the work to be performed and arrange such work accordingly, furnishing required offsets, fittings, and accessories to meet such conditions.

1.4 DELIVERY, STORAGE, AND HANDLING

Protect stored items from the weather, humidity and temperature variations, dirt and dust, or other contaminants. Proper protection and care of all material both before and during installation is the Contractor's responsibility. Replace any materials found to be damaged at the Contractor's expense. During installation, cap piping and similar openings to keep out dirt and other foreign matter.

1.5 MAINTENANCE

1.5.1 General

Submit Data Package 2 plus operation and maintenance data complying with the requirements of Section 01 78 23 OPERATION AND MAINTENANCE DATA and as specified herein.

1.5.2 Extra Materials

Submit spare parts data for each different item of equipment specified, after approval of detail drawings and not later than 2 months prior to the date of beneficial occupancy. Include a complete list of parts and supplies, with current unit prices and source of supply, a recommended spare parts list for 1 year of operation, and a list of the parts recommended by the manufacturer to be replaced on a routine basis in the data.

PART 2 PRODUCTS

2.1 STANDARD COMMERCIAL PRODUCTS

a. Provide materials and equipment which are standard products of a manufacturer regularly engaged in the manufacturing of such products, that are of a similar material, design and workmanship and that have been in satisfactory commercial or industrial use for 2 years prior to bid opening.

b. The 2 year use must include applications of equipment and materials under similar circumstances and of similar size. The 2 years' experience must be satisfactorily completed by a product which has been sold or is offered for sale on the commercial market through advertisements, manufacturer's catalogs, or brochures. Products having less than a 2-year field service record will be acceptable if a certified record of satisfactory field operation, for not less than 6000 hours exclusive of the manufacturer's factory tests, can be shown.

c. Products must be supported by a service organization. System components must be environmentally suitable for the indicated locations. Submit a certified list of qualified permanent service organizations for support of the equipment which includes their

addresses and qualifications. The service organizations must be reasonably convenient to the equipment installation and be able to render satisfactory service to the equipment on a regular and emergency basis during the warranty period of the contract.

d. Exposed equipment moving parts, parts that produce high operating temperature, parts which may be electrically energized, and parts that may be a hazard to operating personnel must be insulated, fully enclosed, guarded, or fitted with other types of safety devices. Install safety devices so that proper operation of equipment is not impaired. Welding and cutting safety requirements must be in accordance with AWS Z49.1.

e. Provide the manufacturer's standard catalog data, at least 5 weeks prior to the purchase or installation of a particular component. Highlight the data to show information such as, but not limited to, material, size, options, performance charts, and curves in adequate detail to demonstrate compliance with contract requirements. Include the manufacturer's recommended installation instructions and procedures in the data provided. Provide data for the following components as a minimum:

(1) Piping and Fittings
(2) Valves
(3) Piping Accessories
(4) Pipe Hangers, Inserts, and Supports

2.2 ELECTRICAL WORK

Electrical equipment and wiring must be in accordance with Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Field wiring must be in accordance with manufacturer's instructions.

2.3 REFRIGERANT PIPING SYSTEM

Provide refrigerant piping, valves, fittings, and accessories in accordance with ASHRAE 15 & 34 and ASME B31.5, except as specified herein. Refrigerant piping, valves, fittings, and accessories must be compatible with the fluids used and capable of withstanding the pressures and temperatures of the service. Refrigerant piping, valves, and accessories used for refrigerant service must be cleaned, dehydrated, and sealed (capped or plugged) prior to shipment from the manufacturer's plant. Submit drawings, at least 5 weeks prior to beginning construction, provided in adequate detail to demonstrate compliance with contract requirements. Drawings must consist of:

a. Piping layouts which identify all valves and fittings.

b. Plans and elevations which identify clearances required for maintenance and operation.

2.4 PIPE, FITTINGS AND END CONNECTIONS (JOINTS)

2.4.1 Copper Tubing

Provide copper tubing conforming to ASTM B280 annealed or hard drawn as required. Copper tubing must bear the product identification markings in accordance with ASTM B280, "ACR" must be present on copper tubing. Copper tubing must be soft annealed where bending is required and hard drawn

where no bending is required. Soft annealed copper tubing must not be used in sizes larger than 1-3/8 inches. Joints must be brazed except that joints on lines 7/8 inchand smaller may be flared. Cast copper alloy fittings for flared copper tube must conform to ASME B16.26 and ASTM B62. Wrought copper and bronze solder-joint pressure fittings must conform to ASME B16.22 and ASTM B75/B75M. Joints and fittings for brazed joint must be wrought-copper or forged-brass sweat fittings. Cast sweat-type joints and fittings are not allowed for brazed joints. Brass or bronze adapters for brazed tubing may be used for connecting tubing to flanges and to threaded ends of valves and equipment.

2.4.2 Solder

Solder must conform to ASTM B32, grade Sb5, tin-antimony alloy for service pressures up to 150 psig. Solder flux must be liquid or paste form, non-corrosive and conform to ASTM B813.

2.4.3 Brazing Filler Metal

Filler metal must conform to AWS A5.8/A5.8M, Type BAg-5 with AWS Type FB3-A or Type FB3-C flux, except Type BCuP-3, BCuP-4, or BCuP-5 may be used for brazing copper-to-copper joints. BAlSi-4 with AWS Type FB1-A flux may be used when joining copper piping to aluminum components.

2.4.4 Brazing Flux

Brazing flux must conform to AWS A5.31/A5.31M, Type FB3-A or Type FB3-C when using Type BAg-5 filler metal. Type FB1-A is to be used with Type BAlSi-4 filler metal.

2.4.5 Press Fittings

Press fittings are not acceptable for use in refrigerant piping systems.

2.5 VALVES

Valves must be designed, manufactured, and tested specifically for refrigerant service. The valve material and all internal components must be compatible with the specific refrigerant and lubricant used. Valve bodies must be of brass, bronze, steel, or ductile iron construction. Valves 1 inch and smaller must have brazed or socket welded connections. Valves larger than 1 inch must have butt welded end connections. Do not use threaded end connections, except in pilot pressure or gauge lines where maintenance disassembly is required and welded flanges cannot be used. Internal parts must be removable for inspection or replacement without applying heat or breaking pipe connections. Valve stems exposed to the atmosphere must be stainless steel or corrosion resistant metal plated carbon steel. Direction of flow must be legibly and permanently indicated on the valve body. Control valve inlets must be fitted with integral or adapted strainer or filter where recommended or required by the manufacturer. Purge, charge and receiver valves must be of manufacturer's standard configuration.

2.5.1 Refrigerant Stop Valves

Valve must be the globe or full-port ball type with a back-seating stem especially packed for refrigerant service. Valve packing must be replaceable under line pressure. Provide valve with a handwheel operator and a seal cap. Valve must be the straight or angle pattern design as

indicated.

2.5.2 Check Valves

Valve must be the swing or lift type as required to provide positive shutoff at the differential pressure indicated. Valve must be provided with resilient seat.

2.5.3 Liquid Solenoid Valves

Provide valves that comply with AHRI 760 I-P and are suitable for continuous duty with applied voltages 15 percent under and 5 percent over nominal rated voltage at maximum and minimum encountered pressure and temperature service conditions. Valves must be direct-acting or pilot-operating type, packless, except that packed stem, seal capped, manual lifting provisions must be furnished. Provide solenoid coils that are moisture-proof, UL approved, totally encapsulated or encapsulated and metal jacketed as required. Valves must have safe working pressure of 610 psi and a maximum operating pressure differential of at least 200 psi at 85 percent rated voltage. Valves must have an operating pressure differential suitable for the refrigerant used.

2.5.4 Expansion Valves

Provide valve conforming to AHRI 750 I-P and ASHRAE 17. Valve must be the diaphragm and spring-loaded type with internal or external equalizers, and bulb and capillary tubing. Provide valve with an external superheat adjustment along with a seal cap. Internal equalizers may be utilized where flowing refrigerant pressure drop between outlet of the valve and inlet to the evaporator coil is negligible and pressure drop across the evaporator is less than the pressure difference corresponding to 2 degrees F of saturated suction temperature at evaporator conditions. Bulb charge must be determined by the manufacturer for the application and such that liquid will remain in the bulb at all operating conditions. Do not use gas limited liquid charged valves and other valve devices for limiting evaporator pressure without a distributor or discharge tube or effective means to prevent loss of control when bulb becomes warmer than valve body. Pilot-operated valves must have a characterized plug to provide required modulating control. A de-energized solenoid valve may be used in the pilot line to close the main valve in lieu of a solenoid valve in the main liquid line. Provide an isolatable pressure gauge in the pilot line, at the main valve. Automatic pressure reducing or constant pressure regulating expansion valves may be used only where indicted or for constant evaporator loads.

2.5.5 Electronic Expansion Valves

Valve must conform to AHRI 1370 I-P and ASHRAE 17. The valve must prevent the return of liquid to the compressor in the event of power loss or low superheat.

2.5.6 Safety Relief Valves

Valve must be the two-way type, unless indicated otherwise. Valve must bear the ASME code symbol. Valve capacity must be certified by the National Board of Boiler and Pressure Vessel Inspectors. Valve must be of an automatically reseating design after activation.

2.5.7 Evaporator Pressure Regulators, Direct-Acting

Valve must include a diaphragm/spring assembly, external pressure adjustment with seal cap, and pressure gauge port. Valve must maintain a constant inlet pressure by balancing inlet pressure on diaphragm against an adjustable spring load. Pressure drop at system design load must not exceed the pressure difference corresponding to a 2 degrees F change in saturated refrigerant temperature at evaporator operating suction temperature. Spring must be selected for indicated maximum allowable suction pressure range.

2.5.8 Refrigerant Access Valves

Provide refrigerant access valves and hose connections in accordance with AHRI 720.

2.6 PIPING ACCESSORIES

2.6.1 Filter Driers

Driers must conform to AHRI 710 I-P. Sizes 5/8 inch and larger must be the full flow, replaceable core type. Sizes 1/2 inch and smaller must be the sealed type. Cores must be of suitable desiccant that will not plug, cake, dust, channel, or break down, and must remove water, acid, and foreign material from the refrigerant. Constructfilter driers so that none of the desiccant will pass into the refrigerant lines. Minimum bursting pressure must be 1,500 psi.

2.6.2 Sight Glass and Liquid Level Indicator

2.6.2.1 Assembly and Components

Assembly must be pressure- and temperature-rated and constructed of materials suitable for the service. Glass must be borosilicate type. Ferrous components subject to condensation must be electro-galvanized.

2.6.2.2 Gauge Glass

Gauge glass must include top and bottom isolation valves fitted with automatic checks, and packing followers; red-line or green-line gauge glass; elastomer or polymer packing to suit the service; and gauge glass guard.

2.6.2.3 Bull's-Eye and Inline Sight Glass Reflex Lens

Provide bull's-eye and inline sight glass reflex lens for dead-end liquid service. For pipe line mounting, provide two plain lenses in one body suitable for backlighted viewing.

2.6.2.4 Moisture Indicator

Indicator must be a self-reversible action, moisture reactive, color changing media. Indicator must be furnished with full-color-printing tag containing color, moisture, and temperature criteria. Unless otherwise indicated, the moisture indicator must be an integral part of each corresponding sight glass.

2.6.3 Vibration Dampeners

Dampeners must be of the all-metallic bellows and woven-wire type.

2.6.4 Flexible Pipe Connectors

Connector must be a composite of interior corrugated phosphor bronze or Type 300 Series stainless steel, as required for fluid service, with exterior reinforcement of bronze, stainless steel or monel wire braid. Assembly must be constructed with a safety factor of not less than 4 at300 degrees F. Unless otherwise indicated, the length of a flexible connector must be as recommended by the manufacturer for the service intended.

2.6.5 Strainers

Strainers used in refrigerant service must have brass or cast-iron body, Y-or angle-pattern, cleanable, not less than 60-mesh noncorroding screen of an area to provide net free area not less than ten times the pipe diameter with pressure rating compatible with the refrigerant service. Screens must be stainless steel or monel and reinforced spring-loaded where necessary for bypass-proof construction.

2.6.6 Pressure and Vacuum Gauges

Provide gauges conforming to ASME B40.100 with throttling type needle valve or a pulsation dampener and shut-off valve. Gauge must be a minimum of 3-1/2 inches in diameter with a range from 0 psig to approximately 1.5 times the maximum system working pressure. Select each gauge range so that at normal operating pressure, the needle is within the middle-third of the range.

2.6.7 Temperature Gauges

Provide industrial duty type temperature gauges for the required temperature range. Gauges must have Fahrenheit scale in 2 degrees graduations scale (black numbers) on a white face. The pointer must be adjustable. Provide rigid stem type temperature gauges in thermowells located within 5 feet of the finished floor. Provide universal adjustable angle type or remote element type temperature gauges in thermowells located 5 to 7 feet above the finished floor. Provide remote element type temperature gauges in thermowells located 7 feet above the finished floor.

2.6.7.1 Stem Cased-Glass

Provide stem cased-glass case composed of polished stainless steel or cast aluminum, 9 inches long, with clear acrylic lens, and non-mercury filled glass tube with indicating-fluid column.

2.6.7.2 Bimetallic Dial

Provide bimetallic dial type case that is greater than 3-1/2 inches, stainless steel, and hermetically sealed with clear acrylic lens. Bimetallic element must be silicone dampened and unit fitted with external calibrator adjustment. Accuracy must be one percent of dial range.

2.6.7.3 Liquid-, Solid-, and Vapor-Filled Dial

Provide liquid-, solid-, and vapor-filled dial type cases that are greater than 3-1/2 inches, stainless steel or cast aluminum with clear acrylic

lens. Fill must be nonmercury, suitable for encountered cross-ambients, and connecting capillary tubing must be double-braided bronze.

2.6.7.4 Thermowell

Thermowell must be identical size, 1/2 or 3/4 inch NPT connection, brass or stainless steel. Where test wells are indicated, provide captive plug-fitted type 1/2 inch NPT connection suitable for use with either engraved stem or standard separable socket thermometer or thermostat. Mercury must not be used in thermometers. Extended neck thermowells must be of sufficient length to clear insulation thickness by 1 inch.

2.6.8 Pipe Hangers, Inserts, and Supports

Provide pipe hangers, inserts, guides, and supports conforming to MSS SP-58.

2.6.9 Escutcheons

Escutcheons must be chromium-plated iron or chromium-plated brass, either one piece or split pattern, held in place by internal spring tension or set screws.

2.7 FABRICATION

2.7.1 Factory Applied Insulation

Factory installed insulation must be in accordance with ASHRAE 90.1 - IP. Factory insulated items installed outdoors are not required to be fire-rated. As a minimum, factory insulated items installed indoors must have a flame spread index no higher than 25 and a smoke developed index no higher than 50. Factory insulated items (no jacket) installed indoors and which are located in air plenums, in ceiling spaces, and in attic spaces must have a flame spread index no higher than 25 and a smoke developed index no higher than 50. Flame spread and smoke developed indexes must be determined by ASTM E84. Test insulation in the same density and installed thickness as the material to be used in the actual construction. Test material supplied by a manufacturer with a jacket as a composite material. Provide jackets, facings, and adhesives that have a flame spread index less than 25 and a smoke developed index less than 50 when tested in accordance with ASTM E84.

PART 3 EXECUTION

3.1 EXAMINATION

After becoming familiar with all details of the work, perform a verification of dimensions in the field. Submit a letter, at least 2 weeks prior to beginning construction, including the date the site was visited, conformation of existing conditions, and any discrepancies found before performing any work.

3.2 INSTALLATION

Pipe and fitting installation must conform to the requirements of ASME B31.1. Cut pipe accurately to measurements established at the jobsite, and work into place without springing or forcing, completely clearing all windows, doors, and other openings. Cutting or other weakening of the building structure to facilitate piping installation is not permitted without written approval. Cut pipe or tubing square, remove

by reaming, and permit free expansion and contraction without causing damage to the building structure, pipe, joints, or hangers.

3.2.1 Directional Changes

Make changes in direction with fittings, except that bending of pipe 4 inches and smaller is permitted, provided a pipe bender is used and wide weep bends are formed. Mitering or notching pipe or other similar construction to form elbows or tees is not permitted. The centerline radius of bends must not be less than 6 diameters of the pipe. Bent pipe showing kinks, wrinkles, flattening, or other malformations will not be accepted.

3.2.2 Functional Requirements

Install piping 1/2 inch/10 feet of pipe in the direction of flow to ensure adequate oil drainage. Properly cap or plug open ends of refrigerant lines or equipment during installation to keep moisture, dirt, or other foreign material out of the system. Piping must remain capped until installation. Equipment piping must be in accordance with the equipment manufacturer's recommendations and the contract drawings. Equipment and piping arrangements must fit into space allotted and allow adequate acceptable clearances for installation, replacement, entry, servicing, and maintenance.

3.2.3 Fittings and End Connections

3.2.3.1 Threaded Connections

Make threaded connections with tapered threads and make tight with PTFE tape complying with ASTM D3308 or equivalent thread-joint compound applied to the male threads only. Do not show more than three threads after the joint is made.

3.2.3.2 Brazed Connections

Perform brazing in accordance with AWS BRH, except as modified herein. During brazing, fill the pipe and fittings with a pressure regulated inert gas, such as nitrogen, to prevent the formation of scale. Before brazing copper joints, clean both the outside of the tube and the inside of the fitting with a wire fitting brush until the entire joint surface is bright and clean. Do not use brazing flux on copper-to-copper connections. Remove surplus brazing material at all joints. Make steel tubing joints in accordance with the manufacturer's recommendations. Paint joints in steel tubing with the same material as the baked-on coating within 8 hours after joints are made. Protect tubing against oxidation during brazing by continuous purging of the inside of the piping using nitrogen. Support piping prior to brazing and do not spring or force.

3.2.3.3 Welded Connections

Fusion-weld joints in steel refrigerant piping. Make branch connections with welding tees or forged welding branch outlets. Thoroughly clean pipe of all scale and foreign matter before the piping is assembled. During welding, fill the pipe and fittings with an inert gas, such as nitrogen, to prevent the formation of scale. Beveling, alignment, heat treatment, and inspection of weld must conform to ASME B31.1. Remove and reweld weld defects at no additional cost to the Government. Store and dry electrodes in accordance with AWS D1.1/D1.1M or as recommended by the manufacturer.

Do not use electrodes that have been wetted or that have lost any of their coating

3.2.3.4 Flared Connections

When flared connections are used, use a suitable lubricant between the back of the flare and the nut in order to avoid tearing the flare while tightening the nut.

3.2.3.5 Flanged Connections

When steel refrigerant piping is used, provide union or flange joints in each line immediately preceding the connection to each piece of equipment requiring maintenance, such as compressors, coils, chillers, control valves, and other similar items. Flanged joints must be assembled square end tight with matched flanges, gaskets, and bolts. Provide gaskets that are suitable for use with the refrigerants to be handled.

3.2.4 Valves

3.2.4.1 General

Install refrigerant stop valves on each side of each piece of equipment such as compressors condensers, evaporators, receivers, and other similar items in multiple-unit installation, to provide partial system isolation as required for maintenance or repair. Install stop valves with stems horizontal unless otherwise indicated. Install ball valves must be installed with stems positioned to facilitate operation and maintenance. Isolating valves for pressure gauges and switches must be external to thermal insulation. Safety switches must not be fitted with isolation valves. Filter dryers having access ports may be considered a point of isolation. Purge valves must be provided at all points of systems where accumulated non-condensable gases would prevent proper system operation. Valves must be furnished to match line size, unless otherwise indicated or approved.

3.2.4.2 Expansion Valves

Install expansion valves with the thermostatic expansion valve bulb located on top of the suction line when the suction line is less than 2-1/8 inches in diameter and at the 4 o'clock or 8 o'clock position on lines larger than 2-1/8 inches. Fasten the bulb securely with two clamps. Insulate ehe bulb . Install the bulb in a horizontal portion of the suction line, if possible, with the pigtail on the bottom. If the bulb must be installed in a vertical line, the bulb tubing must be facing up.

3.2.4.3 Valve Identification

Tag each system valve, including those which are part of a factory assembly. Tags must be in alphanumeric sequence, progressing in direction of fluid flow. Tags must be embossed, engraved, or stamped plastic or nonferrous metal of various shapes, sized approximately 1-3/8 inch diameter, or equivalent dimension, substantially attached to a component or immediately adjacent thereto. Attach tags with nonferrous, heavy duty, bead or link chain, 14 gauge annealed wire, nylon cable bands or as approved. Reference tag numbers in Operation and Maintenance Manuals and system diagrams.

3.2.5 Vibration Dampers

Provide vibration damper in the suction and discharge lines on spring mounted compressors. Install vibration dampers parallel with the shaft of the compressor and anchor firmly at the upstream end on the suction line and the downstream end in the discharge line.

3.2.6 Strainers

Provide strainers immediately ahead of solenoid valves and expansion devices. Strainers may be an integral part of an expansion valve.

3.2.7 Filter Dryer

Provide a liquid line filter dryer on each refrigerant circuit located such that all liquid refrigerant passes through a filter dryer. Size dryers in accordance with the manufacturer's recommendations for the system in which it is installed. Install dryers such that it can be isolated from the system, the isolated portion of the system evacuated, and the filter dryer replaced. Install dryers in the horizontal position except replaceable core filter dryers may be installed in the vertical position with the access flange on the bottom.

3.2.8 Sight Glass

Install a moisture indicating sight glass in all refrigerant circuits down stream of all filter dryers and where indicated. Provide full line size sight glasses.

3.2.9 Discharge Line Oil Separator

Provide discharge line oil separator in the discharge line from each compressor. Connect the oil return line to the compressor as recommended by the compressor manufacturer.

3.2.10 Accumulator

Provide accumulators in the suction line to each compressor.

3.2.11 Flexible Pipe Connectors

Install connectors perpendicular to line of motion being isolated. Fit piping for equipment with bidirectional motion with two flexible connectors, in perpendicular planes. Install reinforced elastomer flexible connectors in accordance with manufacturer's instructions. Provide piping guides and restraints related to flexible connectors as required.

3.2.12 Temperature Gauges

Locate temperature gauges specifically on, but not limited to the following: the sensing element of each automatic temperature control device where a thermometer is not an integral part thereof the liquid line leaving a receiver and the suction line at each evaporator or liquid cooler. Thermowells for insertion thermometers and thermostats must extend beyond thermal insulation surface not less than 1 inch.

3.2.13 Pipe Hangers, Inserts, and Supports

Pipe hangers, inserts, and supports must conform to MSS SP-58, except as modified herein. Do not use pipe hanger types 5, 12, and 26. Fabricate hangers used to support piping 2 inches and larger to permit adequate adjustment after erection while still supporting the load. Support piping subjected to vertical movement, when operating temperatures exceed ambient temperatures, by variable spring hangers and supports or by constant support hangers.

3.2.13.1 Hangers

Do not use Type 3 on insulated piping. Type 24 may be used only on trapeze hanger systems or on fabricated frames.

3.2.13.2 Inserts

Secure Type 18 inserts to concrete forms before concrete is placed. Continuous inserts which allow more adjustments may be used if they otherwise meet the requirements for Type 18 inserts.

3.2.13.3 C-Clamps

Torque Type 19 and 23 C-clamps in accordance with MSS SP-58 and have both locknuts and retaining devices, furnished by the manufacturer. Field-fabricated C-clamp bodies or retaining devices are not acceptable.

3.2.13.4 Angle Attachments

Furnish Type 20 attachments used on angles and channels with an added malleable-iron heel plate or adapter.

3.2.13.5 Saddles and Shields

Where Type 39 saddle or Type 40 shield are permitted for a particular pipe attachment application, the Type 39 saddle, connected to the pipe, must be used on all pipe 4 inches and larger when the temperature of the medium is 60 degrees F or higher. Use Type 40 shields on all piping less than 4 inches and all piping 4 inches and larger carrying medium less than 60 degrees F. Use a high-density insulation insert of cellular glass under the Type 40 shield for piping 2 inches and larger.

3.2.13.6 Horizontal Pipe Supports

Space horizontal pipe supports as specified in MSS SP-58 and install a support no more than 1 foot from the pipe fitting joint at each change in direction of the piping. Space pipe supports no more than 5 feet apart at valves. Pipe hanger loads suspended from steel joist with hanger loads between panel points in excess of 50 pounds must have the excess hanger loads suspended from panel points.

3.2.13.7 Vertical Pipe Supports

Support vertical pipe at each floor, except at slab-on-grade, and at intervals of not more than 15 feet not more than 8 feet from end of risers, and at vent terminations.

3.2.13.8 Pipe Guides

Provide Type 35 guides using, steel, reinforced polytetrafluoroethylene (PTFE) or graphite slides where required to allow longitudinal pipe movement. Provide lateral restraints as required. Provide slide materials that are suitable for the system operating temperatures, atmospheric conditions, and bearing loads encountered.

3.2.13.9 Steel Slides

Where steel slides do not require provisions for restraint of lateral movement, an alternate guide method may be used. On piping 4 inches and larger, usea Type 39 saddle. On piping under 4 inches, a Type 40 protection shield may be attached to the pipe or insulation and freely rest on a steel slide plate.

3.2.13.10 High Temperature Guides with Cradles

Where there are high system temperatures and welding to piping is not desirable, the Type 35 guide must include a pipe cradle, welded to the guide structure and strapped securely to the pipe. Separate the pipe from the slide material by at least 4 inches, or by an amount adequate for the insulation, whichever is greater.

3.2.13.11 Multiple Pipe Runs

In the support of multiple pipe runs on a common base member, use a clip or clamp where each pipe crosses the base support member. Spacing of the base support members must not exceed the hanger and support spacing required for an individual pipe in the multiple pipe run.

3.2.13.12 Seismic Requirements

Support and brace piping and attached valves to resist seismic loads as specified under UFC 3-301-01 and Section 23 05 48.19 BRACING FOR HVAC . Provide structural steel required for reinforcement to properly support piping, headers, and equipment but not shown under this section. Specify material used for support under Section 05 12 00 STRUCTURAL STEEL.

3.2.13.13 Structural Attachments

Attachment to building structure concrete and masonry must be by cast-in concrete inserts, built-in anchors, or masonry anchor devices. Inserts and anchors must be applied with a safety factor not less than 5. Do not attach supports to metal decking. Construct masonry anchors for overhead applications of ferrous materials only. Provide structural steel brackets required to support piping, headers, and equipment, but not shown, under this section. Specify material used for support under Section 05 12 00 STRUCTURAL STEEL.

3.2.14 Pipe Alignment Guides

Provide pipe alignment guides where indicated for expansion loops, offsets, and bends and as recommended by the manufacturer for expansion joints, not to exceed 5 feet on each side of each expansion joint, and in lines 4 inches or smaller not more than 2 feet on each side of the joint.

3.2.15 Pipe Anchors

Provide anchors wherever necessary or indicated to localize expansion or to prevent undue strain on piping. Provide anchors consisting of heavy steel collars with lugs and bolts for clamping and attaching anchor braces, unless otherwise indicated. Install anchor braces in the most effective manner to secure the desired results using turnbuckles where required. Do not attach supports, anchors, or stays where they will injure the structure or adjacent construction during installation or by the weight of expansion of the pipeline. Where pipe and conduit penetrations of vapor barrier sealed surfaces occur, immediately anchor these items adjacent to each penetrated surface, to provide essentially zero movement within penetration seal. Submit detailed drawings of pipe anchors for approval before installation.

3.2.16 Building Surface Penetrations

Do not install sleeves in structural members except where indicated or approved. Provide galvanized sheet metal sleeves in non-load bearing surfaces conforming to ASTM A653/A653M, Coating Class G-90, 20 gauge. Provide uncoated carbon steel pipe sleeves in load bearing surfaces conforming to ASTM A53/A53M, Standard weight. Apply sealants to moisture and oil-free surfaces and elastomers to not less than 1/2 inch depth. Do not install sleeves in structural members.

3.2.16.1 Refrigerated Space

Fit refrigerated space building surface penetrations with sleeves fabricated from hand-lay-up or helically wound, fibrous glass reinforced polyester or epoxy resin with a minimum thickness equal to equivalent size Schedule 40 steel pipe. Construct sleeves with integral collar or fit cold side with a bonded slip-on flange or extended collar. In the case of masonry penetrations where sleeve is not cast-in, fill voids with latex mixed mortar cast to shape of sleeve and assemble flange/external collar type sleeve with butyl elastomer vapor barrier sealant through penetration to cold side surface vapor barrier overlap and fastened to surface with masonry anchors. Flash integral cast-in collar type sleeve as indicated. Normally seal noninsulated penetrating round surfaces to sleeve bore with mechanically expandable seals in vapor tight manner and insulate remaining warm and cold side sleeve depth with not less than 4 inches of foamed-in-place rigid polyurethane or foamed-in-place silicone elastomer. Apply vapor barrier sealant to finish warm side insulation surface. Insulate warm side of penetrating surface beyond vapor barrier sealed sleeve insulation for a distance which prevents condensation. Seal wires in refrigerated space surface penetrating conduit with vapor barrier plugs or compound to prevent moisture migration through conduit and condensation therein.

3.2.16.2 General Service Areas

Extend each sleeve through its respective wall, floor, or roof, and cut flush with each surface. Provide pipes passing through concrete or masonry wall or concrete floors or roofs with pipe sleeves fitted into place at the time of construction. Provide sleeves that allow a minimum of 1/4 inch all-around clearance between bare pipe and sleeves or between jacketed-insulation and sleeves. Except in pipe chases or interior walls, seal the annular space between pipe and sleeve or between jacket over-insulation and sleeve in accordance with Section 07 92 00 JOINT SEALANTS.

3.2.16.3 Waterproof Penetrations

Install pipes passing through roof or floor waterproofing membrane through a 17 ounce copper sleeve, or a 0.032 inch thick aluminum sleeve, each within an integral skirt or flange. Form flashing sleeve, and extend skirt or flange greater than 8 inches from the pipe and set over the roof or floor membrane in a troweled coating of bituminous cement. Extend the flashing sleeve up the pipe a minimum of 2 inches above the roof or floor penetration. Seal the annular space between the flashing sleeve and the bare pipe or between the flashing sleeve and the metal-jacket-covered insulation as indicated. Seal penetrations by either one of the following methods.

3.2.16.3.1 Waterproofing Clamping Flange

Pipes up to and including 10 inches in diameter passing through roof or floor waterproofing membrane may be installed through a cast iron sleeve with caulking recess, anchor lugs, flashing clamp device, and pressure ring with brass bolts. Clamp waterproofing membrane into place and place sealant in the caulking recess.

3.2.16.3.2 Modular Mechanical Type Sealing Assembly

In lieu of a waterproofing clamping flange and caulking and sealing of annular space between pipe and sleeve or conduit and sleeve, a modular mechanical type sealing assembly may be installed. Provide seals consisting of interlocking synthetic rubber links shaped to continuously fill the annular space between the pipe/conduit and sleeve with corrosion protected carbon steel bolts, nuts, and pressure plates. Loosely assemble links with bolts to form a continuous rubber belt around the pipe with a pressure plate under each bolt head and each nut. After the seal assembly is properly positioned in the sleeve, tighten the bolt to cause the rubber sealing elements to expand and provide a watertight seal between the pipe/conduit and the sleeve. Size each seal assembly as recommended by the manufacturer to fit the pipe/conduit and sleeve involved. The Contractor electing to use the modular mechanical type seals must provide sleeves of the proper diameters.

3.2.16.4 Fire-Rated Penetrations

Seal penetration of fire-rated walls, partitions, and floors as specified in Section 07 84 00 FIRESTOPPING.

3.2.16.5 Escutcheons

Provide escutcheons for finished surfaces where exposed piping, bare or insulated, pass through floors, walls, or ceilings, except in boiler, utility, or equipment rooms. Where sleeves project slightly from floors, use special deep-type escutcheons. Secure escutcheon to pipe or pipe covering.

3.2.17 Access Panels

Provide access panels for all concealed valves, vents, controls, and items requiring inspection or maintenance. Provide access panels of sufficient size and locate so that the concealed items may be serviced and maintained or completely removed and replaced. Provide access panels as specified in Section 08 31 00 ACCESS DOORS AND PANELS.

3.2.18 Field Applied Insulation

Field installed insulation is specified in Section 23 07 00 THERMAL INSULATION FOR MECHANICAL SYSTEMS, except as defined differently herein.

3.2.19 Field Painting

Painting required for surfaces not otherwise specified, and finish painting of items only primed at the factory are specified in Section 09 90 00 PAINTS AND COATINGS.

3.2.19.1 Color Coding

Color coding for piping identification is specified in Section 09 90 00 PAINTS AND COATINGS.

3.2.19.2 Color Coding Scheme

Provide a color coding scheme for locating hidden piping in accordance with Section 22 00 00 PLUMBING, GENERAL PURPOSE.

3.2.20 Identification Tags

Provide identification tags made of brass, engraved laminated plastic or engraved anodized aluminum indicating service and item number on all valves and dampers. Tags must be 1-3/8 inch minimum diameter and marking must be stamped or engraved. Indentations must be black for reading clarity. Attach tags to valves with No. 12 AWG copper wire, chrome-plated beaded chain or plastic straps designed for that purpose.

3.3 CLEANING AND ADJUSTING

Clean uncontaminated system(s) by evacuation and purging procedures currently recommended by refrigerant and refrigerant equipment manufacturers, and as specified herein, to remove small amounts of air and moisture. Systems containing moderate amounts of air, moisture, contaminated refrigerant, or any foreign matter are considered contaminated systems. Restore contaminated systems to clean condition including disassembly, component replacement, evacuation, flushing, purging, and re-charging, using currently approved refrigerant and refrigeration manufacturer's procedures. Restore contaminated systems at no additional cost to the Government as determined by the Contracting Officer. Do not use water in any procedure or test.

3.4 REFRIGERANT PIPING TESTS

After all components of the refrigerant system have been installed and connected, subject the entire refrigeration system to pneumatic, evacuation, and startup tests as described herein. Submit a schedule, at least 2 weeks prior to the start of related testing, for each test. Identify the proposed date, time, and location for each test. Conduct tests in the presence of the Contracting Officer. Water and electricity required for the tests will be furnished by the Government. Provide all material, equipment, instruments, and personnel required for the test. Provide the services of a qualified technician, as required, to perform all tests and procedures indicated herein. Coordinate field tests with Section 23 05 93 TESTING, ADJUSTING, AND BALANCING OF HVAC SYSTEMS. Submit 6 copies of the tests report in bound 8 1/2 by 11 inch booklets

documenting all phases of the tests performed. Include initial test summaries, all repairs/adjustments made, and the final test results in the report.

3.4.1 Preliminary Procedures

Prior to pneumatic testing, isolate equipment which has been factory tested and refrigerant charged as well as equipment which could be damaged or cause personnel injury by imposed test pressure, positive or negative, from the test pressure, or remove from the system. Remove safety relief valves and rupture discs that are not part of factory sealed systems, and cap or plug openings.

3.4.2 Pneumatic Test

Provide pressure control and excess pressure protection at the source of test pressure. Valves must be wide open, except those leading to the atmosphere. Test gas must be dry nitrogen, with minus 70 degree F dewpoint and less than 5 ppm oil. Apply test pressure in two stages before any refrigerant pipe is insulated or covered. In accordance with ASME B31.5, a preliminary test not to exceed 25 psi must be applied as a means of locating major leaks. Every joint being tested must be coated with a thick soap or color indicating solution. The second stage test pressure must be at least 110 percent of the design pressure, but cannot exceed 130 percent of the design pressure of any component in the system. For large systems that are not completely visible, the pressure in the system must be gradually increased to one-half of the test pressure after which the pressure must be increased in steps of one-tenth of the test pressure, until the required test pressure has been reached. The test pressure must be continuously maintained for at leas 24 hours, after which it can be reduced to the leak test pressure. A correction factor of 0.3 psi will be allowed for each degree F change between test space initial and final ambient temperature, plus for increase and minus for a decrease. The leak test pressure must be the design pressure, or a pressure specified in the engineering design. To repair leaks, the joint must be taken apart, thoroughly cleaned, and reconstructed as a new joint. Joints repaired by caulking, re-melting, or back-welding/brazing are not acceptable. Following repair, the entire system must be retested using the pneumatic tests described above. Reassemble the entire system once the pneumatic tests are satisfactorily completed.

3.4.3 Evacuation Test

Following satisfactory completion of the pneumatic tests, relieve the pressure and evacuate the entire system to an absolute pressure of 300 micrometers. During evacuation of the system, the ambient temperature must be higher than 35 degrees F. Do not evacuate no more than one system at one time by one vacuum pump. Once the desired vacuum has been reached, close the vacuum line and allow the system to stand for 1 hour. If the pressure rises over 500 micrometers after the 1 hour period, evacuate the system again down to 300 micrometers and let set for another 1 hour period. Do not charge the system until a vacuum of at least 500 micrometers is maintained for a period of 1 hour without the assistance of a vacuum line. If during the testing the pressure rises above 500 micrometers, continue to repeat the evacuation procedures until all residual moisture has been removed. During evacuation, record pressures by a thermocouple-type, electronic-type, or a calibrated-micrometer type gauge.

3.4.4 System Charging and Startup Test

Following satisfactory completion of the evacuation tests, charge the system with the required amount of refrigerant by raising pressure to normal operating pressure and in accordance with manufacturer's procedures. Following charging, the system must operate with high-side and low-side pressures and corresponding refrigerant temperatures, at design or improved values. Test the entire system tested for leaks. Test fluorocarbon systems with halide torch or electronic leak detectors.

3.4.5 Refrigerant Leakage

If a refrigerant leak is discovered after the system has been charged, the leaking portion of the system must be immediatelyisolated from the remainder of the system and the refrigerant pumped into the system receiver or other suitable container. The refrigerant must not be discharged into the atmosphere.

3.4.6 Contractor's Responsibility

At all times during the installation and testing of the refrigeration system, take steps to prevent the release of refrigerants into the atmosphere. The steps must include, but not be limited to, procedures which will minimize the release of refrigerants to the atmosphere and the use of refrigerant recovery devices to remove refrigerant from the system and store the refrigerant for reuse or reclaim. At no time will the allowable leak rate exceed the leak rates allowed in Section 608 of the Clean Air Act: 30 percent of the full charge per year for industrial refrigeration, 20 percent of the full charge per year for commercial refrigeration, and 10 percent of the full charge per year for comfort cooling. Any system leaks within the first year must be repaired in accordance with the requirements herein at no cost to the Government including material, labor, and refrigerant if the leak is the result of defective equipment, material, or installation.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 31 13.00 40

METAL DUCTS

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 QUALITY CONTROL

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION
2.1.1 Design Requirements
2.2 COMPONENTS
2.2.1 Round Sheet Metal Duct Fittings
2.2.1.1 Fittings Construction
2.2.2 Reinforcement
2.2.3 Fittings
2.2.4 Turning Vanes
2.2.5 Dampers
2.2.6 Flexible Connectors for Sheet Metal
2.2.7 Duct Hangers
2.2.8 Manual Volume Dampers
2.2.8.1 Damper Construction
2.2.9 Gravity Backdraft and Relief Dampers
2.2.9.1 Blade Construction
2.2.10 Power-Operated Dampers
2.2.11 Fire Dampers and Wall Collars
2.3 MATERIALS
2.3.1 Galvanized Steel Ductwork Materials
2.3.2 Brazing Materials
2.3.3 Manufactured Round Ductwork (Positive Pressure)

PART 3 EXECUTION

3.1 PREPARATION
3.1.1 Construction Standards
3.2 INSTALLATION
3.2.1 Jointing
3.2.2 Ducts
3.2.2.1 Ductwork Cleaning Provisions
3.3 APPLICATION
3.3.1 Longitudinal Duct Seams
3.3.2 Low Pressure Sheet Metal Ducts
3.3.2.1 Joints and Gaskets
3.3.2.2 Flexible Duct Joints
3.3.2.3 Square Elbows
3.3.2.4 Radius Elbows
3.3.2.5 Outlets, Inlets, and Duct Branches

3.3.2.6 Duct Transitions
3.3.2.7 Branch Connections
3.3.2.8 Access Openings
3.3.2.9 Manual Volume Dampers
3.3.2.10 Flexible Connectors for Sheet Metal
3.3.3 Rectangular Sheet Metal Ducts
3.3.3.1 Medium-Pressure Gages, Joints, and Reinforcement
3.3.3.2 Medium- And High-Pressure Branches, Inlets, Outlets
3.3.3.3 Duct Branch Transition
3.3.3.4 High-Pressure Gages, Joints, and Reinforcement
3.3.4 Round Sheet Metal Ducts
3.3.4.1 Duct Gages and Reinforcement
3.3.4.2 Duct Joints
3.3.4.3 Duct Transitions
3.3.5 Round, High Pressure, Sheet Metal Duct Installation
3.3.5.1 Joints
3.3.5.2 Insulation Ends
3.3.6 Transverse Reinforcement Joints
3.3.7 Joint Gaskets
3.3.8 Radius Elbows
3.3.9 Plenum Connections
3.3.10 Access Openings
3.3.11 Duct Supports
3.3.11.1 Hangers
3.3.11.2 Installation
3.3.11.3 Strap-type Hanger
3.3.11.4 Trapeze Hanger
3.3.11.5 Purlins
3.3.11.6 Vibration Isolation
3.3.12 Flexible Connectors for Steel Metal
3.3.13 Insulation Protection Angles
3.3.14 Duct Probe Access
3.3.15 Openings In Roofs and Walls
3.4 FIELD QUALITY CONTROL
3.4.1 Fire Damper Tests
3.4.2 Ductwork Leakage Tests
3.4.3 Inspection
3.5 CLOSEOUT ACTIVITIES
3.5.1 Operation and Maintenance
3.5.2 Record Drawings

-- End of Section Table of Contents --

SECTION 23 31 13.00 40

METAL DUCTS

PART 1 GENERAL

Section 23 05 48.00 40 VIBRATION AND SEISMIC CONTROLS FOR HVAC PIPING AND EQUIPMENT applies to work in this section.

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN INSTITUTE OF STEEL CONSTRUCTION (AISC)

AISC 325	(2017) Steel Construction Manual
AISC 360	(2016) Specification for Structural Steel Buildings

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS (ASHRAE)

ASHRAE EQUIP IP HDBK	(2012) Handbook, HVAC Systems and Equipment (IP Edition)
ASHRAE FUN IP	(2021) Fundamentals Handbook, I-P Edition

AMERICAN WELDING SOCIETY (AWS)

AWS A5.8/A5.8M	(2019) Specification for Filler Metals for Brazing and Braze Welding

ASTM INTERNATIONAL (ASTM)

ASTM A653/A653M	(2020) Standard Specification for Steel Sheet, Zinc-Coated (Galvanized) or Zinc-Iron Alloy-Coated (Galvannealed) by the Hot-Dip Process
ASTM A924/A924M	(2022) Standard Specification for General Requirements for Steel Sheet, Metallic-Coated by the Hot-Dip Process

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 90A	(2021) Standard for the Installation of Air Conditioning and Ventilating Systems

SHEET METAL AND AIR CONDITIONING CONTRACTORS' NATIONAL ASSOCIATION (SMACNA)

SMACNA 1966	(2020) HVAC Duct Construction Standards Metal and Flexible, 4th Edition

SMACNA 1987 (2006) HVAC Duct Systems Inspection Guide, 3rd Edition

SOCIETY OF AUTOMOTIVE ENGINEERS INTERNATIONAL (SAE)

SAE AMS 2480 (2009; Rev H) Phosphate Treatment, Paint, Base

UNDERWRITERS LABORATORIES (UL)

UL 555 (2006; Reprint Aug 2016) UL Standard for Safety Fire Dampers

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Material, Equipment, and Fixture Lists

SD-02 Shop Drawings

Connection Diagrams

Offset Fitting Configurations

SD-03 Product Data

Equipment and Performance Data

Galvanized Steel Ductwork Materials

Brazing Materials

Round Sheet Metal Duct Fittings

Turning Vanes

Flexible Connectors

Power-Operated Dampers

Fire Dampers and Wall Collars

Gravity Backdraft and Relief Dampers

Manual Volume Dampers

SD-05 Design Data

Design Analysis and Calculations

SD-06 Test Reports

Ductwork Leakage Tests

Operational Tests

SD-07 Certificates

Listing of Product Installations

Galvanized Steel Ductwork Materials

Brazing Materials

Round Sheet Metal Duct Fittings

Turning Vanes

Dampers

Flexible Connectors

SD-10 Operation and Maintenance Data

Operation and Maintenance Manuals

Power Operated Dampers

Fire Dampers and Wall Collars

SD-11 Closeout Submittals

Record Drawings

1.3 QUALITY CONTROL

When furnishing the listing of product installations for medium and high pressure ductwork systems include identification of at least 5 units, similar to those proposed for use, that have been in successful service for a minimum period of 5 years. Include purchaser, address of installation, service organization, and date of installation.

PART 2 PRODUCTS

Include the manufacturer's style or catalog numbers, specification and drawing reference numbers, warranty information, and fabrication site information within material, equipment, and fixture lists.

2.1 SYSTEM DESCRIPTION

Provide low-pressure systems ductwork and plenums where maximum air velocity is 2,000-feet per minute(fpm) and maximum static pressure is 2-inches water gage (wg), positive or negative.

Submit connection diagrams for low pressure ductwork systems indicating the relation and connection of devices and apparatus by showing the general physical layout of all controls, the interconnection of one system (or portion of system) with another, and internal tubing, wiring, and other devices.

High velocity systems ductwork encompass systems where:

a. Minimum air velocity exceeds 2,000-feet per minute (fpm) or static pressure exceeds 2-inches water gage (wg).

b. Medium static pressure ranges from over 2-inches wg through 3-inches wg, positive or negative, or over 3-inches wg through 6-inches wg positive.

d. Do not use rigid fibrous-glass ductwork.

2.1.1 Design Requirements

Submit equipment and performance data for medium and high pressure ductwork systems consisting of use life, system functional flows, safety features, and mechanical automated details. Submit test response and performance characteristics curves for certified equipment.

Submit design analysis and calculations for ductwork systems indicating the manufacturer's recommended air velocities, maximum static pressure, and temperature calculations.

2.2 COMPONENTS

2.2.1 Round Sheet Metal Duct Fittings

Submit offset fitting configurations for approval. Shop fabricate fittings.

2.2.1.1 Fittings Construction

Manufacture as separate fittings, not as tap collars welded or brazed into duct sections.

Provide two-piece type miter elbows for angles less than 31 degrees, three-piece type for angles 31 through 60 degrees, and five-piece type for angles 61 through 90 degrees. Ensure centerline radius of elbows is 1-1/2 times fitting cross section diameter.

Provide conical type crosses, increasers, reducers, reducing tees, and 90-degree tees.

Ensure cutouts in fitting body are equal to branch tap dimension or, where smaller, excess material is flared and rolled into smooth radius nozzle configuration.

2.2.2 Reinforcement

Support inner liners of both duct and fittings by metal spacers welded in position to maintain spacing and concentricity.

2.2.3 Fittings

Make divided flow fittings as separate fittings, not tap collars into duct sections, with the following construction requirements:

a. Sound, airtight, continuous welds at intersection of fitting body and tap

b. Tap liner securely welded to inner liner, with weld spacing not to exceed 3-inches.

c. Pack insulation around the branch tap area for complete cavity filling.

d. Carefully fit branch connection to cutout openings in inner liner without spaces for air erosion of insulation and without sharp projections that cause noise and airflow disturbance.

Continuously braze seams in the pressure shell of fittings. Protect galvanized areas that have been damaged by welding with manufacturer's standard corrosion-resistant coating.

Construct two-piece type elbows for angles through 35 degrees, three-piece type for angles 36 through 71 degrees, and five-piece type for angles 72 through 90 degrees.

2.2.4 Turning Vanes

Provide double-wall type turning vanes, commercially manufactured for high-velocity system service.

2.2.5 Dampers

Construct low pressure drop, high-velocity manual volume dampers, and high-velocity fire dampers in accordance with ASHRAE EQUIP IP HDBK, Chapter 16, ASHRAE FUN IP, Chapter 32 and SMACNA 1966.

2.2.6 Flexible Connectors for Sheet Metal

Use UL listed connectors, 30-ounce per square yard, waterproof, fire-retardant, airtight, woven fibrous-glass cloth, double coated with neoprene. Clear width, not including clamping section, is 6 to 8-inches.

2.2.7 Duct Hangers

For duct hangers in contact with galvanized duct surfaces, provide galvanized steel painted with inorganic zinc.

2.2.8 Manual Volume Dampers

Conform to SMACNA 1966 for volume damper construction.

Equip dampers with an indicating quadrant regulator with a locking feature externally located and easily accessible for adjustment and standoff brackets to allow mounting outside external insulation. Where damper rod lengths exceed 30-inches, provide a regulator at each end of damper shaft.

2.2.8.1 Damper Construction

Provide all damper shafts with two-end bearings.

Provide a full length damper shaft and extend it beyond the damper blade. use a 3/8 -inch square shaft for damper lengths up to 20 -inches and a 1/2 -inch square shaft for damper lengths 20 -inches and larger. Where necessary to prevent damper vibration or slippage, provide adjustable support rods with locking provisions external to duct at damper blade end.

Provide dampers in ducts having a width perpendicular to the axis of the

damper that is greater than 12 -inches of multiblade type having a substantial frame with blades fabricated of 16 -gage metal. Provide blades not exceeding 10 -inches in width and 48 -inches in length, welded to 1/2 -inch diameter shafts. Ensure dampers greater than 48 -inches in width are made in two or more sections with intermediate mullions, each section being mechanically interlocked with the adjoining section or sections. Provide blades with graphite-impregnated nylon bearings and connect so that adjoining blades rotate in opposite directions.

2.2.9 Gravity Backdraft and Relief Dampers

Construct frames of not less than 1-1/2- by 4-inch reinforced 16-gage galvanized carbon steel. Solidly secure frames and mullions in place and seal with elastomer caulking against air bypass.

Provide shaft bearings with graphite-impregnated nylon .

Equip counterbalanced dampers with fixed or adjustable counterbalancing weights.

Gravity backdraft dampers may be equipment manufacturer's standard construction in sizes18 by 18-inch or smaller, when furnished integral with air moving equipment.

2.2.9.1 Blade Construction

Maximum blade width is 9 inches, and maximum blade length is 36 -inches. Blade material is 14-gage 6063 alloy aluminum. Provide blades with mechanically retained seals and 90-degree limit stops.

Blades linked together for relief service dampers are to open not less than 30 degrees on 0.05-inch wg differential pressure.

2.2.10 Power-Operated Dampers

Ensure dampers conform to applicable requirements specified under Section 23 09 13 INSTRUMENTATION AND CONTROL DEVICES FOR HVAC.

2.2.11 Fire Dampers and Wall Collars

Ensure fire damper locations are in accordance with NFPA 90A.

Provide fire dampers in ductwork at firewall barriers.

Construct and label fire dampers in accordance with UL 555 to provide damper and mounting fire-resistance that equals or exceeds fire-resistance of the construction in which installed. For link loads in excess of 20 pounds, provide UL-approved quartzoid links.

Construct wall collars in accordance with UL 555.

2.3 MATERIALS

2.3.1 Galvanized Steel Ductwork Materials

Provide hot-dip galvanized carbon steel ductwork sheet metal of lock-forming quality, with regular spangle-type zinc coating, conforming to ASTM A924/A924M and ASTM A653/A653M, Designation G90. Treat duct surfaces to be painted by annealing.

Conform to ASHRAE EQUIP IP HDBK, Chapter 16, ASHRAE FUN IP, Chapter 32 and SMACNA 1966 for sheet metal gages and reinforcement thickness.

Construct in accord with SMACNA HVAC Duct Construction Standard as follows:
1. Low pressure rectangular duct: Table 2-3, positive or negative.
2. Medium pressure rectangular duct: Table 2-5, positive or negative.
3. Round duct: 10 in wg static pressure Table 3-5, positive or Table 3-13 negative.
4. Round ducts shall be spiral seam.

2.3.2 Brazing Materials

Provide silicon bronze brazing materials conforming to AWS A5.8/A5.8M.

2.3.3 Manufactured Round Ductwork (Positive Pressure)

Duct and fittings suitable to positive 10 inches WG. Ducts shall be machine formed round and/or flat oval as shown on drawings, constructed of G90 galvanized steel. Use spiral lockseam construction. Longitudinal seam construction may be used for ductwork over 80 inches diameter with minimum 16 ga. Use fittings as indicated on drawings, as specified, and as required in accordance with manufacturer's published data.

Unless otherwise indicated, connection shall be slip type with minimum 2 inches insertion length or flanged joint in accordance with manufacturer's recommendations. When flange joints are required, use Van Stone angle rings welded to duct. Internal bracing is not allowed.

PART 3 EXECUTION

3.1 PREPARATION

For sheet metal surfaces to be painted, and surfaces to which adhesives are to be applied, clean surface of oil, grease, and deleterious substances.

Ensure strength is adequate to prevent failure under service pressure or vacuum created by fast closure of duct devices. Provide leaktight, automatic relief devices.

3.1.1 Construction Standards

Provide sheet metal construction in accordance with the recommendations for best practices in ASHRAE EQUIP IP HDBK, Chapter 16, ASHRAE FUN IP, Chapter 32, SMACNA 1966, and NFPA 90A.

Design and fabricate supplementary steel in accordance with AISC 360 and AISC 325.

Where construction methods for certain items are not described in the referenced standards or herein, perform the work in accordance with recommendations for best practice defined in ASHRAE EQUIP IP HDBK.

3.2 INSTALLATION

Fabricate an airtight system. Include reinforcements, bracing, supports, framing, gasketing, sealing, and fastening to provide rigid construction and freedom from vibration, airflow-induced motion and noise, and

excessive deflection at specified maximum system air pressure and velocity.

Provide offsets and transformations as required to avoid interference with the building construction, piping, or equipment.

Make plenum anchorage provisions, sheet metal joints, and other areas airtight and watertight by caulking, mating galvanized steel and concrete surfaces with a two-component elastomer.

3.2.1 Jointing

Enclose dampers located behind architectural intake or exhaust louvers by a rigid sheet metal collar and sealed to building construction with elastomers for complete air tightness.

Provide outside air-intake ducts and plenums made from sheet metal with soldered watertight joints.

3.2.2 Ducts

Wherever ducts pass through firewalls or through walls or floors dividing conditioned spaces from unconditioned spaces, provide a flanged segment in that surface during surface construction.

Where interiors of ducting may be viewed through air diffusion devices, construct the viewed interior with sheet metal and paint flat black.

3.2.2.1 Ductwork Cleaning Provisions

Protect open ducting from construction dust and debris in a manner approved by the Contracting Officer. Clean dirty assembled ducting by subjecting all main and branch interior surfaces to airstreams moving at velocities two times specified working velocities, at static pressures within maximum ratings. This may be accomplished by: filter-equipped portable blowers which remain the Contractor's property; wheel-mounted, compressed-air operated perimeter lances which direct the compressed air and which are pulled in the direction of normal airflow; or other means approved by the Contracting Officer. Use water- and oil- free compressed air for cleaning ducting. After construction is complete, and prior to acceptance of the work, remove construction dust and debris from exterior surfaces. Clean in conformance with SMACNA 1987.

3.3 APPLICATION

3.3.1 Longitudinal Duct Seams

Provide Pittsburgh lock corner seams.

3.3.2 Low Pressure Sheet Metal Ducts

Weld angle iron frames at corners and ends, whenever possible. Rivet or weld angle iron reinforcements to ducts not more than 6-inches on center, with not less than two points of attachment. Spot welding, where used, is 3-inches on center.

Seal standard seam joints with an elastomer compound to comply with SMACNA 1966 Seal Class A, B or C as applicable.

Limit crossbreaking to 4-feet and provide on all ducts 8-inches wide and

wider. Provide bead reinforcement in lieu of crossbreaking where panel popping may occur. Where rigid insulation is applied, crossbreaking is not required.

3.3.2.1 Joints and Gaskets

Bolt companion angle flanges together with 1/4 -inch diameter bolts and nuts spaced 6 -inches on center. Gasket flanged joints with neoprene full-face gaskets 1/8 -inch thick, with Shore A 40 durometer hardness. Use one piece gaskets, vulcanized at joints.

3.3.2.2 Flexible Duct Joints

Between flexible duct without sheet metal collars and round metal ductwork connections make joints by trimming the ends, coating the inside of the flexible duct for a distance equal to depth of insertion with elastomer caulk, and by securing with sheet metal screws or binding with a strap clamp.

3.3.2.3 Square Elbows

Provide single-vane duct turns in accordance with SMACNA 1966.

3.3.2.4 Radius Elbows

Conform to SMACNA 1966 for radius elbows. Provide an inside radius equal to the width of the duct. Where installation conditions preclude use of standard elbows, the inside radius may be reduced to a minimum of 1 times duct width. Install turning vanes in accordance with the following schedule.

	RADIUS OF TURNING VANES IN PERCENT OF DUCT WIDTH		
WIDTH OF ELBOWS INCHES	VANE NO. 1	VANE NO. 2	VANE NO. 3
Up to 16	56	--	--
17 to 48	43	73	--
49 and over	37	55	83

Where two elbows are placed together in the same plane for ducts 30-inches wide and larger, continue the guide vanes through both elbows rather than spaced in accordance with above schedule.

3.3.2.5 Outlets, Inlets, and Duct Branches

Install branches, inlets, and outlets so that air turbulence is reduced to a minimum and air volume properly apportioned. Install adjustable splitter dampers at all supply junctions to permit adjustment of the amount of air entering the branch. Wherever an air-diffusion device is shown as being installed on the side, top, or bottom of a duct, and whenever a branch take-off is not of the splitter type; provide a commercially manufactured 45 degree side-take-off (STO) fitting with manual volume damper to allow adjustment of the air quantity and to provide an even flow of air across the device or duct it services.

3.3.2.6 Duct Transitions

Where the shape of a duct changes, ensure the angle of the side of the transition piece does not exceed 15 degrees from the straight run of duct connected thereto.

Where equipment is installed in ductwork, ensure the angle of the side of the transition piece from the straight run of duct connected thereto does not exceed 15 degrees on the upstream side of the equipment and 22-1/2 degrees on the downstream side of the equipment.

3.3.2.7 Branch Connections

Construct radius tap-ins in accordance with SMACNA 1966.

3.3.2.8 Access Openings

Construct access door in accordance with SMACNA 1966, except that sliding doors may be used only for special conditions upon prior approval. Provide double-panel type doors.

Install access doors and panels in ductwork upstream from coils upstream and downstream from coils adjacent to fire dampers at controls or at any item requiring periodic inspection, adjustment, maintenance, or cleaning , and every 20-feet for indoor air quality housekeeping purposes.

Minimum access opening size is 12 by 18 -inches, unless precluded by duct dimensions or otherwise indicated.

Make airtight access doors that leak by adding or replacing hinges and latches or by construction of new doors adequately reinforced, hinged, and latched.

3.3.2.9 Manual Volume Dampers

Provide balancing dampers of the splitter, butterfly, or multilouver type, to balance each respective main and branch duct.

For dampers regulated through ceilings provide a regulator concealed in a box mounted in the ceiling, with a cover finish aesthetically compatible with ceiling surface. Where ceiling is of removable construction, set regulators above the ceiling, and mark the location on ceiling in a manner acceptable to the Contracting Officer.

3.3.2.10 Flexible Connectors for Sheet Metal

Connect air handling equipment, ducts crossing building expansion joints, and fan inlets and outlets to upstream and downstream components by treated woven-cloth connectors.

Install connectors only after system fans are operative, and vibration isolation mountings have been adjusted. When system fans are operating, ensure connectors are free of wrinkles caused by misalignment or fan reaction. Width of surface is curvilinear.

3.3.3 Rectangular Sheet Metal Ducts

3.3.3.1 Medium-Pressure Gages, Joints, and Reinforcement

Ensure minimum sheet metal gages, joints, and reinforcements between joints are in accordance with ASHRAE EQUIP IP HDBK, Chapter 16, ASHRAE FUN IP, Chapter 32 and SMACNA 1966.

Ensure sheet metal minimum thickness, transverse reinforcement between joints, and joints of ducts are in accordance with the following:

LONGEST SIDE (INCHES)	SHEET METAL GAGE ALL SIDES	COMPANION ANGLE (INCHES)	REINFORCEMENT ANGLES 24 INCHES ON CENTER MAXIMUM (BACK TO BACK)
97 to 108	16	2 by 2 by 1/8, two tie rods along angle	Two 2 by 2 by 1/8, two tie rods along angle
109 to 132	16	2 by 2 by 3/16, two tie rods along angle	Two 2 by 2 by 3/16, two tie rods along angle
133 and longer	14	2 by 2 by 3/16, with tie rods every 48 inches	Two 2 by 2 by 3/16, with tie rods every 48 inches

3.3.3.2 Medium- And High-Pressure Branches, Inlets, Outlets

Install branches, inlets, and outlets to minimize air turbulence and to ensure proper airflow.

Install dampers so that the amount of air entering duct mains is adjustable.

Provide commercially manufactured air extractors to allow adjustment of the air quantity and to provide an even flow of air across the device or duct served.

3.3.3.3 Duct Branch Transition

Where a duct branch handles over 25 percent of the air transported by the duct main, use a complete 90-degree increasing elbow, with an inside radius of 0.75 times duct branch width. Ensure the size of the trailing end of the increasing elbow within the main duct has the same ratio to the main duct size as the ratio of the relative air quantities handled.

Where a duct branch is to handle 25 percent or less of the air handled by the duct main, provide a branch connection with an inside radius of 0.75 times branch duct width, a minimum arc length of 45 degrees, and an outside radius of 1.75 times duct branch width. Place arc tangent to duct main.

3.3.3.4 High-Pressure Gages, Joints, and Reinforcement

Ensure sheet metal minimum thickness, joints, and reinforcement between joints are in accordance with ASHRAE EQUIP IP HDBK, Chapter 16, ASHRAE FUN IP, Chapter 32 and SMACNA 1966.

Use the following types of ASHRAE EQUIP IP HDBK, Chapter 16, ASHRAE FUN IP, Chapter 32 and SMACNA 1966 joints and seams:

Transverse Joints:

a. Welded flange joint without angle

b. Companion angle flanged joint

Longitudinal Seams:

a. Approved lock seams, back brazed, or continuously brazed seams for ducts with largest dimension up to 72-inches

b. Continuously welded or brazed seams for ducts with largest dimension greater than 72-inches

Sheet metal minimum thickness, transverse reinforcement between joints, and companion angle joints of ducts with longest side greater than 96 inches are in accordance with the following:

LONGEST SIDE (inches)	SHEET METAL GAGE ALL SIDES	COMPANION ANGLE (inches)	REINFORCEMENT ANGLES 24 INCHES ON CENTER MAXIMUM (BACK TO BACK)
97 to 108	16	2 by 2 by 1/8, two tie rods along angle	*Two 2 by 2 by 1/8, two tie rods along angle
109 to 132	16	2 by 2 by 3/16, two tie rods along angle	*Two 2 by 2 by 3/16, two tie rods along angle
133 and longer	14	2-1/2 by 2-1/2 by 3/16, with tie rods every 24 inches	*Two 2-1/2 by 2-1/2 by 3/16, with tie rods every 24 inches

3.3.4 Round Sheet Metal Ducts

3.3.4.1 Duct Gages and Reinforcement

Sheet metal minimum thickness, joints, and reinforcement between joints shall be in accordance with ASHRAE EQUIP IP HDBK, Chapter 16, ASHRAE FUN IP, Chapter 32 and SMACNA 1966.

Provide ducts with supplemental girth angle supports, riveted with solid rivets 6 inches on center or tack welded to duct. Locate girth angles as follows:

DIAMETER, INCHES	REINFORCEMENT-MAXIMUM SPACING INCHES
25 to 36	1-1/4 by 1-1/4, 1/8 thick, 72 inches on center

DIAMETER, INCHES	REINFORCEMENT-MAXIMUM SPACING INCHES
37 to 50	1-1/4 by 1-1/4, 1/8 thick, 60 inches on center
51 to 60	1-1/2 by 1-1/2, 1/8 thick, 48 inches on center

Use hex-shaped bolt heads and nuts, 5/16-inch diameter for ducts up to 50-inch diameter, and 3/8-inch diameter for 51-inch diameter ducts and larger.

Continuously weld or braze flanges to duct on outside of duct and intermittently welded with 1-inch welds every 4-inches on inside joint face. Remove excess filler metal from inside face. Protect galvanized areas that have been damaged by welding with manufacturer's standard corrosion-resistant coating.

3.3.4.2 Duct Joints

Provide duct joints manufactured by machine, with spiral locksets up to and including 60-inch diameters, and to dimensional tolerances compatible with fittings provided. Draw-band girth joints are not acceptable.

Prepare slip joints by coating the male fitting with elastomer sealing materials, exercising care to prevent mastic from entering fitting bore. Leave only a thin annular mastic line exposed internally. Use sheet metal screws to make assembly rigid, not less than four screws per joint, maximum spacing 6-inches. Do not use pop rivets. Tape and heat seal all joints.

3.3.4.3 Duct Transitions

Where the shape of a duct changes, ensure the angle of the side of the transition piece does not exceed 15 degrees from the straight run of duct connected thereto.

Where equipment is installed in ductwork, ensure the angle of the side of the transition piece from the straight run of duct connected thereto does not exceed 15 degrees on the upstream side of the equipment and 22-1/2 degrees on the downstream side of the equipment.

3.3.5 Round, High Pressure, Sheet Metal Duct Installation

3.3.5.1 Joints

Provide an inner coupling to align the inner lining to maintain good airflow conditions equivalent to standard round high-pressure duct joints. Butt joints are not suitable for the inner liner. Accomplish this alignment by extending the liner of the fitting for slip joint into the pipe . For ducts over 34-inches inside diameter, provide a separate coupling for inner alignment, with the pressure shells joined by angle-ring flanged connections.

3.3.5.2 Insulation Ends

At the end of an uninsulated section or run where internally insulated

duct connects to uninsulated spiral duct, fitting, fire damper or flexible duct, install an insulated end-fitting to bring the outer pressure shell down to nominal size.

3.3.6 Transverse Reinforcement Joints

Provide transverse reinforcements that are riveted with solid rivets to duct sides 6 inches on center . Weld transverse reinforcement at all corners to form continuous frames.

3.3.7 Joint Gaskets

For flanged joints, use neoprene full-face gaskets 1/8-inch thick, with Shore A 40 durometer hardness. Use one-piece gaskets, vulcanized at joints.

3.3.8 Radius Elbows

Fabricate elbow proportions and radius elbows in accordance with ASHRAE EQUIP IP HDBK, Chapter 16, ASHRAE FUN IP, Chapter 32 and SMACNA 1966.

3.3.9 Plenum Connections

Ensure round duct connections are welded joint bellmouth type.

Ensure rectangular duct connections are bellmouth type, constructed in accordance with ASHRAE EQUIP IP HDBK, Chapter 16, ASHRAE FUN IP, Chapter 32 and SMACNA 1966.

3.3.10 Access Openings

Install access panels in ductwork adjacent to fire dampers.

Minimum size of access opening is 12 by 18 inches, unless precluded by duct dimension.

Frame access openings with welded and ground miter joints, 1/8-inch thick strap steel , with 1/4 -inch studs welded to frame. Ensure cover plates are not less than 16-gage, reinforced as necessary for larger sizes .

In lieu of access doors, use readily accessible flanged duct sections upon approval. Provide stable hanger supports for disconnected duct terminal.

3.3.11 Duct Supports

Install duct support in accordance with ASHRAE EQUIP IP HDBK, Chapter 16, ASHRAE FUN IP, Chapter 32 and SMACNA 1966. Meet the minimum size for duct hangers as specified in ASHRAE EQUIP IP HDBK, Chapter 16, ASHRAE FUN IP, Chapter 32 and SMACNA 1966. Provide two hangers where necessary to eliminate sway. Support attachment to duct surfaces by bolt 4-inches on center.

Take the following into account in selection of a hanging system:

a. Location and precedence of work under other sections

b. Interferences of various piping and electrical conduit

c. Equipment, and building configuration

d. Structural and safety factor requirements

e. Vibration, and imposed loads under normal and abnormal service conditions

Support sizes, configurations, and spacing are given to show the minimal type of supporting components required. If installed loads are excessive for the specified hanger spacing, hangers, and accessories reduce hanger spacing. After system startup, replace any duct support device which due to length, configuration, or size, vibrates or causes possible failure of a member. Do not use a ductwork support system that allows a cascade-type failure to occur.

Do not hang ductwork and equipment from roof deck, piping, or other ducts or equipment. Maximum span between any two points is 10-feet, with lesser spans as required by duct assemblies, interferences, and permitted loads imposed.

Where support from metal deck systems is involved, coordinate support requirements with installation of metal deck.

3.3.11.1 Hangers

Attach hanger rods, angles, and straps to beam clamps. Receive approval from the Contracting Officer for concrete inserts, masonry anchors, and fasteners for the application.

Hardened high-carbon spring-steel fasteners fitted onto beams and miscellaneous structural steel are acceptable upon prior approval of each proposed application and upon field demonstration of conformance to specification requirements. Make fasteners from steel conforming to AISI Type 1070, treated and finished in conformance with SAE AMS 2480, Type Z (zinc phosphate base), Class 2 (supplementary treatment). Verify a 72-hour load-carrying capacity by a certified independent laboratory.

Where ductwork system contains heavy equipment, excluding air-diffusion devices and single-leaf dampers, hang such equipment independently of the ductwork by means of rods or angles of sizes adequate to support the load.

Cross-brace hangers to preclude swaying both vertically and laterally.

3.3.11.2 Installation

Ensure hanger spacing gives a 20-to-1 safety factor for supported load.

Maximum load supported by any two fasteners is 100 pounds.

Install hangers on both sides of all duct turns, branch fittings, and transitions.

Friction rod assemblies are not acceptable.

3.3.11.3 Strap-type Hanger

Support rectangular ducts up to 36-inches by strap-type hangers attached at not less than three places to not less than two duct surfaces in different planes.

Perforated strap hangers are not acceptable.

3.3.11.4 Trapeze Hanger

Support rectangular ducting, 36-inches and larger, by trapeze hangers. Support ducts situated in unconditioned areas and required to have insulation with a vapor-sealed facing on trapeze hangers. Space hangers far enough out from the side of the duct to permit the duct insulation to be placed on the duct inside the trapeze. Do not penetrate the vapor-sealed facing with duct hangers.

Where trapeze hangers are used, support the bottom of the duct on angles sized as follows:

WIDTH OF DUCT, INCHES	MINIMUM BOTTOM ANGLE SIZE, INCHES
30 and smaller	1-1/4 by 1-1/4 by 1/8
31 to 48	1-1/2 by 1-1/2 by 1/8
49 to 72	1-1/2 by 1-1/2 by 3/16
73 to 96	2 by 2 by 1/4
97 and wider	3 by 3 by 1/4

3.3.11.5 Purlins

Do not support ducting from roof purlins at points greater than one-sixth of the purlin span from the roof truss. Do not exceed 400 pounds load per hanger.

If the hanger load must exceed the above limit, provide reinforcing of purlin(s) or additional support beam(s). When an additional beam is used, have the beam bear on the top chord of the roof trusses, and also bear over the gusset plates of top chord. Stabilize the beam by connection to roof purlin along bottom flange.

Purlins used for supporting fire-protection sprinkler mains, electrical lighting fixtures, electrical power ducts, or cable trays are considered fully loaded. Provide supplemental reinforcing or auxiliary support steel for these purlins when used to support ductwork.

3.3.11.6 Vibration Isolation

Isolate the structure from duct support vibration at points indicated. Refer to Section 23 05 48.00 40 VIBRATION AND SEISMIC CONTROLS FOR HVAC PIPING AND EQUIPMENT.

3.3.12 Flexible Connectors for Steel Metal

Connect air-handling equipment, ducts crossing building expansion joints, and fan inlets and outlets to upstream and downstream components with treated woven-cloth connectors.

Install connectors only after system fans are operative and all vibration isolation mountings have been adjusted. When system fans are operating, ensure connectors are free of wrinkles caused by misalignment or fan reaction. Width of surface is curvilinear.

3.3.13 Insulation Protection Angles

Provide galvanized 20-gage sheet, formed into an angle with a 2-inch exposed long leg with a 3/8-inch stiffening break at outer edge, and with a variable concealed leg, depending upon insulation thickness.

Install angles over all insulation edges terminating by butting against a wall, floor foundation, frame, and similar construction. Fasten angles in place with blind rivets through the protection angle, insulation, and sheet metal duct or plenum. Install angles after final insulation covering has been applied.

3.3.14 Duct Probe Access

Provide holes with neat patches, threaded plugs, or threaded or twist-on caps for air-balancing pitot tube access. Provide extended-neck fittings where probe access area is insulated.

3.3.15 Openings In Roofs and Walls

Existing building openings are fixed in size and cannot be resized without authorization. Provide equipment to suit existing opening size.

3.4 FIELD QUALITY CONTROL

3.4.1 Fire Damper Tests

Perform operational tests on each fire damper in the presence of the Contracting Officer by enervating a fusible link with localized heat. Provide and install new links after successful testing.

3.4.2 Ductwork Leakage Tests

Conduct complete leakage test of new ductwork in accordance with Section 23 05 93 TESTING, ADJUSTING, AND BALANCING FOR HVAC. Perform tests prior to installing ductwork insulation.

3.4.3 Inspection

Inspect ductwork in accordance with SMACNA 1987.

3.5 CLOSEOUT ACTIVITIES

3.5.1 Operation and Maintenance

Submit 6 copies of the operation and maintenance manuals 30 calendar days prior to testing the medium and high pressure ductwork systems. Update data and resubmit for final approval no later than 30 calendar days prior to contract completion.

Ensure operation and maintenance manuals are consistent with manufacturer's standard brochures, schematics, printed instructions, general operating procedures and safety precautions.

3.5.2 Record Drawings

Provide record drawings with current factual information. Include deviations from, and amendments to, the drawings. Include concealed or visible changes in the work. Label drawings "As-Built".

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 34 23.00 40

HVAC POWER VENTILATORS

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 QUALITY CONTROL

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION
2.1.1 Design Requirements
2.2 COMPONENTS
2.2.1 Housing Style
2.2.2 Fan Type
2.2.2.1 Type C-PRV Centrifugal, Direct Drive
2.2.3 Fan Motor
2.2.4 Back-Draft Dampers
2.3 MATERIALS
2.3.1 Aluminum Alloy

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Lubrication
3.2 FIELD QUALITY CONTROL
3.2.1 Tests
3.2.2 Final Test Reports
3.3 CLOSEOUT ACTIVITIES

-- End of Section Table of Contents --

SECTION 23 34 23.00 40

HVAC POWER VENTILATORS

PART 1 GENERAL

Provide a power roof ventilators complete with all components and accessory equipment as specified in this section.

Section 23 31 13.00 40 METAL DUCTS applies to work specified in this section.

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN SOCIETY OF CIVIL ENGINEERS (ASCE)

ASCE 7-16	(2017; Errata 2018; Supp 1 2018) Minimum Design Loads and Associated Criteria for Buildings and Other Structures

ASTM INTERNATIONAL (ASTM)

ASTM B37	(2018) Standard Specification for Aluminum for Use in Iron and Steel Manufacture
ASTM B209	(2014) Standard Specification for Aluminum and Aluminum-Alloy Sheet and Plate

UNDERWRITERS LABORATORIES (UL)

UL 705	(2017; Reprint Aug 2022) UL Standard for Safety Power Ventilators

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Shop Drawings

Installation Drawings

SD-03 Product Data

Housing

Fan

Motor

Dampers

SD-06 Test Reports

Final Test Reports

SD-11 Closeout Submittals

Record Drawings

1.3 QUALITY CONTROL

Rate and label ventilators in accordance with the applicable standards of the Air Movement Control Association (AMCA), and indicate if the license bears the AMCA seal for both air and sound.

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION

2.1.1 Design Requirements

Submit the manufacturer's catalog data, including equipment and performance data, for power roof ventilator(s). As a minimum, include the following data:

a. Fan Type

b. Fan Specifications, including:

(1) Number of rotating fan blades/vanes

(2) Number of stationary fan blades/vanes

(3) Rotating speed(s)

(4) Number of belts (if belt-driven)

(5) Belt lengths- measured at the pitch line (if belt-driven)

(6) Diameter of the drive sheave at the drive pitch line (if belt-driven)

(7) Diameter of the driven sheave at the drive pitch line (if belt-driven)

c. Location of Installation

d. Identification Number

e. Date of Installation (Required or Actual Acceptance Date)

f. Applicable reference drawing number(s)

Submit detailed shop drawings for power roof ventilator systems.

Provide roof ventilators that comply with UL 705 and are furnished complete with bases, curbs, flashing flanges, noise baffles, dampers, damper controls, louvers, and screens, as indicated.

Provide ventilators that are designed for windloads in accordance with ASCE 7-16 with the installed design not less than 130 miles per hour windload. Ensure that the structural bracing is properly spaced to accommodate this loading and meets the design requirements of the covering material. Ensure that ventilators are adequately reinforced and well-braced with the joints properly formed. Ensure that the edges are wired or beaded where necessary to ensure rigidity. Prevent galvanic action between different metals in direct contact by providing nonconductive separators. Make all soldering even and smooth.

Provide corrosion-resistant steel bolts, rivets, and other fastenings used in connection with protected metal.

2.2 COMPONENTS

2.2.1 Housing Style

Provide inline style power roof ventilator as indicated.

2.2.2 Fan Type

Provide fans of the following types:

2.2.2.1 Type C-PRV Centrifugal, Direct Drive

For Type C-PRV ventilators, provide a centrifugal inline exhaust fan with direct drive, nonoverloading, backward-inclined wheel. Provide a vibration-isolated drive with an elastomer. Provide drive components that are mounted in a compartment isolated from the airstream.

2.2.3 Fan Motor

Provide single-phase, 120 V, 60 Hz, split-phase, direct drive EC motor less than 1/2 horsepower.

Provide three-phase , 460 V, 60 Hz motors 1/2 horsepower and larger.

Provide motors with local disconnects to allow for fan and motor maintenance. Provide all motors with thermal-overload protection. For motors located in airstreams, use a totally enclosed type.

2.2.4 Back-Draft Dampers

Provide motorized damper at wall louvers.

Interlock damper-actuating motor with the fan motor.

2.3 MATERIALS

Provide manufacturers' standard materials.

2.3.1 Aluminum Alloy

Provide aluminum alloy in accordance with ASTM B209 and ASTM B37.

PART 3 EXECUTION

3.1 INSTALLATION

Submit installation drawings for power roof ventilators.

Install power roof ventilators in accordance with the manufacturer's installation instructions. Coordinate installation of ventilators with other work. Coordinate anchors, attachments, and other items to be built for installation as the work progresses. Rigidly install ventilators in a weathertight and watertight manner that is free from vibration. Refer to Section 23 05 48.00 40 VIBRATION AND SEISMIC CONTROLS FOR HVAC PIPING AND EQUIPMENT for vibration isolation considerations.

3.1.1 Lubrication

Ensure the movable parts of dampers and related operating hardware are lubricated in accordance with manufacturer's printed instructions and that they operate smoothly and quietly without binding.

3.2 FIELD QUALITY CONTROL

3.2.1 Tests

After installation, test each power roof ventilator to demonstrate proper operation at indicated and specified performance requirements, including the running, balance, noise, and proper direction of fan rotation.

3.2.2 Final Test Reports

Provide final test reports to the Contracting Officer. Provide reports with a cover letter/sheet clearly marked with the system name, date, and the words "Final Test Reports - Forward to the Systems Engineer/Condition Monitoring Office/Predictive Testing Group for inclusion in the Maintenance Database."

3.3 CLOSEOUT ACTIVITIES

Submit detailed record drawings upon completion of the installation.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 36 00.00 40

AIR TERMINAL UNITS

PART 1 GENERAL

1.1 REFERENCES
1.2 ADMINISTRATIVE REQUIREMENTS
1.2.1 Pre-Installation Meetings
1.3 SUBMITTALS
1.4 QUALITY CONTROL

PART 2 PRODUCTS

2.1 EQUIPMENT
2.1.1 Verification of Performance
2.1.2 Shutoff Single-Duct Air Terminal Units
2.1.2.1 Configuration
2.1.2.2 Casing
2.1.2.3 Volume Damper
2.1.2.4 Electric Heating Coil
2.1.2.5 DDC Controls
2.1.2.6 Control Sequence

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Identification
3.1.2 Connections
3.2 FIELD QUALITY CONTROL
3.2.1 Leak Test
3.2.2 Operational Test
3.3 SYSTEM STARTUP
3.4 CLOSEOUT ACTIVITIES
3.4.1 Operation and Maintenance
3.4.2 Demonstration

-- End of Section Table of Contents --

SECTION 23 36 00.00 40

AIR TERMINAL UNITS

PART 1 GENERAL

Section 23 31 13.00 40 METAL DUCTS applies to work specified in this section.

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AIR DUCT COUNCIL (ADC)

ADC Standards Manual	(2008; 5th Edition) Flexible Duct Performance Installation Standards

AIR-CONDITIONING, HEATING AND REFRIGERATION INSTITUTE (AHRI)

AHRI 880 I-P	(2011) Performance Rating of Air Terminals

ASTM INTERNATIONAL (ASTM)

ASTM E84	(2020) Standard Test Method for Surface Burning Characteristics of Building Materials

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National Electrical Code
NFPA 90A	(2021) Standard for the Installation of Air Conditioning and Ventilating Systems

UNDERWRITERS LABORATORIES (UL)

UL 181	(2013; Reprint Dec 2021) UL Standard for Safety Factory-Made Air Ducts and Air Connectors

1.2 ADMINISTRATIVE REQUIREMENTS

Coordinate layout and installation of air terminal units and suspension system with other construction that penetrates ceilings or is supported by them, including light fixtures, HVAC equipment, fire-suppression system, communication and security systems, and partition assemblies.

1.2.1 Pre-Installation Meetings

Submit itemized lists for all materials, equipment, and fixtures to be incorporated in the work 30 days prior to commencement of work. Ensure list includes manufacturer's style or catalog numbers, specification and

drawing reference numbers, warranty information, and fabrication site information. Submit product data for each type of air terminal unit indicated, including rated capacities, furnished specialties, sound-power ratings, and accessories:

a. Single-Duct Air Terminal Units Submit records of existing conditions consisting of the results of Contractor's survey of work area conditions and features of existing structures and facilities within and adjacent to the jobsite. Commencement of work constitutes acceptance of existing conditions.

Submit shop drawings which detail equipment assemblies and indicate dimensions, required clearances, method of field assembly, components, and location and size of each field connection. Include a schedule showing unique model designation, room location, model number, size, and accessories furnished. Include wiring diagrams to show power, signal, and control wiring.

Provide units with the configuration, capacity, and static-pressure characteristics indicated.

Ensure dimensional data stated constitutes nominal sizing, which has been adjusted by the manufacturer when necessary to accommodate acoustic material thickness.

Ensure units proposed are identical to units having at least 2 years of proven satisfactory field service.

Provide certification that units and the list of spare parts are ADC Standards Manual tested and rated.

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Records of Existing Conditions

SD-02 Shop Drawings

Shutoff Single-Duct Air Terminal Units

SD-03 Product Data

Shutoff Single-Duct Air Terminal Units

SD-06 Test Reports

Test Report

SD-07 Certificates

List of Spare Parts

SD-10 Operation and Maintenance Data

Operation and Maintenance Manuals

SD-11 Closeout Submittals

Record Drawings

1.4 QUALITY CONTROL

Indicate on drawings the size, profiles, and dimensional requirements of air terminal units that are based on the specific system indicated.

Conform to NFPA 70, Article 100 for electrical components, devices, and accessories. List and label items as defined in NFPA 70, Article 100, by a testing agency acceptable to authorities having jurisdiction, and marked for intended use.

Ensure Air Terminals are certified under the AHRI 880 I-P Certification Program and carry the ARI Seal.

When air terminal devices are furnished with reheat coils, either integrally or remotely mounted, control panels of terminal devices shall be mounted on the same side of air terminal device as reheat coil piping connection.

PART 2 PRODUCTS

2.1 EQUIPMENT

2.1.1 Verification of Performance

Rate air terminal units according to AHRI 880 I-P.

2.1.2 Shutoff Single-Duct Air Terminal Units

2.1.2.1 Configuration

Provide a volume-damper assembly inside unit casing with control components located inside a protective metal shroud.

2.1.2.2 Casing

Provide 0.032-inch galvanized steel casing. Ensure the casing includes an integral mixing baffle to efficiently mix the hot and cold airstream.

a. Casing Lining

Attach a 3/4-inch adhesive of polyurethane foam insulation complying with UL 181 erosion requirements, and having a maximum flame-spread index of 25, and a maximum smoke-developed index of 50, for both insulation and adhesive, when tested according to ASTM E84. Coat any cut edges of fiberglass exposed to the airstream with NFPA 90A approved seal.

For the air inlet provide round stub connection for duct attachment. For the air outlet provide s-slip and drive connections. Provide removable panels for access to diverter and other parts requiring service, adjustment, or maintenance; with airtight gasket.

2.1.2.3 Volume Damper

The damper assembly shall be heavy-gauge, galvanized steel with a solid shaft rotating in bearings. The damper shaft shall incorporate a visual position indicator etched into the end of the damper shaft to clearly indicate damper position over the full range of 90 degrees.

The damper assembly shall incorporate a peripheral gasket on the damper blades for tight airflow shutoff. Air leakage past the closed damper shall not exceed 2 percent of the unit maximum rated airflow at 3 inch water gauge inlet static pressure, tested in accordance with ASHRAE 130.

2.1.2.4 Electric Heating Coil

Provide a slip-in-type, open-coil design with integral control box factory wired and installed. The electric heating coil shall be ETL listed to UL 1995 and CSA 22.2, and provided by the terminal unit manufacture. Include the following features:

a. Primary and secondary over-temperature protection

b. Nickel chrome 80/20 heating elements

c. Airflow switch

d. Non-interlocking disconnect switch

e. Fuses (for coils more than 48 A)

f. Switches and relays

g. Magnetic contactor for each step of control (for three-phase coils)

h. SCR controller

i. The electric coil casing shall be constructed from a minimum 20 gauge, 0.038 inch galvanized steel.

j. NEMA 250, Type 1 enclosure with hinged access door for access to all controls and safety devices.

2.1.2.5 DDC Controls

Provide bidirectional damper operators and microprocessor-based controller. Provide with room sensor that is compatible with temperature controls specified. Provide factory mounted 50 VA control transformer.

a. Damper Actuators

Provide a 24 V, powered closed, powered open damper actuator.

b. Terminal Unit Controller

Provide a pressure independent, variable-air volume controller with electronic airflow transducers factory calibrated to minimum and maximum air volumes. Include the following features:

(1) Proportional, plus integral control of room temperature

(2) Time-proportional reheat-coil control

(3) Occupied and unoccupied operating mode

(4) Remote reset of airflow or temperature set points

(5) Adjusting and monitoring with portable terminal

(6) Room Sensor

Provide a wall mounting room sensor, with temperature set-point adjustment and access for connection of portable operator terminal.

2.1.2.6 Control Sequence

Make suitable for operation with duct pressures between 0.25 and 3.0-inch wg inlet static pressure. Provide a factory-mounted and -piped, 5-micron filter; velocity-resetting, adjustable, high-limit control, with amplifying relay. Provide a system-powered, wall-mounting thermostat.

PART 3 EXECUTION

3.1 INSTALLATION

Install air terminal units level and plumb, and in accordance with NFPA 90A. Maintain sufficient clearance for normal service and maintenance.

3.1.1 Identification

Label each air terminal unit with plan number, nominal airflow, maximum and minimum factory-set airflows, coil type, and ARI certification seal.

3.1.2 Connections

Coordinate piping installations and specialty arrangements with schematics on Drawings and with requirements specified in piping systems.

Install piping adjacent to air terminal units to allow service and maintenance.

3.2 FIELD QUALITY CONTROL

Perform the following field tests and inspections and prepare a test report.

After installing air terminal units and after electrical circuitry has been energized, test for compliance with requirements.

3.2.1 Leak Test

After installation, fill water coils and test for leaks. Repair leaks and retest until no leaks exist.

3.2.2 Operational Test

After electrical circuitry has been energized, start units to confirm proper motor rotation and unit operation.

Test and adjust controls and safeties. Replace damaged and malfunctioning

controls and equipment. Remove and replace malfunctioning units and retest.

3.3 SYSTEM STARTUP

Engage a factory-authorized service representative to perform startup service.

Complete installation and startup checks according to manufacturer's written instructions and do the following:

a. Verify that inlet duct connections are as recommended by air terminal unit manufacturer to achieve proper performance.

b. Verify that controls and control enclosure are accessible.

c. Verify that control connections are complete.

d. Verify that nameplate and identification tag are visible.

e. Verify that controls respond to inputs as specified.

3.4 CLOSEOUT ACTIVITIES

3.4.1 Operation and Maintenance

Submit 6 copies of the operation and maintenance manuals 30 calendar days prior to testing the following items. Update and re-submit data for final approval no later than 30 calendar days prior to contract completion. Concurrently, submit record drawings providing current factual information, including deviations and amendments to the drawings, and concealed and visible changes in the work.

3.4.2 Demonstration

Engage a factory-authorized service representative to train Owner's maintenance personnel to adjust, operate, and maintain air terminal units.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 37 13.00 40

DIFFUSERS, REGISTERS, AND GRILLES

PART 1 GENERAL

1.1 REFERENCES
1.2 ADMINISTRATIVE REQUIREMENTS
1.3 SUBMITTALS

PART 2 PRODUCTS

2.1 PERFORMANCE REQUIREMENTS
2.2 COMPONENTS
2.2.1 Air Diffusion Device Construction
2.2.2 Types of Air Diffusion Devices
2.2.2.1 Type DSA
2.2.2.2 Type GS
2.2.2.3 Type GSE
2.2.2.4 Type RS

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Operations and Maintenance Manuals

-- End of Section Table of Contents --

SECTION 23 37 13.00 40

DIFFUSERS, REGISTERS, AND GRILLES

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS (ASHRAE)

ASHRAE 113	(2013) Method of Testing for Room Air Diffusion
ASHRAE EQUIP IP HDBK	(2012) Handbook, HVAC Systems and Equipment (IP Edition)
ASHRAE FUN IP	(2021) Fundamentals Handbook, I-P Edition

1.2 ADMINISTRATIVE REQUIREMENTS

Section 23 31 13.00 40 METAL DUCTS applies to work specified in this section.

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Material, Equipment, and Fixture Lists

Records of Existing Conditions

SD-02 Shop Drawings

Fabrication Drawings

Installation Drawings

SD-03 Product Data

Equipment and Performance Data

PART 2 PRODUCTS

2.1 PERFORMANCE REQUIREMENTS

Certify air diffusion devices having been tested and rated in accordance with Chapter 19-ASHRAE EQUIP IP HDBK, Chapter 16-ASHRAE FUN IP, and ASHRAE 113, where such certification is required.

Submit equipment and performance data for air-diffusion devices consisting of sound data in terms of Noise Criteria (NC) index for the capacity range of the device.

2.2 COMPONENTS

2.2.1 Air Diffusion Device Construction

Preclude flutter, rattle, or vibration on air-diffusion device construction and mounting. Refer to Section 23 05 48.00 40 VIBRATION AND SEISMIC CONTROLS FOR HVAC PIPING AND EQUIPMENT for vibration isolation considerations. Modify devices and provide accessories necessary for mounting in indicated surface construction.

Provide color as indicated on drawings.

Provide supply diffusers with combination damper and equalizing grid. Ensure dampers are extracting-splitter type, except as otherwise indicated. Equalizing grids shall consist of individually adjustable vanes designed for equalizing airflow into diffuser neck and providing directional control of airflow.

Ensure air-diffusion device volume and pattern adjustments can be made from the face of the device. Make volume adjustments by tamper-deterring device.

Provide gaskets for supply-terminal air devices mounted in finished surfaces.

Include within the material, equipment, and fixture lists the manufacturer's style or catalog numbers, specification and drawing reference numbers, warranty information, and fabrication site information.

Submit records of existing conditions consisting of the results of Contractor's survey of work area conditions and features of existing structures and facilities within and adjacent to the jobsite. Commencement of work constitutes acceptance of existing conditions.

Submit fabrication drawings for air-diffusion devices consisting of fabrication and assembly details to be performed in the factory.

2.2.2 Types of Air Diffusion Devices

2.2.2.1 Type DSA

Provide type DSA supply diffuser, Diffusers shall be aluminum constuctions, and shall consist of a seamless, one-piece, precision formed backpan that incorporates a round inlet collar of sufficient length for connecting rigid or flexible duct. The inner plaque assembly shall be completely removable from the room side to allow for full access to any dampers or other ductwork components located near the diffuser neck.

Include pattern adjustments horizontal, vertical projection, and an intermediate position or range.

Provide a baked enamel finish.

Provide antismudge rings.

Provide integral extended surface to fit into module of lay-in ceiling.

Provide 1/2 inch fiberglass external insulation with foil vapor barrior.

2.2.2.2 Type GS

Provide type GS supply grilles double deflection type with adjustable face bars parallel to short dimension and adjustable rear bars parallel to long dimension.

Provide a baked enamel finish.

Provide aluminum construction.

Provide integral extended surface to fit into module of lay-in ceiling or walls.

2.2.2.3 Type GSE

Provide type GSE series return or general exhaust grille with a rectangular, eggcrate face with a1/2 by 1/2 by 1/2 inch aluminum core, white baked enamel exterior finish, black matte finish on exposed-to-view interior surface for lay-in mounting.

Provide aluminum border.

2.2.2.4 Type RS

Provide type RS supply register, double-deflection type, with adjustable face bars parallel to short dimension and adjustable rear bars parallel to long dimension with opposed-blade type dampers.

Provide a baked enamel finish.

Provide aluminum construction.

Provide integral extended surface to fit into module of lay-in ceiling.

PART 3 EXECUTION

3.1 INSTALLATION

Install equipment as indicated and specified and in accordance with manufacturer's recommendations.

Submit installation drawings for air-diffusion devices. Indicate on drawings overall physical features, dimensions, ratings, service requirements, and equipment weights.

Unless otherwise indicated, size ductwork drop to diffusers or grilles to match unit collar sizes.

Seal connections between ductwork drops to diffusers or grilles airtight.

Support independently diffusers and grilles for T-bar mounting that exceed weight limit of ceiling suspension system in which they are to be installed.

3.1.1 Operations and Maintenance Manuals

Provide operation and maintenance manuals consistent with manufacturer's standard brochures, schematics, printed instructions, general operating procedures and safety precautions.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 74 33.00 40

PACKAGED, OUTDOOR, HEATING AND COOLING MAKEUP AIR-CONDITIONERS

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 QUALITY CONTROL
1.4 WARRANTY

PART 2 PRODUCTS

2.1 EQUIPMENT
2.1.1 Packaged Rooftop Air-Conditioning Units
2.1.1.1 Condensing Section
2.1.1.2 Cooling Coil
2.1.1.3 Outdoor/Return Air Section
2.1.1.4 Electric Heating Section
2.1.1.5 Supply Fans
2.1.1.6 Exhaust Fan
2.1.1.7 Casing
2.1.1.8 Controls
2.1.1.9 Filters
2.1.1.10 Roof Curb

PART 3 EXECUTION

3.1 INSTALLATION
3.2 Examination
3.3 FIELD QUALITY CONTROL
3.3.1 Quality Control
3.4 Start-up Service
3.5 Demonstration and Training
3.6 CLOSEOUT ACTIVITIES

-- End of Section Table of Contents --

SECTION 23 74 33.00 40

PACKAGED, OUTDOOR, HEATING AND COOLING MAKEUP AIR-CONDITIONERS

PART 1 GENERAL

Section 23 31 13.00 40 METAL DUCTS applies to work specified in this section.

Section 23 05 48.00 40 VIBRATION AND SEISMIC CONTROLS FOR HVAC PIPING AND EQUIPMENT applies to work specified in this section.

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AIR-CONDITIONING, HEATING AND REFRIGERATION INSTITUTE (AHRI)

ANSI/AHRI 210/240	(2008; Add 1 2011; Add 2 2012) Performance Rating of Unitary Air-Conditioning & Air-Source Heat Pump Equipment

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Packaged Rooftop Air-Conditioning Units

Cooling Coil

Controls

Casing

Installation Drawings

SD-03 Product Data

Equipment and Performance Data

Air-Conditioning Systems

Cooling Coil

Controls

Casing

Filters

Condensing Section

Supply Fans

SD-07 Certificates

List of Product Installations

Unit Parts Only Warranty

Compressor Parts Only Warranty

SD-10 Operation and Maintenance Data

Operation and Maintenance Manuals

1.3 QUALITY CONTROL

Submit a list of product installations of packaged air-conditioning units showing a minimum of five installed units, similar to those proposed for use, that have been in successful service for a minimum period of 5 years. Provide a list that includes the purchaser, address of installation, service organization, and date of installation.

1.4 WARRANTY

The manufacturer shall provide 12-month unit parts only warranty, and 5-year compressor parts only warranty. Defective parts shall be repaired or replaced during the warranty period at no charge. The warranty period shall commence at startup or six months after shipment, whichever occurs first.

PART 2 PRODUCTS

Submit equipment and performance data for packaged air-conditioning units, consisting of use life, power ratings, capacity ranges, face area classifications, and rotational velocities.

2.1 EQUIPMENT

2.1.1 Packaged Rooftop Air-Conditioning Units

Provide an air-conditioner that consists of matched assemblies. Provide a packaged unit complete with a frame and enclosure, interconnecting piping and wiring, necessary controls and safety devices, and an operating charge of oil. Ensure that the unit is ready for full-capacity operation after removal of the shipping protection,c

2.1.1.1 Condensing Section

Outdoor coils shall be cast aluminum, micro-channel coils. Plate fins shall be protected and brazed between adjoining flat tubes such that they shall not extend outside the tubes. A sub-cooling coil shall be an integral part of the main outdoor air coil. Each outdoor air coil shall be factory leak tested with high-pressure air under water.

Outdoor air coils shall be protected from incidental contact to coil fins by a coil guard. Coil guard shall be constructed of cross wire welded steel with PVC coating.

Fan motors shall be an ECM type motor for proportional control. The unit controller shall proportionally control the speed of the condenser fan motors to maintain the head pressure of the refrigerant circuit from ambient condition of 0~120°F. Mechanical cooling shall be provided to 0° F. The motor shall include thermal overload protection and protect the motor in the case of excessive motor temperatures. The motor shall have phase failure protection and prevent the motor from operation in the event of a loss of phase.

The condenser fan shall be low noise blade design. Fan blade design shall be a dynamic profile for low tip speed. Fan blade shall be of a composite material.

The unit shall have scroll compressors. One of the compressors shall be an inverter compressor providing proportional control. The unit controller shall control the speed of the compressor to maintain the discharge air temperature. The inverter compressor shall have a separate oil pump and low oil safety protection.

Pressure transducers shall be provided for the suction pressure and head pressure. Temperature sensor shall be provided for the suction temperature and the refrigerant discharge temperature of the compressors. All of the above devices shall be an input to the unit controller and the values be displayed at the unit controller.

Each circuit shall be dehydrated and factory charged with R-410A Refrigerant and oil.

2.1.1.2 Cooling Coil

The indoor coil section shall be installed in a draw through configuration, upstream of the supply air fan. The coil section shall be complete with a factory piped cooling coil and an ASHRAE 62.1 compliant double sloped drain pan. The drain pan shall be stainless steel and positively sloped. The slope of the drain pan shall be in two directions and comply with ASHRAE Standard 62.1. The drain pan shall have a minimum slope of 1/8" per foot to provide positive draining. The drain pan shall extend beyond the leaving side of the coil. The drain pan shall have a threaded drain connection extending through the unit base.

The direct expansion (DX) cooling coils shall be fabricated of seamless high efficiency copper tubing that is mechanically expanded into high efficiency aluminum plate fins. Coils shall be a multi-row, staggered tube design with a minimum of 3 rows. All cooling coils shall have an interlaced coil circuiting that keeps the full coil face active at all load conditions. All coils shall be factory leak tested with high pressure air under water.

The cooling coil shall have an electronic controlled expansion valve. The unit controller shall control the expansion valve to maintain liquid subcooling and the superheat of the refrigerant system. The refrigerant suction lines shall be fully insulated from the expansion valve to the compressors.

2.1.1.3 Outdoor/Return Air Section

Unit shall be provided with an outdoor air economizer section. The economizer section shall include outdoor, return, and exhaust air dampers. The economizer operation shall be fully integral to the mechanical cooling and allow up to 100% of mechanical cooling if needed to maintain the cooling discharge air temperature. The outdoor air hood shall be factory installed and constructed from galvanized steel finished with the same durable paint finish as the main unit. The hood shall include moisture eliminator filters to drain water away from the entering air stream. The outside and return air dampers shall be sized to handle 100% of the supply air volume. The dampers shall be parallel blade design. Damper blades shall be gasketed with side seals to provide an air leakage rate of 1.5 cfm / square foot of damper area at 1" differential pressure in according with testing defined in AMCA 500. A barometric exhaust damper shall be provided to exhaust air out of the back of the unit. A bird screen shall be provided to prevent infiltration of rain and foreign materials. Exhaust damper blades shall be lined with vinyl gasketing on contact edges. Control of the dampers shall be by a factory installed direct coupled actuator. Damper actuator shall be of the modulating, spring return type. A comparative enthalpy control shall be provided to sense and compare enthalpy in both the outdoor and return air streams to determine if outdoor air is suitable for "free" cooling. If outdoor air is suitable for "free" cooling, the outdoor air dampers shall modulate in response to the unit's temperature control system.

Provide factory installed and tested, outdoor air monitor that controls outdoor air +/- 15% accuracy down to 40 cfm per ton.

Economizer assembly Fault Detection and Diagnostics (FDD) shall be 90.1, IECC, and California Title 24 compliant. MicroTech III controls shall display a warning, and write a warning to the BAS, if the economizer malfunctions in accordance with 90.1, IECC, and Title 24 specifications.

2.1.1.4 Electric Heating Section

The rooftop unit shall include an electrical resistance heating coil section. Staged electric heating coil modules shall be factory installed downstream of the supply air fan in the heating section of the rooftop unit. Heating coils shall be constructed of a low watt density, nickel - chromium alloy resistance wire with intermediate supports that include ceramic bushings. The electrical contactors shall be of the full line-breaking type with all the electrical power legs being disconnected when the contactors are not energized. All electrical circuit wiring shall be designed with copper conductors, aluminum wires are not acceptable. Heating element branch circuits shall be individually fused to a maximum of 48 Amps per NEC requirements. The power supply for the electric heater shall be factory wired into the units main power block or disconnect switch.

The heating modules shall have an automatic reset, high temperature limit safety protection. A secondary high limit protection shall also be provided that requires a manual reset. An airflow switch shall be provided with the heating module to prevent the electric heater from operating in the event of no airflow.

The electric heat elements shall be controlled by the factory installed DDC unit control system. The heater shall have proportional SCR control. The unit controller shall modulate the electric heater to maintain the

discharge air temperature setpoint.

Field installed heating modules shall require a field ETL certification. Duct heaters mounted within the rooftop unit in the field shall not be acceptable. The manufacturer's rooftop unit ETL certification shall cover the complete unit including the electric heating modules.

2.1.1.5 Supply Fans

Supply fan shall be a single width, single inlet (SWSI) airfoil centrifugal fan. The fan wheel shall be Class II construction with fan blades that are continuously welded to the hub plate and end rim. The supply fan shall be a direct drive fan mounted to the motor shaft. Belts and sheaves are not acceptable due to the additional maintenance.

All fan assemblies shall employ solid steel fan shafts. Heavy-duty pillow block type, self-aligning, grease lubricated ball bearings shall be used. Bearings shall be sized to provide a L-50 life at 250,000 hours. The entire fan assembly shall be isolated from the fan bulkhead with a flexible collar and mounted on 1" spring isolators.

All fan assemblies shall be statically and dynamically balanced at the factory, including a final trim balance, prior to shipment.

Supply fan and motor assembly combinations larger than 8 hp or 22" diameter shall be internally isolated on 1" deflection, spring isolators and include removable shipping tie downs.

The motor shall be T Frame and open drip proof. Overload protection and speed control is provided by the factory installed VFD and rooftop unit controller. The motor shall have phase failure protection and prevent the motor from operation in the event of a loss of phase. Motors shall be premium efficiency.

The supply fan shall be capable of airflow modulation from 30% to 100% of the scheduled designed airflow. The fan shall not operate in a state of surge at any point within the modulation range.

2.1.1.6 Exhaust Fan

Exhaust fan shall be a single width, single inlet (SWSI) airfoil centrifugal fan. The fan wheel shall be Class II construction with aluminum fan blades that are continuously welded to the hub plate and end rim. The exhaust fan shall be a direct drive fan mounted to the motor shaft. Belts and sheaves are not acceptable due to the additional maintenance.

The fan motor shall be a totally enclosed EC motor that is speed controlled by the rooftop unit controller. The motor shall include thermal overload protection and protect the motor in the case of excessive motor temperatures. The motor shall have phase failure protection and prevent the motor from operation in the event of a loss of phase. Motors shall be premium efficiency.

The unit DDC controller shall provide building static pressure control. The unit controller shall provide proportional control of the exhaust fans from 25% to 100% of the supply air fan designed airflow to maintain the adjustable building pressure setpoint. The field shall mount the required

sensing tubing from the building to the factory mounted building static pressure sensor.

2.1.1.7 Casing

Panel construction shall be double-wall construction for all panels. All floor panels shall have a solid galvanized steel inner liner on the air stream side of the unit to protect insulation during service and maintenance. Insulation shall be a minimum of 2" thick with an R-value of 13.0, and shall be 2 part injected foam. Panel design shall include no exposed insulation edges. Unit cabinet shall be designed to operate at total static pressures up to 5.0 inches w.g

Exterior surfaces shall be constructed of painted galvanized steel, for aesthetics and long-term durability. Paint finish will include a base primer with a high-quality polyester resin topcoat. Finished, unabraded panel surfaces shall be exposed to an ASTM B117 salt spray environment and exhibit no visible red rust at a minimum of 3,000 hours exposure. Finished, abraded surfaces shall be tested per ASTM D1654, having a mean scribe creepage not exceeding 1/16" at 1,000 hours minimum exposure to an ASTM B117 salt spray environment. Measurements of results shall be quantified using ASTM D1654 in conjunction with ASTM D610 and ASTM D714 to evaluate blister and rust ratings.

Service doors shall be provided on the fan section, filter section, control panel section, and heating vestibule in order to provide user access to unit components. All service access doors shall be mounted on multiple, stainless steel hinges and shall be secured by a latch system. Removable service panels secured by multiple mechanical fasteners are not acceptable.

The unit base shall overhang the roof curb for positive water runoff and shall seat on the roof curb gasket to provide a positive, weathertight seal. Lifting brackets shall be provided on the unit base to accept cable or chain hooks for rigging the equipment.

2.1.1.8 Controls

Provide a complete integrated microprocessor based Direct Digital Control (DDC) system to control all unit functions including temperature control, scheduling, monitoring, unit safety protection, including compressor minimum run and minimum off times, and diagnostics. This system shall consist of all required temperature sensors, pressure sensors, controller and keypad/display operator interface. All MCBs and sensors shall be factory mounted, wired and tested.

The stand-alone DDC controllers shall not be dependent on communications with any on-site or remote PC or master control panel for proper unit operation. The microprocessor shall maintain existing set points and operate stand alone if the unit loses either direct connect or network communications. The microprocessor memory shall be protected from voltage fluctuations as well as any extended power failures. All factory and user set schedules and control points shall be maintained in nonvolatile memory. No settings shall be lost, even during extended power shutdowns.

The DDC control system shall permit starting and stopping of the unit locally or remotely. The control system shall be capable of providing a remote alarm indication. The unit control system shall provide for outside air damper actuation, emergency shutdown, remote heat enable/disable,

remote cool enable/disable, heat indication, cool indication, and fan operation.

All digital inputs and outputs shall be protected against damage from transients or incorrect voltages. All field wiring shall be terminated at a separate, clearly marked terminal strip.

The DDC controller shall have a built-in time schedule. The schedule shall be programmable from the unit keypad interface. The schedule shall be maintained in nonvolatile memory to insure that it is not lost during a power failure. There shall be one start/stop per day and a separate holiday schedule. The controller shall accept up to sixteen holidays each with up to a 5-day duration. Each unit shall also have the ability to accept a time schedule via BAS network communications.

An electronic variable frequency drive shall be provided for the supply air fan. Each drive shall be factory installed out of the air stream in a conditioned cabinet. Drives shall meet UL Standard 95-5V. The completed unit assembly shall be listed by a recognized safety agency, such as ETL. Drives are to be accessible through a hinged door assembly. Mounting arrangements that expose drives to high temperature unfiltered ambient air are not acceptable.

The supply air fan drive output shall be controlled by the factory installed main unit control system and drive status and operating speed shall be monitored and displayed at the main unit control panel.

To increase the efficiency of the cooling system the DDC controller shall include a discharge air temperature reset program for part load operating conditions.

2.1.1.9 Filters

Unit shall be provided with a draw-through filter section. The filter rack shall be designed to accept a 2" prefilter and a 4" final filter. The unit design shall have a hinged access door for the filter section. The manufacturer shall ship the rooftop unit with 2" MERV 8 and 4" MERV 13 filters.

2.1.1.10 Roof Curb

A prefabricated heavy gauge galvanized steel, insulated plenum curb shall be provided for field assembly on the roof decking prior to unit shipment. The roof curb shall be a full perimeter type with complete perimeter support of the air handling section and condensing section. The curb shall be a minimum of 36" high and include a nominal 2" x 4" wood nailing strip. Gasket shall be provided for field mounting between the unit base and roof curb.

PART 3 EXECUTION

3.1 INSTALLATION

Install equipment in accordance with the manufacturer's recommendations.

Submit installation drawings for packaged air-conditioning units in accordance with referenced standards in this section.

3.2 Examination

Prior to start of installation, examine area and conditions to verify correct location for compliance with installation tolerances and other conditions affecting unit performance. See unit IOM.

Examine roughing-in of plumbing, electrical and HVAC services to verify actual location and compliance with unit requirements. See unit IOM.

Proceed with installation only after all unsatisfactory conditions have been corrected.

3.3 FIELD QUALITY CONTROL

3.3.1 Quality Control

Test and rate components of the air-conditioning systems as a system in accordance with ANSI/AHRI 210/240.

3.4 Start-up Service

Engage a factory authorized service representative to perform startup service. Clean entire unit, comb coil fins as necessary, install clean filters. Measure and record electrical values for voltage and amperage. Refer to Division 23 "Testing, Adjusting and Balancing" and comply with provisions therein.

3.5 Demonstration and Training

Engage a factory authorized service representative to train owner's maintenance personnel to adjust, operate and maintain the entire unit. Refer to Division 01 Section Closeout Procedures and Demonstration and Training.

3.6 CLOSEOUT ACTIVITIES

Submit 3 copies of the operation and maintenance manuals at least 30 calendar days before testing the packaged air-conditioning units. Update and resubmit data for final approval at least 30 calendar days before contract completion.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 81 29

DUCTLESS SPLIT AIR CONDITIONERS

PART 1 GENERAL

1.1 SUMMARY
1.2 REFERENCES
1.3 SUBMITTALS
1.4 QUALITY ASSURANCE
1.5 QUALITY CONTROL
1.5.1 Qualifications
1.5.1.1 Qualification Of Installer
1.5.2 Standard Products
1.5.3 Manufacturer's Engineering Data
1.5.4 Manufacturer's Instructions
1.6 PROJECT SEQUENCING
1.7 DELIVERY, STORAGE, AND HANDLING
1.8 WARRANTY

PART 2 PRODUCTS

2.1 MATERIALS
2.1.1 Safety Devices
2.2 CONTROLS
2.2.1 Zone Control
2.3 INDOOR FAN COIL UNITS
2.3.1 Wall Surface-Mounted Units
2.4 OUTDOOR COMPRESSOR UNIT
2.4.1 Casing
2.4.2 Compressor
2.5 COMPONENTS
2.5.1 Refrigerant Piping
2.5.2 Condensate Drain Piping
2.6 EQUIPMENT ACCESSORIES AND MISCELLANEOUS EQUIPMENT
2.6.1 Refrigerant Signs
2.6.1.1 Installation Identification

PART 3 EXECUTION

3.1 EXAMINATION
3.2 INSTALLATION
3.2.1 Equipment General
3.2.2 Safety Devices
3.2.3 Controls
3.2.4 Electrical Equipment / Motors
3.2.5 Condensate Removal
3.2.6 Access Panels
3.2.7 Air Filters
3.2.8 Flashing and Pitch Pockets

3.2.9 Identification Tags and Plates
3.2.10 Refrigerant Signs
3.2.11 Field Applied Insulation
3.2.12 Piping
3.2.12.1 Pipe Hangers and Supports
3.2.12.2 Refrigerant Piping
3.2.13 Auxiliary Drain Pans, Drain Connections, And Drain Lines
3.3 REFRIGERANT PIPING TESTS
3.4 REFRIGERANT CHARGING
3.5 CLEANING
3.6 CLOSEOUT ACTIVITIES
3.6.1 Extra Materials
3.6.2 Maintenance Service Providers
3.6.3 Warranty
3.6.4 Operation And Maintenance Manual
3.6.5 Posted Instructions

-- End of Section Table of Contents --

SECTION 23 81 29

DUCTLESS SPLIT AIR CONDITIONERS

PART 1 GENERAL

1.1 SUMMARY

Provide a complete Air Source, Heat Pump type Ductless Split consisting of one or more outdoor compressor units and multiple indoor fan coil units as specified in this Section and in accordance with the following:

a. Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC applies to the ductless split system, and all work under this Section must be in accordance with Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC including but not limited to the open system, protocol, installation, submittal, testing and training requirements of that Section. Unless the specific ductless split system being installed is specifically excepted from the open protocol requirements by Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC, the use of non-CEA-709.1-D Non-ASHRAE 135 networks are prohibited.

   The ductless split control system must be in accordance with Section 25 05 11.01 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS.

b. The complete system must be a tested combination in accordance with AHRI 1230.

c. Provide heating /cooling control for each zone.

1.2 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AIR-CONDITIONING, HEATING AND REFRIGERATION INSTITUTE (AHRI)

AHRI 1230	(2010; Addendum 1 2011; Addendum 2 2014) Performance Rating of Variable Refrigerant Flow (VRF) Multi-Split Air-Conditioning and Heat Pump Equipment
ANSI/AHRI 270	(2008) Sound Rating of Outdoor Unitary Equipment

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS (ASHRAE)

ANSI/ASHRAE 15 & 34	(2013) ANSI/ASHRAE Standard 15-Safety Standard for Refrigeration Systems and ANSI/ASHRAE Standard 34-Designation and Safety Classification of Refrigerants
ASHRAE 90.1 - IP	(2019) Energy Standard for Buildings Except Low-Rise Residential Buildings

ASHRAE 135	(2020; Interpretation 1-8 2021; Errata 1-2 2021; Addenda CD 2021; Addenda BV-CE 2022; Interpretation 9-12 2022; Interpretation 13-17 2023; Addenda BV-CF 2023; Errata 3 2023) BACnet—A Data Communication Protocol for Building Automation and Control Networks

AMERICAN SOCIETY OF MECHANICAL ENGINEERS (ASME)

ASME B31.5	(2022) Refrigeration Piping and Heat Transfer Components

AMERICAN WELDING SOCIETY (AWS)

AWS A5.8/A5.8M	(2019) Specification for Filler Metals for Brazing and Braze Welding
AWS Z49.1	(2021) Safety in Welding and Cutting and Allied Processes

CONSUMER ELECTRONICS ASSOCIATION (CEA)

CEA-709.1-D	(2014) Control Network Protocol Specification

MANUFACTURERS STANDARDIZATION SOCIETY OF THE VALVE AND FITTINGS INDUSTRY (MSS)

MSS SP-58	(2018) Pipe Hangers and Supports - Materials, Design and Manufacture, Selection, Application, and Installation

UNDERWRITERS LABORATORIES (UL)

UL 1995	(2015; Reprint Aug 2022) UL Standard for Safety Heating and Cooling Equipment

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Qualification Of Installer

Verification Of Existing Conditions

SD-03 Product Data

Spare Parts Data

Manufacturer's Standard Catalog Data

Sample Warranty

SD-05 Design Data

Manufacturer's Engineering Data

SD-07 Certificates

Service Organizations

Warranty

Electronic Refrigerant Leak Detector Calibration

SD-08 Manufacturer's Instructions

Manufacturer's Instructions

SD-09 Manufacturer's Field Reports

Refrigerant Charging

SD-11 Closeout Submittals

Posted Instructions

Inventory

1.4 QUALITY ASSURANCE

Complete VRF systems must be purchased from a single supplier. The VRF system supplier must be responsible for providing a fully functional VRF system.

1.5 QUALITY CONTROL

1.5.1 Qualifications

1.5.1.1 Qualification Of Installer

Submit 3 copies of qualifications prior to installation. The installers must be trained and qualified to install the same type of VRF system components to be installed under this contract by the same manufacturer. Include training certificates in submittal. The installer must have performed three complete installations of VRF systems of the same type and manufacturer that resulted in successful commissioning. Include project VRF installation and product information, location, customer contact information and VRF manufacturer representative contact information. The customer and VRF representative will be contacted to validate information given.

1.5.2 Standard Products

Provide materials and equipment that are standard products of a manufacturer regularly engaged in the manufacturing of such products, which are of a similar material, design and workmanship. The standard products must have been in satisfactory commercial or industrial use for 3 years immediately prior to the solicitation of this contract. The 3 year use includes applications of equipment and materials under similar circumstances and of similar size. The 3 years' experience must be

satisfactorily completed by a product which has been sold on the commercial market through advertisements, manufacturer's catalogs, or brochures. Products must be supported by a service organization. Ensure system components are environmentally suitable for the indicated geographic locations.

1.5.3 Manufacturer's Engineering Data

Submit VRF manufacturer's engineering data with the shop drawings under separate cover. Strike out irrelevant items and options not to be installed. Provide all input and output reports for all selection procedures required by the manufacturer and as required by this section. Engineering data must include:

a. Selection Procedures:
   (1) Indoor and Outdoor Units
   (2) Piping Material and Fittings
   (3) Refrigerant Mass for system
   (4) Refrigerant Classification

b. System Efficiency Curves/Data including:
   (1) Efficiency correlated with OAT
   (2) At least five (5) data points covering full range of operation
   (3) Minimum and maximum values over the operational range
   (4) Efficiency at Standard AHRI conditions.

1.5.4 Manufacturer's Instructions

Submit VRF manufacturer's instructions with the shop drawings under separate cover. Strike out irrelevant items and options not to be installed. Provide with the following:

a. Installation: Include mechanical, electrical, controls and piping complete installation requirements.

b. Operation: Include startup, normal operation and shutdown procedures.

c. Maintenance: Include preventative.

1.6 PROJECT SEQUENCING

Project sequencing must be in accordance with Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC.

1.7 DELIVERY, STORAGE, AND HANDLING

Protect stored items from the weather, humidity and temperature variations, dirt and dust, or other contaminants. Properly protect and care for all material both before and during installation. Submit an inventory of all the stored items. Replace any materials found to be damaged, at no additional cost to the Government. During installation, keep piping and similar openings capped to keep out dirt and other foreign matter.

1.8 WARRANTY

Provide VRF manufactured equipment with the 1 year unit parts warranty, and 10 year compressor parts warranty, in addition to the Warranty of Construction. Submit Sample Warranty prior to construction. Compare

warranty requirements with the requirements of this contract and identify discrepancies in the submittal that would prevent coverage of warranty by the manufacturer.

PART 2 PRODUCTS

All products used to meet this specification must meet the indicated requirements, but not all products specified here will be required by every project.

2.1 MATERIALS

Provide Manufacturer's standard catalog data, at least 5 weeks prior to the purchase or installation of a particular component, highlighted to show material, size, options, performance charts and curves, in adequate detail to demonstrate compliance with contract requirements. If field installed vibration isolation is specified for a unit, include vibration isolator literature containing catalog cuts and certification that the isolation characteristics of the isolators provided meet the manufacturer's recommendations. Submit data for each specified component. Minimum efficiency requirements must be in accordance with ASHRAE 90.1 - IP.

2.1.1 Safety Devices

Exposed moving parts, parts that produce high operating temperature, parts which may be electrically energized, and parts that may be a hazard to operating personnel must be insulated, fully enclosed, guarded, or fitted with other types of safety devices.

2.2 CONTROLS

The control system, components and network must be in accordance with Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC.

2.2.1 Zone Control

Provide a Space Sensor Module, in accordance with Section 23 09 13 INSTRUMENTATION AND CONTROL DEVICES FOR HVAC, for each fan coil unit unless otherwise indicated in contract drawings and with the following additional requirements:

a. Displays the current temperature, temperature setpoint, fans status, occupancy status and conditioning mode at the same time. If information is displayed electronically then it must be illuminated.

b. Temperature setpoint adjustment in one degree increments.

c. Fans speed control (At least: High-low-Auto).

2.3 INDOOR FAN COIL UNITS

Provide with the following:

a. Factory complete, tested and pre-wired with all necessary electronic and refrigerant controls.

b. Equipped with auto-restart function and test run capability either via a switch or controller.

c. Refrigerant: Refrigerant circuits factory-charged with dehydrated inert gas.

d. Coils: Direct expansion type constructed from copper, aluminum, or copper and aluminum.

e. Fans: Direct-drive, with statically and dynamically balanced impellers; variable speed or multi-speed supporting at least high and low speeds unless otherwise indicated; motor thermally protected.

f. Return Air Filter: Washable long-life net filter with mildew proof resin, or replaceable, unless otherwise indicated.

g. Condensate Drainage: Built-in condensate drain pan with drain connection.

h. Dedicated electronic modulating refrigerant expansion and flow control.

i. Unit must be in accordance with UL 1995 and AHRI 1230.

j. For units with Built-In Condensate Pumps, provide condensate safety shutoff and alarm. For units without Built-In Condensate Pump, provide built in or field supplied overflow protection.

2.3.1 Wall Surface-Mounted Units

Provide with the following:

a. Finished white casing, with removable front grille; sound insulation; wall mounting plate; condensate drain pan.

b. Airflow Control: Auto-swing louver that closes automatically when unit stops; adjustable discharge angle, set using remote controller; upon restart, discharge angle defaulting to same angle as previous operation.

c. Fan: Direct-drive cross-flow type.

d. Condensate Drain Connection: Side (end), not concealed in wall.

2.4 OUTDOOR COMPRESSOR UNIT

Provide with the following:

a. The outdoor unit must have one or more variable capacity compressors or alternative method resulting in three or more steps of capacity needed to load match the indoor unit fan coils at all times.

b. The unit must be factory complete, tested and pre-wired with all necessary electronic and refrigerant controls.

c. The sound pressure dB(A) at rated conditions must be a value of 58 decibels at 3 feet from the front of the unit when rated in accordance with ANSI/AHRI 270.

d. The unit must automatically restart normal operation after a power failure of any duration without reprogramming or manual assistance.

e. Oil recovery cycle must be automatic occurring a minimum of 2 hours after start of operation and then at least every 8 hours of operation.

f. Each outdoor unit must have it's own dedicated power feed, each with disconnect and main power circuit breaker.

h. The unit must be in compliance with ANSI/ASHRAE 15 & 34, factory tested, cleaned, dehydrated, charged, and sealed. Provide refrigerant charging valves. Filter-drier must be provided in liquid line.

i. The outdoor units capacity must meet or exceed the scheduled value in the contract drawings. The ratio of the outdoor unit capacity to the total connected indoor capacity must be in accordance with the manufacturer's recommendations for selecting the outdoor unit.

j. Unit must be in accordance with UL 1995 and AHRI 1230.

2.4.1 Casing

Construct the unit of zinc coated, heavy-gage (14-gage minimum) galvanized steel. Provide cabinet panels with lifting handles and water- and air-tight seal. Insulate all exposed vertical panels, top covers and base pan.

2.4.2 Compressor

Each compressor system must have the following:

a. High pressure safety switch, and internal thermal overload protection.

b. Factory installed vibration dampeners on all mounting points.

d. Factory installed crank case heater or other control logic to ensure reliable operation in freezing environments.

e. Oil separator with an oil balance circuit.

2.5 COMPONENTS

2.5.1 Refrigerant Piping

Provide refrigerant piping external to equipment in accordance with Section 23 23 00 REFRIGERANT PIPING.

2.5.2 Condensate Drain Piping

Provide condensate drain piping in accordance with manufacturer's recommendations and as shown in the drawings.

2.6 EQUIPMENT ACCESSORIES AND MISCELLANEOUS EQUIPMENT

2.6.1 Refrigerant Signs

Refrigerant signs must be a medium-weight aluminum type with a baked enamel finish. Signs must be suitable for indoor or outdoor service. Signs must have a white background with red letters not less than 0.5 inches in height.

2.6.1.1 Installation Identification

Provide each new refrigeration system with a refrigerant sign which indicates the following as a minimum:

a. Contractor's name.

b. Refrigerant number and amount of refrigerant.

c. The lubricant identity and amount.

d. Field test pressure applied.

PART 3 EXECUTION

3.1 EXAMINATION

After becoming familiar with all details of the work, submit verification of existing conditions at least 2 weeks prior to beginning construction, indicating the date the site was visited, confirming existing conditions, and noting any discrepancies found.

3.2 INSTALLATION

The VRF system must be installed by the contractor identified in Qualification Of Installer. The contractor must install the VRF system in accordance with the manufacturer's instructions and Shop Drawings.

3.2.1 Equipment General

Provide necessary supports for all equipment, appurtenances, and pipe as required. Isolate outdoor units from the building structure. If mechanical vibration isolators are not provided, provide vibration absorbing foundations. Each foundation must include isolation units consisting of machine and floor or foundation fastenings, together with intermediate isolation material. In lieu of concrete pad foundation, concrete pedestal block with isolators placed between the pedestal block and the floor may be provided. Concrete pedestal block must be of mass not less than three times the equipment weight. Concrete for foundations must be as specified in Section 03 30 00 CAST-IN-PLACE CONCRETE. Equipment must be properly leveled, aligned, and secured in place in accordance with manufacturer's instructions. Air-source outdoor units must be installed per manufacturer's recommendations and must not blow air in the direction of other outdoor unit intakes.

3.2.2 Safety Devices

Safety devices must be installed so that proper operation of equipment is not impaired. Welding and cutting safety requirements must be in accordance with AWS Z49.1.

3.2.3 Controls

Install Controls in accordance with Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC, as indicated by the Points Schedule and to provide the following functionality:

a. On/Off selection for each individual fan coil unit and group.

b. Temperature set point adjustment for each fan coil unit.

c. Fan speed adjustment for each fan coil.

d. Heat/cool/automatic changeover mode selection for indoor and outdoor units.

e. Priority settings for restriction of local access for start/stop, heat/cool mode and set point adjustment.

f. Temperature limitation in both heating and cooling mode.

g. Weekly occupancy schedule with start up and shut off times, temperature settings and operation modes. Yearly occupancy schedule for holidays and periods of non-use.

h. Reset for non-blocking malfunction codes and maintenance warnings.

Provide a Local Display panel as indicated on the points schedule and to provide access to the above specified functionality. The Local Display Panel must additionally indicate current date and time.

3.2.4 Electrical Equipment / Motors

Install electrical equipment, motors, motor efficiencies, and wiring in accordance with Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM.

3.2.5 Condensate Removal

Provide condensate removal through gravity flow where possible. Where gravity flow is not possible, provide a condensate pump sufficient ensure complete removal of condensate.

3.2.6 Access Panels

Provide access panels for all concealed equipment, valves, controls, dampers, refrigerant fittings, and other fittings for inspection, maintenance and removal. Size panel large enough as to be able to remove the part without modification or damage to the surroundings.

3.2.7 Air Filters

Allow access space for servicing filters. Install filters with suitable sealing to prevent bypassing of air. Perform and document that proper indoor air quality during construction procedures have been followed in accordance with Section 01 33 29 SUSTAINABILITY REQUIREMENTS AND REPORTING, paragraph Indoor Air Quality During Construction; this includes providing documentation showing that after construction ends, and prior to occupancy, new filters were provided and installed.

3.2.8 Flashing and Pitch Pockets

Provide flashing and pitch pockets for equipment supports and roof penetrations and flashing where piping or ductwork passes through exterior walls in accordance with Section 07 60 00 FLASHING AND SHEET METAL.

3.2.9 Identification Tags and Plates

Provide equipment, gages, thermometers, valves, and controllers with tags

numbers stamped or engraved into the material for their use. Provide plates and tags of brass or suitable nonferrous rigid material, securely mounted or attached. Provide minimum letter and numeral size of 1/8 inch high.

3.2.10 Refrigerant Signs

Locate refrigerant signs with in reading distance of outdoor unit.

3.2.11 Field Applied Insulation

Apply field applied insulation as specified in Section 23 07 00 THERMAL INSULATION FOR MECHANICAL SYSTEMS, except as defined differently herein.

3.2.12 Piping

3.2.12.1 Pipe Hangers and Supports

Design and fabrication of pipe hangers, supports, and welding attachments must conform to MSS SP-58. Installation of hanger types and supports for bare and covered pipes must conform to MSS SP-58 for the system temperature range. Unless otherwise indicated, horizontal and vertical piping attachments must conform to MSS SP-58.

3.2.12.2 Refrigerant Piping

Cut pipe to measurements established at the site and work into place without springing or forcing. Install piping with sufficient flexibility to provide for expansion and contraction due to temperature fluctuation and as indicated in shop drawings. Where pipe passes through building structure pipe joints must not be concealed, but must be located where they may be readily inspected. Install piping to be insulated with sufficient clearance to permit application of insulation. Install piping as indicated and detailed, to avoid interference with other piping, conduit, or equipment. Except where specifically indicated otherwise, run piping plumb and straight and parallel to walls and ceilings. Provide sleeves of suitable size for lines passing through building structure. Braze refrigerant piping with silver solder complying with AWS A5.8/A5.8M. Inside of tubing and fittings must be free of flux. Clean parts to be jointed with emery cloth and keep hot until solder has penetrated full depth of fitting and extra flux has been expelled. Cool joints in air and remove flame marks and traces of flux. During brazing operation, prevent oxide film from forming on inside of tubing by slowly flowing dry nitrogen through tubing to expel air. Make provisions to automatically return oil on halocarbon systems. Installation of piping must comply with ASME B31.5. All refrigerant lines external to units must have field applied insulation per Section 23 07 00 THERMAL INSULATION FOR MECHANICAL SYSTEMS unless otherwise indicated.

All refrigerant lines external to units must be isolated from system vibrations including those generated by compressors, fans, or pumps, to minimize the risk of refrigerant leaks.

3.2.13 Auxiliary Drain Pans, Drain Connections, And Drain Lines

Provide auxiliary drain pans under units located above finished ceilings or over mechanical or electrical equipment. Pan must extend beyond the limits of the units. Provide separate drain lines for the unit drain and auxiliary drain pans. Trap drain pans from the bottom to ensure complete

pan drainage. Provide drain lines full size of drain opening. Traps and piping to drainage disposal points must conform to Section 22 00 00 PLUMBING, GENERAL PURPOSE.

3.3 REFRIGERANT PIPING TESTS

Perform refrigerant piping tests as specified in Section 23 23 00 REFRIGERANT PIPING and per manufacturer's recommendations in the presence of the contracting officer. Use electronic type leak detector with a sensitivity of 0.1 ounces/year and a calibrated reference leak rated at 0.17 ounces/year. Submit current electronic refrigerant leak detector calibration certificate prior to testing. Before testing the refrigerant piping system, perform a test of the leak detector with the reference leak fitting in the presence of the Contracting Officer.

3.4 REFRIGERANT CHARGING

After refrigerant piping test and before system performance test, perform evacuation and dehydration procedures in accordance with manufacturers recommendations and requirements and Section 23 23 00 REFRIGERANT PIPING. Evacuate system to a minimum of 0.004 inches Hg for one hour or per manufacturers requirements. Use fresh oil in the vacuum pump. Connect electronic vacuum gauge to system piping for measurement. The refrigerant must be to the weight specified in the shop drawing calculations. The supplemental refrigerant must be weighed in with an electronic scale. Supplemental refrigerant must be introduced to the system in a liquid state for refrigerant blends. Conduct refrigerant charging in the presence of the Contracting Officer. Submit refrigerant charging report before system performance test. Outline refrigerant charging procedures in the report. Report must indicated who performed and witnessed the task. Provide signatures from all parties.

3.5 CLEANING

Equipment must be wiped clean, with all traces of oil, dust, dirt, or paint spots removed. Temporary filters must be provided for all fans that are operated during construction, and new filters must be installed after all construction dirt has been removed from the building. System must be maintained in this clean condition until final acceptance. Bearings must be properly lubricated with oil or grease as recommended by the manufacturer. Belts must be tightened to proper tension. Control valves and other miscellaneous equipment requiring adjustment must be adjusted to setting indicated or directed. Fans must be adjusted to the speed indicated by the manufacturer to meet specified conditions.

3.6 CLOSEOUT ACTIVITIES

Provide closeout activities in addition to and in accordance with Section 01 78 00 CLOSEOUT SUBMITTALS.

3.6.1 Extra Materials

Submit spare parts data for each different item of equipment specified, after approval of detail drawings and not later than 2 months prior to the date of beneficial occupancy. Include in the data a complete list of parts and supplies, with current unit prices and source of supply, a recommended spare parts list for 1 year of operation, and a list of the parts recommended by the manufacturer to be replaced on a routine basis.

3.6.2 Maintenance Service Providers

Submit a certified list of qualified permanent service organizations, which includes their addresses and qualifications, for support of the equipment. The service organizations must be reasonably convenient to the equipment installation and be able to render satisfactory service to the equipment on a regular and emergency basis during the warranty period of the contract.

3.6.3 Warranty

Submit warranty certificate to the Contracting Officer.

3.6.4 Operation And Maintenance Manual

Provide the following in addition to and accordance with Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC:

a. Condensed operating instructions listing step-by-step procedures required for system startup, operation, abnormal shutdown, emergency shutdown, and normal shutdown.

b. Manufacturer's Engineering Data.

c. Manufacturer's Instructions.

d. Shop Drawings on 11 by 17 inches sheets.

3.6.5 Posted Instructions

Submit the field posted instructions, at least 2 weeks prior to construction completion. Including equipment layout, wiring and control diagrams, piping, valves and control sequences, and typed condensed operation instructions on one sheet of paper. The condensed operation instructions must include preventative maintenance procedures, methods of checking the system for normal and safe operation, and procedures for safely starting and stopping the system. The posted instructions must cover all of the items contained in the approved operation and maintenance manuals as well as demonstrations of routine maintenance operations The posted instructions must be framed under glass or laminated plastic and be posted where indicated by the Contracting Officer.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

SECTION 23 83 00.00 20

ELECTRIC SPACE HEATING EQUIPMENT

PART 1 GENERAL

1.1 REFERENCES
1.2 GENERAL REQUIREMENTS
1.3 SUBMITTALS

PART 2 PRODUCTS

2.1 ELECTRIC UNIT AND CABINET HEATERS
2.1.1 Enclosure
2.1.2 Heating Element
2.1.3 Controls
2.1.4 Wiring
2.1.5 Thermostat
2.1.6 Disconnect Means
2.1.7 Motor
2.1.8 Finish
2.2 UNIT HEATERS
2.2.1 Heating Elements
2.2.2 Housing
2.2.3 Outlet Grille
2.2.4 Fan Motor
2.2.5 Built-in Controls
2.2.6 Disconnect Means

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Unit Heaters
3.1.2 Cabinet Heaters
3.2 FIELD QUALITY CONTROL
3.2.1 Field Inspection
3.2.2 Insulation Resistance Tests
3.2.3 Operational Tests

-- End of Section Table of Contents --

SECTION 23 83 00.00 20

ELECTRIC SPACE HEATING EQUIPMENT

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2023) National Electrical Code

UNDERWRITERS LABORATORIES (UL)

UL 1025	(1980; R 1990, Bul. 1991) Electric Air Heaters

1.2 GENERAL REQUIREMENTS

Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM, applies to this section, with the additions and modifications specified herein.

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Heater Installation Drawing

SD-03 Product Data

Electric Unit and Cabinet Heaters

Thermostat

SD-10 Operation and Maintenance Data

Electric Unit and Cabinet Heaters, Data Package 5

Submit in accordance with Section 01 78 23 OPERATION AND MAINTENANCE DATA.

PART 2 PRODUCTS

2.1 ELECTRIC UNIT AND CABINET HEATERS

UL 1025; wattage, voltage, phase, number of steps, Btu/hr and CFM as indicated. Provide control-circuit terminals and single source of power supply. Heaters 5 Kw and larger shall be 3-phase, with load balanced on each of the three phases. Limit leaving air temperature to 140 degrees F with entering air of 60 degrees F.

2.1.1 Enclosure

The back box shall be designed as a recessed rough in box in either masonry or frame installations. The back box shall be heavy gauge galvanized steel and shall contain knockouts through which power leads enter.

The louvered front cover shall be of heavy 20g steel with a powder paint finish. A plug button shall be provided to replace the thermostat knob and render the unit tamper-resistant.

2.1.2 Heating Element

Steel finned tubular elements or industrial grade, steel sheath with brazed copper plated steel fins and epoxy sealed ends.

2.1.3 Controls

Include limit controls for overheat protection of heaters. For remote thermostatic operation, provide contactor rated for 100,000 duty cycles. Provide a control transformer to supply 24-volt thermostat control circuit for each heater.

2.1.4 Wiring

Completely factory-prewired to terminal strips, ready to receive branch circuit and control connections for 140 degrees F copper wiring.

2.1.5 Thermostat

Provide tamper resistant integral thermostat, adjustable without requiring removal of heater components. Thermostat operating range shall be approximately 50 degrees F to a maximum of 75 degrees F with operating differential of 3 degrees F or less.

2.1.6 Disconnect Means

Provide factory-installed safety disconnect switch in the housing or in an auxiliary matching control section with "off" position marking on the face plate.

2.1.7 Motor

The fan motor shall be totally enclosed, impedance protected, and permanently lubricated. Fan control shall be of the bimetallic, snap-action type and shall activate fan after heating element reaches operating temperature, and continue to operate the fan after the thermostat is satisfied and until all heated air has been discharged.

2.1.8 Finish

All sheet metal parts, except the galvanized steel back box, shall be phosphatized, then completely painted by a powder paint process.

2.2 UNIT HEATERS

2.2.1 Heating Elements

Industrial grade, 0.475″ diameter steel sheath with brazed copper plated steel fins and epoxy sealed ends. Draw-thru airflow design pulls air across the heating elements to ensure cool element operation and even air distribution resulting in long element life.

2.2.2 Housing

Heating elements and motor are enclosed in a heavy gauge galvanized steel cabinet with a durable camel polyester powder coat finish.

2.2.3 Outlet Grille

Individually adjustable louvers are provided to direct airflow. A protective outlet fan guard is provided to prevent insertion of foreign objects.

2.2.4 Fan Motor

Permanently lubricated and thermally protected motor.

2.2.5 Built-in Controls

All units include an automatic reset thermal cutout that will de-energize the heater if anovertemperature condition occurs. A manual reset thermal cutout, in addition to an automatic reset thermal cutout, is standard on heaters 10 KW and above. A fan relay isprovided to allow the elements to heat up before fan startup and purges the heater of residual heat after shutdown. A 24-volt transformer and disconnecting contactor areprovided on most heaters. Single-phase heaters rated at 5 KW or less have line voltage controls; 24-volt control and contactor are available. Power fusing is standard on allheaters rated over 48 amps.

2.2.6 Disconnect Means

Provide factory-installed safety disconnect switch in the housing or in an auxiliary matching control section with "off" position marking on the face plate.

PART 3 EXECUTION

3.1 INSTALLATION

Install in conformance with the approved heater installation drawing, NFPA 70, UL listing, and manufacturer's instructions, with necessary clearances for air circulation, maintenance, inspection, service testing and repair. Connect to electrical supply in accordance with Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM.

3.1.1 Unit Heaters

Mount units plumb, square and level with ceiling and walls.

3.1.2 Cabinet Heaters

Where recessed mounting is indicated, seal entire recessed opening from exterior wall cavities, and provide a minimum 1/2-inch thick rigid fire resistant insulation on the wall behind the cabinet. Verify manufacturer's clearance requirements from electrical cords, drapes, and other furnishings.

3.2 FIELD QUALITY CONTROL

Provide necessary personnel, instruments, and equipment to perform tests. Notify the Contracting Officer 5 working days prior to scheduled testings and locations.

3.2.1 Field Inspection

Prior to initial operation, inspect installed equipment for conformance with drawings and specifications.

3.2.2 Insulation Resistance Tests

Test 600-volt wiring to verify that no short circuits or grounds exist. Tests shall be made using an instrument which applies a voltage of approximately 500 volts and provides a direct reading of resistance in ohms.

3.2.3 Operational Tests

Test equipment circuits and devices to demonstrate proper operation.Test each item of control equipment not less than 5 times.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 05 11.01

CYBERSECURITY FOR MECH-HVAC FACILITY-RELATED CONTROL SYSTEMS

PART 1 GENERAL

1.1 CONTROL SYSTEM APPLICABILITY
1.2 RELATED REQUIREMENTS
1.3 REFERENCES
1.4 DEFINITIONS
1.4.1 Administrator Account
1.4.2 Computer
1.4.3 Controller
1.4.4 Mission Space
1.4.5 Network
1.4.6 Network Connected
1.4.6.1 Wireless Network Connected
1.4.7 Network Media
1.4.8 User Account Support Levels
1.4.8.1 FULLY Supported
1.4.8.2 MINIMALLY Supported
1.4.8.3 NOT Supported
1.4.9 Manual Local Input
1.4.10 Card Reader
1.4.11 User Interface
1.4.11.1 Local User Interface
1.4.11.2 Remote User Interface
1.4.11.3 Types of User Interface (by capability)
1.4.11.3.1 Read-Only User Interface
1.4.11.3.2 Limited User Interface
1.4.11.3.3 Full User Interface
1.4.11.3.4 View-Only User Interface
1.4.11.4 Other User Interface Terminology
1.4.11.4.1 Writable User Interface
1.4.11.4.2 Privileged User Interface
1.4.12 Wireless Network
1.4.13 Wired Broadcast Network
1.5 ADMINISTRATIVE REQUIREMENTS
1.5.1 Points of Contact
1.5.2 Coordination
1.6 SUBMITTALS
1.7 CYBERSECURITY DOCUMENTATION
1.7.1 Proposed STIG and SRG Applicability Report
1.7.2 Cybersecurity Interconnection Schedule
1.7.3 Network Communication, Ports, Protocols and Services Report
1.7.4 Control System Inventory Reports
1.7.5 Software and Configuration Backups
1.7.6 Cybersecurity Network (Riser) Diagram
1.7.7 STIG, SRG and Vendor Guide Compliance Result Report
1.7.8 Control System Cybersecurity Documentation

1.7.8.1 For Mech-HVAC Control System Devices
1.7.8.1.1 Mech-HVAC Control System Devices FULLY Supporting User Accounts
1.7.8.1.2 All Other Mech-HVAC Control System Devices
1.7.8.2 Default Requirements for Control System Devices
1.8 SOFTWARE LICENSING
1.9 CYBERSECURITY DURING CONSTRUCTION
1.9.1 Contractor Computer Equipment
1.9.1.1 Operating System
1.9.1.2 Anti-Malware Software
1.9.1.3 Passwords and Passphrases
1.9.1.4 User-Based Authentication
1.9.1.5 Demonstration of Compliance
1.9.1.6 Contractor Computer Cybersecurity Compliance Statements
1.9.2 Temporary IP Networks
1.9.2.1 Network Boundaries and Connections
1.9.3 Government Access to Network
1.9.4 Temporary Wireless IP Networks
1.9.5 Passwords and Passphrases
1.9.6 Contractor Temporary Network Cybersecurity Compliance Statements
1.10 CYBERSECURITY DURING WARRANTY PERIOD

PART 2 PRODUCTS

2.1 ETHERNET SWITCH
2.2 DAISY CHAIN IP CONTROLLERS

PART 3 EXECUTION

3.1 CYBERSECURITY HARDENING AND CONFIGURATION GUIDES
3.2 NETWORK REQUIREMENTS
3.2.1 Wireless and Wired Broadcast Communication
3.2.1.1 Wireless and Wired Broadcast IP Communications
3.2.1.2 Non-IP Wireless Communication
3.2.2 Non-IP Control Networks
3.2.3 IP Control Networks
3.2.3.1 IP Network Routers
3.2.3.2 IP Devices With Multiple Ethernet Connections
3.2.4 Device Identification and Authentication
3.2.4.1 For Mech-HVAC Control System Devices
3.2.4.2 Default Requirements for Control System Devices
3.2.5 Cryptographic Module Authentication
3.3 ACCESS CONTROL REQUIREMENTS
3.3.1 User Accounts
3.3.1.1 Controllers
3.3.1.1.1 Mech-HVAC Control Systems
3.3.2 Unsuccessful Logon Attempts
3.3.2.1 Devices MINIMALLY Supporting Accounts
3.3.2.2 Devices FULLY Supporting Accounts
3.3.2.3 High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements
3.3.3 System Use Notification
3.3.3.1 System Use Notification for Remote User Interfaces
3.3.3.2 System Use Notification for Local User Interfaces
3.3.4 Permitted Actions Without Identification or Authentication
3.3.5 Enclosures
3.4 USER IDENTIFICATION AND AUTHENTICATION
3.4.1 User Identification and Authentication for All System Types

3.4.2 User Identification and Authentication for Specific System Types
3.4.2.1 Mech-HVAC Control Systems Devices
3.4.3 User Identification and Authentication for Specific Devices
3.4.4 Implementation of Identification and Authorization Requirements
3.4.5 Password-Based Authentication Requirements
3.4.5.1 Passwords for Controllers FULLY Supporting Accounts
3.4.5.2 Passwords for Remote Interfaces
3.4.5.3 Passwords for Devices Minimally Supporting Accounts
3.4.5.4 Password Configuration and Reporting
3.4.6 Authenticator Feedback
3.5 CYBERSECURITY AUDITING
3.5.1 Audit Events, Content of Audit Records, and Audit Generation
3.5.1.1 For Mech-HVAC Control System Controllers
3.5.1.1.1 Mech-HVAC Control System Controllers FULLY Supporting User Accounts
3.5.1.1.1.1 Audited Events
3.5.1.1.1.2 Audit Event Information To Record
3.5.1.1.2 Other Mech-HVAC Control System Controllers
3.5.1.2 Default Requirements for Control System Controllers
3.5.1.2.1 Controllers Which FULLY Support Accounts
3.5.1.2.1.1 Audited Events
3.5.1.2.1.2 Audit Event Information To Record
3.5.1.2.2 Controllers Which Do Not FULLY Support Accounts
3.5.2 Audit Time Stamps
3.5.3 Audit Storage Capacity and Audit Upload
3.6 REQUIREMENTS FOR LEAST FUNCTIONALITY
3.6.1 Device Capabilities
3.6.2 Software
3.7 SYSTEM AND COMMUNICATION PROTECTION
3.7.1 Denial of Service Protection
3.8 SAFE MODE AND FAIL SAFE OPERATION
3.9 SYSTEM MAINTENANCE TOOL SOFTWARE
3.10 DEVICE POWER
3.11 VULNERABILITY SCANNING
3.11.1 Controllers
3.12 FIPS 201-2 REQUIREMENT
3.13 SYSTEM AND INTEGRATION INTEGRITY
3.14 CONTROL SYSTEM CYBERSECURITY TESTING
3.14.1 Control System Cybersecurity Testing Procedures
3.14.2 Control System Cybersecurity Testing Execution
3.14.3 Control System Cybersecurity Testing Report
3.15 FIELD QUALITY CONTROL, CYBERSECURITY VALIDATION SUPPORT
3.16 CYBERSECURITY TRAINING

-- End of Section Table of Contents --

SECTION 25 05 11.01

CYBERSECURITY FOR MECH-HVAC FACILITY-RELATED CONTROL SYSTEMS

PART 1 GENERAL

Many subparts in this Section contain text in curly braces ("{" and "}") indicating which cybersecurity control and control correlation identifier (CCI) the requirements of the subpart relate to. The text inside these curly braces is for Government reference only and enables coordination of the requirements of this Section with the RMF process throughout the design and construction process. Text in curly braces are not contractor requirements.

This Section refers to Security Requirements Guide (SRGs) and Security Technical Implementation Guide (STIGs). STIGs and SRGs are available online at the Information Assurance Support Environment (IASE) website at https://public.cyber.mil/stigs/downloads/ and an SRG/STIG Applicability Guide and Collection Tool is available at https://public.cyber.mil/stigs/SCAP/. Not all control system components have applicable STIGs or SRGs. The "Control Systems SRG" does not apply to work performed under this Section; all requirements within this section to apply applicable SRGs DO NOT include the "Control Systems SRG".

1.1 CONTROL SYSTEM APPLICABILITY

There are multiple versions of this Section associated with this project. Different versions have requirements applicable to different control systems. This specific Section applies only to the following control systems:

UFGS Section Reference	Device	AIR FORCE PIT Level	Network Connectivity & Communication Protocol	Drawing/ Specification Cross-Reference	C-I-A Impact Ratings
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS	Microprocessor Based HVAC DDC	2A	BACnet/IP over Ethernet	M701 M801 M802	LOW- LOW- LOW

UFGS Section Reference	Device	AIR FORCE PIT Level	Network Connectivity & Communication Protocol	Drawing/ Specification Cross-Reference	C-I-A Impact Ratings
22 00 00 PLUMBING, GENERAL PURPOSE 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS	Electric Water Heater	2A	BACnet/IP over Ethernet	M701	LOW-LOW-LOW
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS	Thermostatic Mixing Valve (TMV)	2A	BACnet/IP over Ethernet	M701	LOW-LOW-LOW
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS	Packaged Rooftop Unit	2A	BACnet/IP over Ethernet	M701 M801 M802	LOW-LOW-LOW
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC	Fan Coils	0A	Dry Contacts over Copper Cables	M701 M801 M802	LOW-LOW-LOW
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC	Heat Pump	0A	Dry Contacts over Copper Cables	M701 M801 M802	LOW-LOW-LOW
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC	Fan	0A	Dry Contacts over Copper Cables	M701 M801 M802	LOW-LOW-LOW
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC	Unit Heater	0A	Analog and Discrete I/O over Copper Cables to DDC	M801	LOW-LOW-LOW

UFGS Section Reference	Device	AIR FORCE PIT Level	Network Connectivity & Communication Protocol	Drawing/ Specification Cross-Reference	C-I-A Impact Ratings
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC	VAV for Rooftop Unit	0A	Analog and Discrete I/O over Copper Cables to DDC	M801	LOW-LOW-LOW
22 00 00 PLUMBING, GENERAL PURPOSE	Water Meter to DDC	0A	4-20 mA (Analog) or Pulse Counter over Copper Cables	M701 M802	LOW-LOW-LOW
26 20 00 - INTERIOR DISTRIBUTION SYSTEM	Electrical Meter to DDC	2A	Ethernet (Per Client Comment) to DDC/UMCS	E601 M802	LOW-LOW-LOW
26 20 00 - INTERIOR DISTRIBUTION SYSTEM	Generator	0A	Analog and Discrete I/O over Copper Cables to DDC	E601 M802	LOW-LOW-LOW

1.2 RELATED REQUIREMENTS

This section does not contain sufficient requirements to procure a control system and must be used in conjunction with other Sections which specify control systems. This Section adds cybersecurity requirements to the control systems specified in other Sections, and as these requirements are conditioned on the control system being provided, there may be requirements in this Section that will not apply to this project. All Sections containing facility-related control systems or control system components are related to the requirements of this Section. Review all specification sections to determine related requirements.

In cases where a requirement is specified in both this Section and in another Section, the more stringent requirement must be met. In cases where a requirement in this Section conflicts with the requirements of another Section such that both requirements cannot be met at the same time, request direction from the Contracting Officer to determine which requirement applies to the project.

1.3 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST FIPS 140-2 (2001) Security Requirements for Cryptographic Modules

NIST FIPS 201-2 (2013) Personal Identity Verification

(PIV) of Federal Employees and Contractors

U.S. DEPARTMENT OF DEFENSE (DOD)

DODI 8551.01	(2014) Ports, Protocols, and Services Management (PPSM)
DTM 08-060	(2008) Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement

1.4 DEFINITIONS

1.4.1 Administrator Account

An administrator account is an account with full permissions to a device, application, or operating system, including the ability to create and modify other user accounts.

Note that the operating system Administrator Account may be different than Administrator Accounts for applications hosted on that operating system. Also, most controllers will not have any support for accounts and will therefore not have an 'Administrator Account'.

1.4.2 Computer

A computer is one of the following:

a. a device running a non-embedded desktop or server version of Microsoft Windows

b. a device running a non-embedded version of MacOS

c. a device running a non-embedded version of Linux

d. a device running a version or derivative of the Android Operating System, where Android is considered separate from Linux

e. a device running a version of Apple iOS

Unless otherwise indicated or clear from context use of the word "device" in this Section includes computers.

1.4.3 Controller

A device other than a computer or Ethernet switch.

1.4.4 Mission Space

A device or media is in mission space if physical access to the device or media is controlled by the organization served by the device. For example, a variable air volume (VAV) box controller in a suspended ceiling is in mission space if the VAV box serves that room; an electrical switchgear in an electrical room or an air handling unit (AHU) in a mechanical room or on a rooftop may still be considered to be in mission space if the organization (mission) served by that switchgear or AHU controls access to the electrical room, mechanical room or rooftop.

1.4.5 Network

A network is a group of two or more devices that can communicate using a network protocol. Network protocols must provide a method for addressing devices on the network; a communication method that does not provide an addressing scheme is not a networked form of communication. Devices that communicate using a method of communication that does not support device addressing are not using a network. Addresses may be other than IP addresses, and addressing may be at either Open Systems Interconnection (OSI) layer 2 or layer 3.

1.4.6 Network Connected

A component is network connected (or "connected to a network") only when the device has a network transceiver which is directly connected to the network and implements the network protocol. A device lacking a network transceiver (and accompanying protocol implementation) can never be considered network connected. Note that (unlike many IT definitions of "Network Connected") a device connected to a non-IP network is still considered network connected (an IP connection or IP address is not required for a device to be network connected).

1.4.6.1 Wireless Network Connected

Any device that supports wireless network communication is network connected to a wireless network, regardless of whether the device is communicating using wireless. Unless physically disabled, devices with wireless transceivers support wireless, it is not sufficient to disable the wireless in software.

1.4.7 Network Media

The thing that provides the communication channel between the devices on a network. Typically wire, but might include wireless, fiber optic, or even power line (some network protocols allow sending network signals over power wiring).

1.4.8 User Account Support Levels

The support for user accounts is categorized in this Section as one of three levels:

1.4.8.1 FULLY Supported

Device supports configurable individual accounts. Accounts can be created, deleted, modified, etc. Privileges can be assigned to accounts. These devices support user-based (as opposed to role-based) authentication.

1.4.8.2 MINIMALLY Supported

Device supports a small, fixed number of accounts (perhaps only one). Accounts cannot be modified. A device with only a "User" and an "Administrator" account would fit this category. Similarly, a device with two PINs for logon - one for restricted and one for unrestricted rights would fit here (in other words, the accounts do not have to be the traditional "username and password" structure). These devices typically only support role-based authentication.

Examples of devices which MINIMALLY support accounts are a) a variable

frequency drive with a single account which requires a PIN for access to configuration; and b) a room lighting control touchpad interface that has a single account.

1.4.8.3 NOT Supported

Device does not support any Access Enforcement therefore the whole concept of "account" is meaningless.

1.4.9 Manual Local Input

Manual Local Inputs are system analog or binary inputs that are adjustable by a person but are, by intrinsic hardware design, very limited in potential capabilities. Manual Local Inputs do not have touch screens or full keyboards, but may have a few buttons or dials to allow input. Manual Local Inputs do not have full graphic screens or dot-matrix displays, but may have simple lights (LEDs) or 7-segment displays. Manual Local Inputs do not have any sort of menu structure, each button has a single well-defined function.

Examples of Manual Local Inputs are H-O-A switches, simple thermostats, and disconnect switches.

1.4.10 Card Reader

A card reader is an input/output device whose primary function is to assist in two-factor authentication. A card reader must have an interface to read data from a card and may be able to write data to a card. A card reader may have a means (such as buttons, keypad, touchscreen, etc.) for a user to input a PIN or password, as well as a limited display.

1.4.11 User Interface

A User Interface (UI) is something other than a Manual Local Input or Card Reader that allows a person to interact with the system or device. Note that while a Card Reader is not by itself a User Interface, a User Interface may contain a Card Reader in order for it to authenticate its user. Within control systems, there are a wide range of User Interfaces.

Two important distinctions are 1) whether the user interface is Local or Remote, and 2) the effective capabilities of the User Interface to alter data, which is the "privilege" of the user interface (where effective privilege available to a specific user at a specific user interface is the combination of the greatest privilege offered by the user interface and the specific account the user is logged into).

1.4.11.1 Local User Interface

A Local User Interface is a user interface where the physical hardware the user interacts with (keyboard, buttons, display, etc.) is physically part of the device being affected. All of the relevant characteristics of the user interface are embodied within a single device.

Note that a Local UI may be able to access data in a different device, Local versus Remote in this context refers to the user interface itself; the capability to access data in a different device is covered under "Full User Interface".

1.4.11.2 Remote User Interface

A Remote User Interface implements a Client/Server model where the physical hardware the user interacts with (Client) is physically distinct from the device being affected (Server). Most or all of the security and functionality characteristics of the user interface are defined by the Server, not the Client. The Client and Server communicate via a network connection. A common example of a remote user interface is a web-based interface where the browser (client) is generally on different hardware than the web server (server). A Remote UI remains a Remote UI even if the user happens to be at a Client on the same hardware as the Server. What is important is that a) the Client may be on different hardware than the Server and b) the majority of the security and functional characteristics of the interface are defined at the Server.

Note that this definition of "remote" is consistent with that generally used in the control industry but is not aligned with the NIST 800-53 definition of "Remote", which refers to "outside the system". The term "Remote" here better aligns with the NIST 800-53 definition of "Network" (remote from within the system) Access.

1.4.11.3 Types of User Interface (by capability)

User interfaces are also categorized by their capabilities as being Read Only, Limited, or Full.

1.4.11.3.1 Read-Only User Interface

A Read Only User Interface (also referred to as a View-Only User Interface) is a user interface that only allows for reading data, it does not allow (have the capability to) modify data. A Read Only User Interface may be either Local or Remote. A User Interface that is configured to be Read Only (by some other means than the interface itself, such as using configuration software on a laptop) is a Read-Only Interface. Note a Read Only User Interface may have buttons (or touch screen, etc.) allowing the user to navigate through the presentation of data.

Examples of a Read Only User Interfaces are a) a publicly viewable "energy dashboard" showing weather data and energy usage within a building and b) digital wayfinding signage.

1.4.11.3.2 Limited User Interface

A Limited User Interface is a user interface that - by design - can only alter information local to the user interface. Note that the determination of "alter" includes only direct interactions, it explicitly excludes interactions that might occur as secondary effects. For example, an interface changing the flow setpoint in a pump controller is a direct interaction, the subsequent change in flow (as well as any subsequent downstream changes in valve position) are not direct interactions.

Two examples of LIMITED UIs are: a) a variable speed drive has a Limited Local User Interface which allows the user to change properties within the drive, but does not allow affecting things outside the drive; and b) a typical home WiFi Router has a Limited Remote User Interface which allows configuration of the Router, but does not allow direct interaction with other devices.

1.4.11.3.3 Full User Interface

A Full User Interface can alter information in devices outside the device with the user interface. For example, a typical Local Display Panel is a Full Local User Interface while a browser-based front end is a Full Remote User Interface.

1.4.11.3.4 View-Only User Interface

See Read-Only User Interface

1.4.11.4 Other User Interface Terminology

In addition to defining whether a user interface is a Hardware Limited, Read-Only, Limited or Full, and whether it is Local or Remote, user interfaces are classified by whether they are writable or privileged.

1.4.11.4.1 Writable User Interface

Any User Interface that is not Read-Only is Writable. (Limited User Interfaces and Full User Interfaces are both writable user interfaces (as they are capable of changing a value)).

1.4.11.4.2 Privileged User Interface

A Privileged UI is a UI that has sufficient capabilities or functionality that it requires specific cybersecurity measures to be put in place to limit its unauthorized use. Ultimately, whether a specific user interface is considered a Privileged User Interface must be determined by usage. Unless otherwise specified, user interfaces can be determined to be privileged or not using the following:

a. Read-Only User Interfaces are not privileged user interfaces.

b. Full User Interfaces are privileged user interfaces.

c. User interfaces that allow for configuration of auditing or allows for modification or deletion of audit logs are privileged user interface.

d. User interfaces that allow for reprogramming a network connected device is a privileged user interface.

e. Except as specified above, a Limited User Interface must be determined to be privileged or not based on the specific capabilities and use case of the user interface. In general however, user interfaces that do not offer significant capabilities above and beyond those available at that location via other means (e.g. such as a disconnect switch, breaker, or hand-off-auto switch, or physical attack) are not privileged.

1.4.12 Wireless Network

Any network that communicates without using wires or fiber optics as the communication media. Wireless networks include: WiFi, Bluetooth, ZigBee, cellular, satellite, long and short wave radio, 2.4 GHz, free space optical, point-to-point laser, microwave, and IR.

1.4.13 Wired Broadcast Network

Wired Broadcast Networks are any network, such as powerline carrier networks and modem (wired telephony), that use wire-based technologies where there is not a clearly defined boundary for signal propagation.

1.5 ADMINISTRATIVE REQUIREMENTS

1.5.1 Points of Contact

Coordinate with the following Points of Contact as indicated in this Section and as required. Not all projects will require coordination with all Points of Contact. When coordination is required and no Point of Contact is indicated, coordinate with the Contracting Officer (KO).

a. Government Computer Access Point of Contact: Contracting Office (KO)

b. HTTPS Certificate Point of Contact: Contracting Officer (KO)

c. Email Address Point of Contact: Contracting Officer (KO)

d. Password Point of Contact: Contracting Officer (KO)

e. Mobile Code Point of Contact: Contracting Officer (KO)

1.5.2 Coordination

Coordinate the execution of this Section with the execution of all other Sections related to control systems as indicated in the paragraph RELATED REQUIREMENTS. Items that must be considered when coordinating project efforts include but are not limited to:

a. If requesting permission for wireless or wired broadcast communication, the Wireless and Wired Broadcast Communication Request submittal must be approved prior to control system device selection and installation.

b. If requesting permission for alternate account lock permissions, the Device Account Lock Exception Request must be approved prior to control system device selection and installation.

c. If requesting permission for the use of a device with multiple physical connections to IP networks, the Multiple IP Connection Device Request must be approved prior to control system device selection and installation.

d. Wireless testing may be required as part of the control system testing. See requirements for the Wireless Communication Test Report submittal.

e. If the Device Audit Record Upload Software is to be installed on a computer not being provided as part of the control system, coordination is required to identify the computer on which to install the software.

f. The Cybersecurity Interconnection Schedule must be coordinated with other work that will be interconnected to, and interconnections must be approved by the Government before relying on them for system functionality.

g. Cybersecurity testing support must be coordinated across control systems and with the Government cybersecurity testing schedule.

h. Passwords must be coordinated with the indicated contact for the project site.

i. If applicable, HTTPS web server certificates must be obtained from the indicated HTTPS Certificate Point of Contact.

j. Contractor Computer Cybersecurity Compliance Statements must be provided for each contractor using contractor owned computers.

1.6 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Device Account Lock Exception Request; G

Multiple Ethernet Connection Device Request; G

Contractor Computer Cybersecurity Compliance Statements; G

Contractor Temporary Network Cybersecurity Compliance Statements; G

Cybersecurity Interconnection Schedule ; G

Proposed STIG and SRG Applicability Report; G

Pre-Construction Control System Inventory Report ; G

SD-02 Shop Drawings

Network Communication, Ports, Protocols and Services Report; G

Cybersecurity Network (Riser) Diagram ; G

SD-03 Product Data

Control System Cybersecurity Documentation; G

SD-06 Test Reports

Control System Cybersecurity Testing Procedures; G

Control System Cybersecurity Testing Report; G

SD-07 Certificates

Software Licenses; G

SD-11 Closeout Submittals

Confidential Password Report; G

Enclosure Keys; G

Software and Configuration Backups; G

System Maintenance Tool Software; G

Control System Scanning Tools; G

STIG, SRG and Vendor Guide Compliance Result Report; G

Final Control System Inventory Report; G

1.7 CYBERSECURITY DOCUMENTATION

{For Government Reference Only: This subpart (and its subparts) relates to PL-7; CCI-003071}

1.7.1 Proposed STIG and SRG Applicability Report

For each model of network connected or network infrastructure device, use the DISA SRG/STIG Applicability Guide and Collection Tool (available at https://public.cyber.mil/stigs/SCAP/to identify applicable STIGs or SRGs and provide a report indicating applicable STIGs and SRGs for each model. Provide the Proposed STIG and SRG Applicability Report concurrently with the Pre-Construction Control System Inventory Report.

1.7.2 Cybersecurity Interconnection Schedule

{For Government Reference Only: This subpart relates to CA-3(b), PL-8, SC-7(9), SC-7(11); CCI-000258, CCI-003072, CCI-003073, CCI-003075, CCI-002398, CCI-002399, CCI-002401, CCI-002402, CCI-002403.}

Provide a completed Cybersecurity Interconnection Schedule documenting network connections between the installed system and other systems. Provide the following information for each device directly communicating between systems: Device Identifier, Device Manufacturer, Device Description, Transport layer Protocol, Network Address, Port (if applicable), MAC (Layer 2) address (if applicable), Media, Application Protocol, Service (if applicable), Descriptive Purpose of communication.

If other control system Sections used on this project include submittals documenting this information, provide copies of those submittals to meet this requirement.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Cybersecurity Interconnection Schedule as an editable Microsoft Excel file (a template Cybersecurity Interconnection Schedule in Excel format is available at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-1

1.7.3 Network Communication, Ports, Protocols and Services Report

{For Government Reference Only: This subpart (and its subparts) relates to CA-9, PL-8; CCI-002102, CCI-002103, CCI-002104, CCI-002105, CCI-003072, CCI-003073, CCI-003075 and also the submittal requirements associated with CM-6, CM-7, including CM-7(3), CCI-000388.}

Provide a Network Communication, Ports, Protocols and Services Report. For each networked device, document device identifier and the

communication characteristics of the device including communication protocols, services used, encryption employed, and a general description of what information is communicated over the network. For each device using IP communication, document all TCP and UDP ports used. For each device using non-IP communication, document communication protocol and media used. If other control system Sections used on this project include submittals documenting this information, provide copies of those submittals to meet this requirement.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Network Communication, Ports, Protocols and Services Report as an editable Microsoft Excel file.

1.7.4 Control System Inventory Reports

{For Government Reference Only: This subpart (and its subparts) relates to CM-8(a), SI-17, IA-3; CCI-000389, CCI-000392, CCI-000398, CCI-002773, CCI-002774, CCI-002775, CCI-000777, CCI-000778, CCI-001958}

Provide a Pre-Construction Control System Inventory Report report and a Final Control System Inventory Report, using the Inventory Spreadsheet listed under this Section at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-1 In the Control System Inventory Reports, document all networked devices, including network infrastructure devices. For each device provide all applicable information for which there is a field on the spreadsheet in accordance with the instructions on the spreadsheet.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Control System Inventory Reports as editable Microsoft Excel files. Provide the Pre-Construction Control System Inventory Report concurrently with the Proposed STIG and SRG Applicability Report

1.7.5 Software and Configuration Backups

{For Government Reference Only: This subpart (and its subparts) relates to CP-10; CCI-000550, CCI-000551, CCI-000552}

For all controllers, provide a backup of the controller configuration and the source code for all loaded application programs (all software that is not common to every controller of the same manufacturer and model).

If any or all of these are provided under another Section, provide documentation indicating this and referencing those submittals.

1.7.6 Cybersecurity Network (Riser) Diagram

{For Government Reference Only: This subpart (and its subparts) relates to PL-2(a), PL-8; CCI-003051, CCI-003053, CCI-003072, CCI-003073, CCI-003075}

Provide a cybersecurity network (riser) diagram of the complete control system including all network and device hardware. For each device, include the device identifier, device type, and manufacturer. If the control system specifications require a riser diagram submittal, provide a copy of that submittal as the cybersecurity riser diagram. Otherwise, provide a riser diagram in one-line format overlayed on a facility schematic.

1.7.7 STIG, SRG and Vendor Guide Compliance Result Report

For every component (device or software) with an applicable STIG or SRG in the Proposed STIG and SRG Applicability Report, document compliance with the STIG or SRG requirements.

a. For components which are scannable by the Evaluate-STIG tool (available online at (CAC Required), include the Evaluate-STIG report and raw scan results in addition to the final, manually reviewed and revised, documentation of compliance with STIG and SRG requirements. Checklist files should not contain any findings with a Not Reviewed (NR) status after manual reviews.

b. For components which do not support automated scanning, a manual review using the General Purpose STIG option should be done. A completed Checklist file should not contain any findings with a Not Reviewed (NR) status after manual reviews

For every component (device or software) with manufacturer provided cybersecurity documentation, procedure, or method for secure configuration or installation, provide a report documenting how the component was configured and any deviation from the manufacturer instructions.

1.7.8 Control System Cybersecurity Documentation

{For Government Reference Only: This subpart (and its subparts) relates to SA-5(a),SA-5(b),SA-5(c), SA-22(b); CCIs: CCI-003124, CCI-003125, CCI-003126, CCI-003127, CCI-003128, CCI-003129, CCI-003130, CCI-003131, CCI-003374}

Provide a Control System Cybersecurity Documentation submittal containing the indicated information for each device and software application.

1.7.8.1 For Mech-HVAC Control System Devices

1.7.8.1.1 Mech-HVAC Control System Devices FULLY Supporting User Accounts

For all Mech-HVAC Control System Devices which FULLY support user accounts, provide:

a. Documentation that describes secure configuration of the device {For Government Reference Only: relates to CCI-003124}

b. Documentation that describes secure operation of the device {For Government Reference Only: relates to CCI-003124}

c. Documentation that describes effective use and maintenance of security functions or mechanisms for the device {For Government Reference Only: relates to CCI-003127}

d. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device {For Government Reference Only: relates to CCI-003128}

e. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms; or a specific indication that there are no user-accessible security functions or mechanisms in the device {For

Government Reference Only: relates to CCI-003129}

f. Documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

1.7.8.1.2 All Other Mech-HVAC Control System Devices

For all Mech-HVAC Control System Devices which do not FULLY support user accounts, provide:

a. Documentation that describes secure configuration of the device; or a specific indication that there are no secure configuration steps that apply {For Government Reference Only: relates to CCI-003124}

b. Documentation that describes effective use and maintenance of security functions or mechanisms for the device; or a specific indication that there are no security functions or mechanisms in the device {For Government Reference Only: relates to CCI-003127}

c. For devices which include a user interface, documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

1.7.8.2 Default Requirements for Control System Devices

For control system devices where Control System Cybersecurity Documentation requirements are not otherwise indicated in this Section, provide:

a. Documentation that describes secure configuration of the device {For Government Reference Only: relates to CCI-003124}

b. Documentation that describes secure installation of the device {For Government Reference Only: relates to CCI-003125}

c. Documentation that describes secure operation of the device {For Government Reference Only: relates to CCI-003124}

d. Documentation that describes effective use and maintenance of security functions or mechanisms for the device {For Government Reference Only: relates to CCI-003127}

e. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device {For Government Reference Only: relates to CCI-003128}

f. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms {For Government Reference Only: relates to CCI-003129}

g. Documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

h. Documentation that describes user responsibilities in maintaining the security of the device {For Government Reference Only: relates to

CCI-003131}

i. Documentation of the published last date of support by the manufacturer or indication that a published date is not available. {For Government Reference Only: relates to CCI-003374}

1.8 SOFTWARE LICENSING

{For Government Reference Only: This subpart (and its subparts) relates to SI-2(a), SI-2(c), SI-7(14); CCI-001227, CCI-002605, CCI-002737}

For all software provided that has not already been licensed to the government or project site, provide a license to the Government for a period of no less than 5 years, and the license must also include the following software updates:

a. Security and bug-fix patches issued by the software manufacturer.

b. Security patches to address any vulnerability identified in the National Vulnerability Database at http://nvd.nist.gov with a Common Vulnerability Scoring System (CVSS) severity rating of MEDIUM or higher.

Provide a single Software Licenses submittal with documentation of the software licenses for all software provided

1.9 CYBERSECURITY DURING CONSTRUCTION

{For Government Reference Only: This subpart (and its subparts) relates to AC-18, CA-3; CCI-000258}

In addition to the control system cybersecurity requirements indicated in this section, meet following requirement throughout the construction process.

1.9.1 Contractor Computer Equipment

Contractor owned computers may be used for construction. Contractor computers connected to the control system, control system network, or a control system component at any point during construction must meet the following requirements:

1.9.1.1 Operating System

The operating system must be an operating system currently supported by the manufacturer of the operating system. The operating system must be current on security patches and operating system manufacturer required updates.

1.9.1.2 Anti-Malware Software

The computer must run anti-malware software from a reputable software manufacturer. Anti-malware software must be a version currently supported by the software manufacturer, must be current on all patches and updates, and must use the latest definitions file. Computers used on this project must perform a full antivirus scan at least once per day. Computers which have connected to any other network since the last full antivirus scan must perform a full antivirus scan prior to connection to the control system network or to the temporary contractor-installed IP network.

Perform an antivirus scan on all removable media (e.g., external hard drives, CDs, DVDs, USB flash drives) prior to connecting to the control system environment.

1.9.1.3 Passwords and Passphrases

The passwords and passphrases for computers, applications, and web-based applications supporting passwords must be changed from their default values. Passwords must be a minimum of eight characters with a minimum of one uppercase letter, one lowercase letter, one number and one special character.

1.9.1.4 User-Based Authentication

Each user must have a unique account; sharing of a single account between multiple users is prohibited.

1.9.1.5 Demonstration of Compliance

The Government has the right to require demonstration of computer compliance with these requirements at any time during the project.

1.9.1.6 Contractor Computer Cybersecurity Compliance Statements

Provide a single submittal containing completed Contractor Computer Cybersecurity Compliance Statements for each company using contractor owned computers. Contractor Computer Cybersecurity Compliance Statements must use the template published at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-1 Each Statement must be signed by a cybersecurity representative for the relevant company.

1.9.2 Temporary IP Networks

Temporary contractor-installed IP networks may be used during construction. When used, temporary contractor-installed IP networks connected to the control system, control system network, or a control system component at any point during construction must meet the following requirements:

1.9.2.1 Network Boundaries and Connections

The network must not extend outside the project site and must not connect to any IP network other than those specifically provided or furnished for this project. Any and all access to the network from outside the project site is prohibited.

1.9.3 Government Access to Network

Government personnel must be allowed to have complete and immediate access to the network at any time in order to verify compliance with this specification.

1.9.4 Temporary Wireless IP Networks

In addition to the other requirements on temporary IP networks, temporary wireless IP (WiFi) networks, when permitted, must not interfere with existing wireless networks, must use WPA2 security and must not broadcast the network name (SSID). Network names (SSID) for wireless networks must

be changed from their default values.

1.9.5 Passwords and Passphrases

The passwords and passphrases for all network devices and network access must be changed from their default values. Passwords must be a minimum 8 characters with a minimum of one uppercase letter, one lowercase letter, one number and one special character.

1.9.6 Contractor Temporary Network Cybersecurity Compliance Statements

Provide a single submittal containing completed Contractor Temporary Network Cybersecurity Compliance Statements for each company implementing a temporary IP network. Contractor Temporary Network Cybersecurity Compliance Statements must use the template published at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-1 Each Statement must be signed by a cybersecurity representative for the relevant company. If no temporary IP networks will be used, provide a single copy of the Statement indicating this.

1.10 CYBERSECURITY DURING WARRANTY PERIOD

All work performed on the control system after acceptance must be performed using Government Furnished Equipment or equipment specifically and individually approved by the Government.

PART 2 PRODUCTS

All products used on this project must meet the indicated requirements, but not all products specified here will be required by every project.

2.1 ETHERNET SWITCH

Not Applicable

2.2 DAISY CHAIN IP CONTROLLERS

Controllers used as Daisy Chain IP Controllers must be IP controllers with exactly two Ethernet network connections and basic built-in switch capabilities to allow implementation of an Ethernet network in a daisy chain architecture. Switches incorporated by Daisy Chain IP Controllers are not required to meet the requirements for Ethernet Switches as defined in this Section.

PART 3 EXECUTION

3.1 CYBERSECURITY HARDENING AND CONFIGURATION GUIDES

Install, configure, and harden all hardware and software furnished on this project in accordance with manufacturer provided documentation, procedures, or methods for secure configuration or installation. Do not implement specific hardening actions if that action would conflict with required functionality or another requirement of this Section.

3.2 NETWORK REQUIREMENTS

3.2.1 Wireless and Wired Broadcast Communication

{For Government Reference Only: This subpart (and its subparts) relates

to AC-18, AC-18(3); CCI-001438, CCI-001439, CCI-002323, CCI-001441, CCI-001449}

Unless explicitly authorized by the Government, do not use any wireless or wired broadcast communication.

3.2.1.1 Wireless and Wired Broadcast IP Communications

Do not install wireless or wired broadcast IP networks, including: do not install a wireless access point; do not install or configure an ad-hoc wireless network; do not install or configure a WiFi Direct communication.

When explicitly authorized by the Government, wireless IP communication may be used to communicate with an existing wireless network.

3.2.1.2 Non-IP Wireless Communication

For LOW Impact Systems: When non-IP wireless communication is explicitly authorized by the Government, use the maximum level of encryption supported by the specific protocol employed and select signal strength and radiated power to the minimum necessary for reliable communication.

3.2.2 Non-IP Control Networks

When control system specifications require particular communication protocols, use only those communication protocols and only as specified. Do not implement any other communication protocol.

When control system specifications do not indicate requirements for communication protocols, use only those protocols required for operation of the system as specified.

3.2.3 IP Control Networks

{For Government Reference Only: This subpart relates to CM-6(a), CM-7(a), CM-7(b), CM-7(1)(b), SC-41; CCI-001588, CCI-000381, CCI-000380, CCI-000381, CCI-000382, CCI-001761, CCI-001762, CCI-002544, CCI-002545, CCI-002546.}

IP Networks must be Ethernet networks and must use switches which are Ethernet Switches or Daisy Chain IP Controllers as defined in this Section. Do not use nonsecure functions, ports, protocols and services as defined in DODI 8551.01 unless those ports, protocols and services are specifically required by the control system specifications or otherwise specifically authorized by the Government. Do not use ports, protocols and services that are not specified in the control system specifications or required for operation of the control system.

3.2.3.1 IP Network Routers

Do not install any device that performs IP routing.

3.2.3.2 IP Devices With Multiple Ethernet Connections

Except for Ethernet Switches and Daisy Chain IP Controllers, devices must not have more than one Ethernet connection to IP networks unless doing so is required by the project specifications and the specific application is approved. If a device with Multiple Ethernet Connections to IP networks is required, provide a Multiple Ethernet Connection Device Request using

the Multiple Ethernet Connection Device Request Template at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-1 to request approval for each device. If a device with Multiple Ethernet Connections to IP networks is not required, instead provide a document stating that no approval is being requested.

3.2.4 Device Identification and Authentication

{For Government Reference Only: This subpart (and its subparts) relates to IA-3; CCI-000777, CCI-000778, CCI-001958.}

3.2.4.1 For Mech-HVAC Control System Devices

Devices using HTTP as a control protocol must use HTTPS instead.

3.2.4.2 Default Requirements for Control System Devices

For control system devices where Device Identification and Authentication requirements are not otherwise indicated in this Section: Devices using HTTP as a control protocol must use HTTPS instead.

3.2.5 Cryptographic Module Authentication

{For Government Reference Only: This subpart (and its subparts) relates to IA-7; CCI-000803}

For devices (including but not limited to NIST FIPS 140-2 compliant radios) that have STIG/SRGs related to cryptographic module authentication (CCI-000803), comply with the requirements of those STIG/SRGs.

3.3 ACCESS CONTROL REQUIREMENTS

3.3.1 User Accounts

{For Government Reference Only: This subpart (and its subparts) relate to AC-2(a), AC-3, AC-6(1), AC-6(10), AC-6(2), AC-6(9), CM-11(2), and IA-2; CCI-002110, CCI-000213, CCI-001558, CCI-002221, CCI-002222, CCI-002223, CCI-002235, CCI-000039, CCI-001419, CCI-002234, CCI-001812, and CCI-000764. }

Any user interface supporting user accounts (either FULLY or MINIMALLY) must limit access according to specified limitations for each account. Install and configure any device having a STIG or SRG in accordance with that STIG or SRG.

All user interfaces FULLY supporting accounts must implement user-based authentication where each account is uniquely assigned to a specific user. User interfaces FULLY supporting accounts must implement at least three (3) levels of user account privilege including: 1) an account with read-only permissions 2) an account with full permissions including account creation and modification and 3) an account with greater permissions than read-only but without account creation and modification. Disable any unnecessary or unused accounts. Disable any "guest-level" accounts that are created on the system by default.

3.3.1.1 Controllers

For user interfaces provided by controllers, provide access control in accordance with the User Interface Requirements table for the applicable

control system and user interface type.

a. For table entries of "NA": NA means Not Applicable, there are no interfaces in this category.

b. For table entries of "None Required": The user interface is not required to support user accounts.

c. For table entries of "MINIMALLY": The user interface must at least MINIMALLY support user accounts.

d. For table entries of "FULLY": The user interface must at FULLY support user accounts.

e. For table entries of "KEY": The user interface must have physical security in the form of either a key lock on the interface itself or be furnished inside a lockable enclosure. Where this is required for a read only interface, the lockable enclosure must prevent viewing of data on the interface; for other interfaces, this lockable enclosure must prevent using the interface to alter data.

f. For table entries of "Physical Security": For Local FULL interfaces, the interface must be located inside mission space. For Local Limited (not FULL) interfaces, the user interface must either a) be located within mission space or b) be protected by physical security at least as good as the control devices (and equipment controlled by the control devices) affected by the interface. For purposes of this requirement, 'affected' includes controllers with data that can be directly altered by the interface, as well as mechanical and/or electrical equipment directly controlled by those controllers, but does not include other interactions.

g. Entries of the form "X and Y" must meet both the requirement indicated for X and the requirement indicated for Y. For example, an entry of "MINIMALLY and Physical Security" indicates the user interface must both MINIMALLY support accounts and have physical security.

h. Entries of the form "X or Y" must meet either the requirement indicated for X or the requirement indicated for Y.

3.3.1.1.1 Mech-HVAC Control Systems

User Interface Requirements for LOW Impact Mech-HVAC Control Systems	
User Interface Type	**Access Control Requirement**
Local Read Only (see note 1)	None Required
Local Limited, Non-privileged	MINIMALLY
Local Limited, Privileged	MINIMALLY and/or Physical Security
Local Full	MINIMALLY
Remote Read Only	None Required

User Interface Requirements for LOW Impact Mech-HVAC Control Systems	
User Interface Type	**Access Control Requirement**
Remote Limited, Non-Privileged	MINIMALLY
Remote Limited, Privileged AND Remote Full (see note 2)	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged	

3.3.2 Unsuccessful Logon Attempts

{For Government Reference Only: This subpart (and its subparts) relate to AC-7 (a), AC-7 (b); CCI-000043, CCI-000044, CCI-001423, CCI-002236, CCI-002237, CCI-002238}

Except for high availability user interfaces indicated as exempt, devices must meet the indicated requirements for handling unsuccessful logon attempts. If a device cannot meet these requirements, document device capabilities to protect from subsequent logon attempts and propose alternate protections in a Device Account Lock Exception Request submittal. Do not implement alternate protection measures in lieu of the indicated requirements without explicit permission from the Government. If no Device Account Lock Exceptions are requested, provide a document stating that no approval is being requested as the Device Account Lock Exception Request.

3.3.2.1 Devices MINIMALLY Supporting Accounts

For LOW Impact Systems: Devices which MINIMALLY (but not FULLY) support accounts must lock the user account after five consecutive failed login attempts and must unlock the user account after 15 minutes have elapsed without an unsuccessful login attempt or by a successful login to a separate administrator account.

3.3.2.2 Devices FULLY Supporting Accounts

Devices which FULLY support accounts must meet the following requirements.

a. It must lock the user account when three unsuccessful logon attempts occur within a 15 minute interval.

b. Once an account is locked, the account must stay locked until unlocked by an administrator. If the account being locked is the sole administrator account on the device, the account must stay locked for 1 hour and then automatically unlock.

c. Once the indicated number of unsuccessful logon attempts occurs, delay further logon prompts by 5 seconds.

3.3.2.3 High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements

There are no high availability interfaces which are exempt from unsuccessful logon attempts requirements.

3.3.3 System Use Notification

{For Government Reference Only: This subpart (and its subparts) relates to AC-8; CCI-000048, CCI-002247, CCI-002243, CCI-002244, CCI-002245, CCI-002246, CCI-000050, CCI-002248}

3.3.3.1 System Use Notification for Remote User Interfaces

Remote user interfaces must display a warning banner meeting the requirements of DTM 08-060 on screen.

3.3.3.2 System Use Notification for Local User Interfaces

Devices which are connected to a network and have a local user interface must display a warning banner meeting the requirements of DTM 08-060 on the user interface screen if capable of doing so and must have a permanently affixed label with an approved banner from DTM 08-060 if unable to display the warning banner on the screen. Where it is impractical (perhaps due to device size) to affix the label to the device, affix the label to the device enclosure.

Labels must be machine printed or engraved, plastic or metal, designed for permanent installation, must use a font no smaller than 14 point, and must provide a high contrast between font and background colors.

3.3.4 Permitted Actions Without Identification or Authentication

{For Government Reference Only: This subpart (and its subparts) relates to AC-14; CCI-000061, CCI-000232}

The control system must require identification and authentication before allowing any actions except read-only actions by a user acting from a user interface which MINIMALLY or FULLY supports accounts.

3.3.5 Enclosures

Prior to final acceptance of the system, lock all lockable enclosures. Submit an Enclosure Keys submittal with all copies of keys for all enclosures and a key inventory list documenting all keys. Label each key with the matching enclosure identifier.

3.4 USER IDENTIFICATION AND AUTHENTICATION

{For Government Reference Only: This subpart (and its subparts) relates to IA-2, IA-2(1),IA-2(12), IA-5 IA-5(b), IA-5(c), IA-5(e), IA-5(g), IA-5(1), IA-5(11); CCI-000764, CCI-000765, CCI-001953, CCI-001954, CCI-001544, CCI-001989, CCI-000182, CCI-001610, CCI-000192, CCI-000193, CCI-000194, CCI-000205, CCI-001619, CCI-001611, CCI-001612, CCI-001613, CCI-001614, CCI-000195, CCI-001615, CCI-000196, CCI-000197, CCI-000199, CCI-000198, CCI-001616, CCI-001617, CCI-000200, CCI-001618, CCI-002041, CCI-002002, CCI-002003. }

This subpart indicates requirements for specific methods of identification

and authentication for users and user accounts. Where these requirements conflict apply the following order of precedence: 1) If present, Device Specific Requirements take precedence over any other requirements; and then 2) multifactor authentication requirements take precedence over password requirements.

3.4.1 User Identification and Authentication for All System Types

Unless otherwise indicated, all user interfaces supporting accounts (either FULLY or MINIMALLY) must implement Identification and Authorization via passwords.

3.4.2 User Identification and Authentication for Specific System Types

System specific requirements are in addition to and supersede those indicated for all system types. When no additional requirements are indicated for a specific system type the requirements for all systems still apply to that system type.

3.4.2.1 Mech-HVAC Control Systems Devices

No additional system specific requirements apply.

3.4.3 User Identification and Authentication for Specific Devices

There are no additional device specific user interface requirements

3.4.4 Implementation of Identification and Authorization Requirements

Identification and Authorization must be met by one of the following methods:

a. Direct implementation in the user interface.

b. For remote interfaces: an implementation shared between the remote user interface server and the remote user interface client. For example, a requirement for PIV authentication may be met on a remote user interface by a PIV reader on a web browser client which sends the authentication information via HTTPS to the remote server.

3.4.5 Password-Based Authentication Requirements

3.4.5.1 Passwords for Controllers FULLY Supporting Accounts

All controllers FULLY supporting accounts and supporting password-based authentication must enforce the following requirements:

a. Minimum password length of 15 characters

b. Password must contain at least one uppercase character.

c. Password must contain at least one lowercase character.

d. Password must contain at least one numeric character.

e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.

f. Password must have a maximum lifetime of sixty (60) days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.

g. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters.

h. Passwords must be cryptographically protected during storage and transmission.

3.4.5.2 Passwords for Remote Interfaces

Passwords for connecting to a Remote User Interface supporting password-based authentication must enforce the following requirements:

a. Minimum password length of 15 characters

b. Password must contain at least one uppercase character.

c. Password must contain at least one lowercase character.

d. Password must contain at least one numeric character.

e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.

f. Password must have a maximum lifetime of 60 days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.

g. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters (where location is significant, a character may be reused if it is in a different position).

h. Passwords must be cryptographically protected during storage and transmission.

3.4.5.3 Passwords for Devices Minimally Supporting Accounts

Devices MINIMALLY supporting accounts must support passwords with a minimum length of four characters.

3.4.5.4 Password Configuration and Reporting

For all devices with a password, change the password from the default password. Coordinate selection of passwords with the Password Point of Contact. Do not use the same password for more than one device unless specifically instructed to do so. Provide a Confidential Password Report documenting the password for each device and describing the procedure to change the password for each device.

Do not provide the Password Summary Report in electronic format. Provide two hardcopies of the Password Summary Report, each copy in its own sealed envelope.

3.4.6 Authenticator Feedback

{For Government Reference Only: This subpart relates to IA-6; CCI-000206}

Devices must never show authentication information, including passwords, on a display. Devices that momentarily display a character as it is entered, and then obscure the character, are acceptable. For devices that have STIGs or SRGs related to obscuring of authenticator feedback (CCI-000206), comply with the requirements of those STIGS/SRGs.

3.5 CYBERSECURITY AUDITING

Where an auditing requirement exists for email notification, notify via email the application administrator and Information System Security Officer (ISSO) of the event. Coordinate with the Email Address Point of Contact for email addresses. If outgoing email is not available to the system, disable email notifications.

3.5.1 Audit Events, Content of Audit Records, and Audit Generation

{For Government Reference Only: This subpart (and its subparts) relates to AU-2(a), AU-2(c), AU-2(d), AU-3, AU-10, AU-12, AU-14(b), AU-14(1), AU-14(2), AU-14(3), CM-5(1), SC-7 (9); CCI-000123, CCI-001571, CCI-000125, CCI-001485, CCI-000130, CCI-000131, CCI-000132, CCI-001230, CCI-000133, CCI-000134, CCI-001487, CCI-000166, CCI-001899, CCI-000169, CCI-001459, CCI-000171, CCI-000172, CCI-001910, CCI-001914, CCI-001919, CCI-001464, CCI-001462, CCI-001920, CCI-001814, CCI-002400. }

For devices that have STIG/SRGs related to audit events, content of audit records or audit generation, comply with the requirements of those STIG/SRGs.

If auditing requirements can be met using existing control system alarm or event capabilities, those existing capabilities may be used to meet these requirements.

3.5.1.1 For Mech-HVAC Control System Controllers

3.5.1.1.1 Mech-HVAC Control System Controllers FULLY Supporting User Accounts

For each controller which FULLY supports accounts, provide the capability to select audited events and the content of audit logs. Configure controllers to audit the indicated events, and to record the indicated information for each auditable event.

3.5.1.1.1.1 Audited Events

Configure each controller to audit the following events:

a. Successful and unsuccessful logon attempts to the controller

b. Successful logouts

c. All account creations, modifications, disabling, and terminations.

d. All controller shutdown and startup

3.5.1.1.1.2 Audit Event Information To Record

Configure each controller to record, for each auditable event, the following information (where applicable to the event):

a. what type of event occurred

b. when the event occurred

c. the identity of any individuals or subjects associated with the event

3.5.1.1.2 Other Mech-HVAC Control System Controllers

There are no requirements to perform auditing at Mech-HVAC field controllers that do not FULLY support accounts.

3.5.1.2 Default Requirements for Control System Controllers

For control system controllers where Audit Events, Content of Audit Records, and Audit Generation are not otherwise indicated in this Section:

3.5.1.2.1 Controllers Which FULLY Support Accounts

For each controller which FULLY supports accounts, provide the capability to select audited events and the content of audit logs. Configure controllers to audit the indicated events, and to record the indicated information for each auditable event.

3.5.1.2.1.1 Audited Events

Configure each controller to audit the following events:

a. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels)

b. Successful and unsuccessful logon attempts

c. Successful logouts

d. Concurrent logons from different workstations

e. All account creations, modifications, disabling, and terminations.

f. All kernel module load, unload, and restart

3.5.1.2.1.2 Audit Event Information To Record

Configure each controller to record, for each auditable event, the following information (where applicable to the event):

a. what type of event occurred

b. when the event occurred

c. where the event occurred

d. the source of the event

e. the outcome of the event

f. the identity of any individuals or subjects associated with the event

3.5.1.2.2 Controllers Which Do Not FULLY Support Accounts

For each controller which does not FULLY support accounts configure the controller to audit all controller shutdown and startup events and to record for each event the type of event and when the event occurred.

3.5.2 Audit Time Stamps

{For Government Reference Only: This subpart (and its subparts) relates to AU-8; CCI-000159, CCI-001889, CCI-001890.}

Any device (computer or controller) generating audit records must have an internal clock capable of providing time with a resolution of one second. Clocks must not drift more than 10 seconds per day. Configure the system so that each device (computer or controller) generating audit records maintains accurate time to within 1 second. Note that if the control system specifications include requirement for clocks, the most stringent requirement applies.

3.5.3 Audit Storage Capacity and Audit Upload

{For Government Reference Only: This subpart (and its subparts) relates to AU-4; CCI-001848, CCI-001849}

The creation of audit records must never interfere with normal device operation. Devices must cease collection of auditing information if required to maintain normal operation.

a. For devices that have STIG/SRGs related to audit storage capacity (CCI-001848 or CCI-001849) comply with the requirements of those STIG/SRGs.

b. For controllers capable of generating audit records, provide 60 days worth of secure local storage, assuming 10 auditable events per day.

3.6 REQUIREMENTS FOR LEAST FUNCTIONALITY

{For Government Reference Only: This subpart (and its subparts), along with the Network Communication, Ports, Protocols and Services Report submittal specified elsewhere in this section, relates to CM-6(a), CM-6(c), CM-7, CM-7(1)(b), SC-41; CCI-000363, CCI-000364, CCI-000365, CCI-001588, CCI-001755, CCI-000381, CCI-000380, CCI-000382, CCI-001761, CCI-001762, CCI-002544, CCI-002545, CCI-002546. }

For devices that have a STIG or SRG related to Requirements for Least Functionality (such as configuration settings and port and device I/O access for least functionality), install and configure the device in accordance with that STIG or SRGs.

3.6.1 Device Capabilities

For Mech-HVAC Control Systems: Do not provide devices with remote user interfaces or with full user interfaces where one was not required. Do not use a networked sensor or actuator where a non-networked sensor or actuator would suffice.

For Other Control Systems: Do not provide devices with remote user interfaces or with full user interfaces where one was not required.

3.6.2 Software

For software that has a STIG or SRG related to Requirements for Least Functionality (such as configuration settings and port access for least functionality), install and configure the software in accordance with that STIG or SRG.

Do not install software that is not specifically required to meet a contract requirement. Remove any previously installed that is not specifically required to meet a contract requirement. Do not implement functionality within software
that is not specifically required to meet contract requirements.

3.7 SYSTEM AND COMMUNICATION PROTECTION

3.7.1 Denial of Service Protection

{For Government Reference Only: This subpart relates to SC-5, SC-12, SC-7(a); CCI-001093, CCI-002385, CCI-002386, CCI-002430, CCI-001097. }

To the greatest extent practical, implement control logic without reliance on the network. Except when required to meet the requirements of the control system Section (where the requirement can only be met using computer hardware), do not implement control logic in computers.

3.8 SAFE MODE AND FAIL SAFE OPERATION

{For Government Reference Only: This subpart (and its subparts) relates to CP-12, SI-10(3), SI-17; CCI-002855, CCI-002856, CCI-002857, CCI-002754, CCI-002773, CCI-002774, CCI-002775}

For all control system components with an applicable STIG or SRG, configure the component in accordance with all applicable STIGs and SRGs.

3.9 SYSTEM MAINTENANCE TOOL SOFTWARE

{For Government Reference Only: This subpart (and its subparts) relates to MA-3; CCI-000865.}

Submit and license to the Government all software required to operate, maintain and modify the control system such the Government or their agents are able to perform repair, replacement, upgrades, and expansions of the system without subsequent or future dependence on the Contractor, Vendor or Manufacturer. Submit hard copies of user manuals for each software with the software submittal. Provide any hardware keys or dongles, software keys, license numbers, and other information required to enable the Government to access or change the system.

For software provided and licensed to the Government under the requirements of another Section, submit a statement indicating the Section and Submittal under which the software was provided. For software provided to meet the requirements of this Section and not provided and licensed under another Section, submit software and software user manuals on DVD or CD as a Technical Data Package and submit one hard copy of the software user manual for each piece of software.

3.10 DEVICE POWER

{For Government Reference Only: This subpart (and its subparts) relates to PE-11, PE-11(1); CCI-002955, CCI-000961. }

For LOW Impact Systems: Provide emergency power in accordance with the control system and equipment specification Sections,

3.11 VULNERABILITY SCANNING

{For Government Reference Only: This subpart (and its subparts) relates to RA-5 RA-5(a),RA-5(b),RA-5(c),RA-5(d); CCI-001054, CCI-001055, CCI-000156, CCI-001641, CCI-001643, CCI-001057, CCI-001058, CCI-001059. }

All IP devices must be scannable, such that the device can be scanned by industry standard IP network scanning utilities without harm to the device, application, or functionality.

3.11.1 Controllers

Provide controllers that are scannable by standard control system discovery tools or control system browsers and return meaningful status information including the network inputs and outputs for the controller. This information must contain sufficient detail to detect vulnerabilities or exploits of the controller.

Provide all software needed to scan the control system as the Control System Scanning Tools submittal. If the software required to scan the system is already installed at the project site or is provided under a separate section instead provide a statement indicating this.

3.12 FIPS 201-2 REQUIREMENT

{For Government Reference Only: This subpart (and its subparts) relates to SA-4 (10); CCI-003116}

Devices in the following systems which implement PIV must be on the NIST FIPS 201-2 approved product list (https://www.idmanagement.gov/approved-products-list/): NONE.

3.13 SYSTEM AND INTEGRATION INTEGRITY

3.14 CONTROL SYSTEM CYBERSECURITY TESTING

3.14.1 Control System Cybersecurity Testing Procedures

Prepare and submit Control System Cybersecurity Testing Procedures explaining step-by-step, the actions and expected results that will demonstrate that the control system meets the requirements of this Section. The Control System Cybersecurity Testing Procedures may be submitted as a Technical Data Package.

3.14.2 Control System Cybersecurity Testing Execution

Using the Control System Cybersecurity Testing Procedures verify that the control system meets the requirements of this Section. UNLESS GOVERNMENT WITNESSING OF A TEST IS SPECIFICALLY WAIVED BY THE GOVERNMENT, PERFORM ALL TESTS WITH A GOVERNMENT WITNESS. If testing reveals deficiencies in the

system, correct the deficiency and retest until successful.

3.14.3 Control System Cybersecurity Testing Report

Prepare and submit a Control System Cybersecurity Testing Report documenting all tests performed and their results. Include all tests in the Control System Cybersecurity Testing Procedures and any additional tests performed during testing. Document test failures and repairs conducted with the test results. The Control System Cybersecurity Testing Report may be submitted as a Technical Data Package

3.15 FIELD QUALITY CONTROL, CYBERSECURITY VALIDATION SUPPORT

In addition to testing and testing support required by other Sections, provide a minimum of 16 hours of technical support for cybersecurity testing of control systems to support the DoD Risk Management Framework process Cybersecurity assessment of the control system. This support is independent of (and in addition to) the Control System Cybersecurity Testing specified in this section.

3.16 CYBERSECURITY TRAINING

Provide eight hours of classroom and hands-on training for six Government personnel on the cybersecurity operation and maintenance of the control system provided. This training is in addition to and must be coordinated with control system training specified in other Sections.

The Government will provide the training location. Training must cover, at a minimum: (a) applying software and firmware updates, (b) user account creation, modification and deletion, (c) audit log upload procedures and (d) identification of privileged user interfaces and system impact of those interfaces. Training session must include a question and answer period during which government staff questions about cybersecurity aspects of the control system are answered.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 05 11.02

CYBERSECURITY FOR FLS FACILITY-RELATED CONTROL SYSTEMS

PART 1 GENERAL

1.1 CONTROL SYSTEM APPLICABILITY
1.2 RELATED REQUIREMENTS
1.3 REFERENCES
1.4 DEFINITIONS
1.4.1 Administrator Account
1.4.2 Computer
1.4.3 Controller
1.4.4 Mission Space
1.4.5 Network
1.4.6 Network Connected
1.4.6.1 Wireless Network Connected
1.4.7 Network Media
1.4.8 User Account Support Levels
1.4.8.1 FULLY Supported
1.4.8.2 MINIMALLY Supported
1.4.8.3 NOT Supported
1.4.9 Manual Local Input
1.4.10 Card Reader
1.4.11 User Interface
1.4.11.1 Local User Interface
1.4.11.2 Remote User Interface
1.4.11.3 Types of User Interface (by capability)
1.4.11.3.1 Read-Only User Interface
1.4.11.3.2 Limited User Interface
1.4.11.3.3 Full User Interface
1.4.11.3.4 View-Only User Interface
1.4.11.4 Other User Interface Terminology
1.4.11.4.1 Writable User Interface
1.4.11.4.2 Privileged User Interface
1.4.12 Wireless Network
1.4.13 Wired Broadcast Network
1.5 ADMINISTRATIVE REQUIREMENTS
1.5.1 Points of Contact
1.5.2 Coordination
1.6 SUBMITTALS
1.7 CYBERSECURITY DOCUMENTATION
1.7.1 Proposed STIG and SRG Applicability Report
1.7.2 Cybersecurity Interconnection Schedule
1.7.3 Network Communication, Ports, Protocols and Services Report
1.7.4 Control System Inventory Reports
1.7.5 Software and Configuration Backups
1.7.6 Cybersecurity Network (Riser) Diagram
1.7.7 STIG, SRG and Vendor Guide Compliance Result Report
1.7.8 Control System Cybersecurity Documentation

1.7.8.1 Default Requirements for Control System Devices
1.8 SOFTWARE LICENSING
1.9 CYBERSECURITY DURING CONSTRUCTION
1.9.1 Contractor Computer Equipment
1.9.1.1 Operating System
1.9.1.2 Anti-Malware Software
1.9.1.3 Passwords and Passphrases
1.9.1.4 User-Based Authentication
1.9.1.5 Demonstration of Compliance
1.9.1.6 Contractor Computer Cybersecurity Compliance Statements
1.9.2 Temporary IP Networks
1.9.2.1 Network Boundaries and Connections
1.9.3 Government Access to Network
1.9.4 Temporary Wireless IP Networks
1.9.5 Passwords and Passphrases
1.9.6 Contractor Temporary Network Cybersecurity Compliance Statements
1.10 CYBERSECURITY DURING WARRANTY PERIOD

PART 2 PRODUCTS

2.1 ETHERNET SWITCH
2.2 DAISY CHAIN IP CONTROLLERS
2.3 DATABASE AND WEB SERVER SOFTWARE FOR MODERATE IMPACT SYSTEMS

PART 3 EXECUTION

3.1 CYBERSECURITY HARDENING AND CONFIGURATION GUIDES
3.2 NETWORK REQUIREMENTS
3.2.1 Wireless and Wired Broadcast Communication for Fire Protection Systems
3.2.2 Non-IP Control Networks
3.2.3 IP Control Networks
3.2.3.1 IP Network Routers
3.2.4 Device Identification and Authentication
3.2.4.1 Default Requirements for Control System Devices
3.2.5 Cryptographic Module Authentication
3.3 ACCESS CONTROL REQUIREMENTS
3.3.1 User Accounts
3.3.1.1 Controllers
3.3.1.1.1 Fire Protection Systems
3.3.1.2 Additional User Account Expiration Requirements In MODERATE Impact Systems:
3.3.1.2.1 For Other Control System Devices FULLY Supporting Accounts
3.3.2 Unsuccessful Logon Attempts
3.3.2.1 Devices MINIMALLY Supporting Accounts
3.3.2.2 Devices FULLY Supporting Accounts
3.3.2.3 High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements
3.3.3 System Use Notification
3.3.3.1 System Use Notification for Remote User Interfaces
3.3.3.2 System Use Notification for Local User Interfaces
3.3.4 Session Lock and Session Termination Requirements In MODERATE Impact Systems:
3.3.4.1 Session Termination
3.3.4.2 Session Lock
3.3.4.3 Session Lock and Termination for Controllers
3.3.4.4 Session Lock and Termination Exceptions

3.3.5 Permitted Actions Without Identification or Authentication
3.3.6 Physical Security in MODERATE Impact Systems
3.3.6.1 Physical Security for Media
3.3.6.1.1 Physical Security for Media Inside Mission Space
3.3.6.1.2 Physical Security for Media Outside Mission Space
3.3.6.1.3 Physical Security for Non-Network Media in Fire Protection Systems
3.3.6.2 Physical Security for Devices
3.3.6.2.1 Physical Security for Devices in Fire Protection Systems
3.3.6.3 Physical Security for User Interfaces
3.3.7 Enclosures
3.4 USER IDENTIFICATION AND AUTHENTICATION
3.4.1 User Identification and Authentication for All System Types
3.4.2 User Identification and Authentication for Specific System Types
3.4.3 User Identification and Authentication for Specific Devices
3.4.4 Implementation of Identification and Authorization Requirements
3.4.5 Password-Based Authentication Requirements
3.4.5.1 Passwords for Controllers FULLY Supporting Accounts
3.4.5.2 Passwords for Remote Interfaces
3.4.5.3 Passwords for Devices Minimally Supporting Accounts
3.4.5.4 Password Configuration and Reporting
3.4.6 Authenticator Feedback
3.5 CYBERSECURITY AUDITING
3.5.1 Audit Events, Content of Audit Records, and Audit Generation
3.5.1.1 Default Requirements for Control System Controllers
3.5.1.1.1 Controllers Which FULLY Support Accounts
3.5.1.1.1.1 Audited Events
3.5.1.1.1.2 Audit Event Information To Record
3.5.1.1.2 Controllers Which Do Not FULLY Support Accounts
3.5.2 Audit Time Stamps
3.5.3 Audit Storage Capacity and Audit Upload
3.5.3.1 Audit Log Storage Notification In MODERATE Impact Systems
3.6 REQUIREMENTS FOR LEAST FUNCTIONALITY
3.6.1 Device Capabilities
3.6.2 Software
3.7 SYSTEM AND COMMUNICATION PROTECTION
3.7.1 Denial of Service Protection and Application Partitioning In MODERATE Impact Systems:
3.7.1.1 Default Requirements for MODERATE Impact Control Systems
3.7.2 Mobile Code In MODERATE Impact Systems:
3.7.3 Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems
3.7.3.1 Radio Interfaces for Fire Protection Systems
3.7.3.2 Fire Suppression System Network Isolation
3.8 SAFE MODE AND FAIL SAFE OPERATION
3.9 SYSTEM MAINTENANCE TOOL SOFTWARE
3.10 DEVICE POWER
3.10.1 Device Behavior on Loss of Power In MODERATE Impact Systems:
3.11 VULNERABILITY SCANNING
3.11.1 Controllers
3.12 FIPS 201-2 REQUIREMENT
3.13 SYSTEM AND INTEGRATION INTEGRITY
3.13.1 Software, Firmware, and Information Integrity In MODERATE Impact Systems:
3.14 CONTROL SYSTEM CYBERSECURITY TESTING
3.14.1 Control System Cybersecurity Testing Procedures
3.14.2 Control System Cybersecurity Testing Execution

3.14.3 Control System Cybersecurity Testing Report
3.15 FIELD QUALITY CONTROL, CYBERSECURITY VALIDATION SUPPORT
3.16 CYBERSECURITY TRAINING

-- End of Section Table of Contents --

SECTION 25 05 11.02

CYBERSECURITY FOR FLS FACILITY-RELATED CONTROL SYSTEMS

PART 1 GENERAL

Many subparts in this Section contain text in curly braces ("{" and "}") indicating which cybersecurity control and control correlation identifier (CCI) the requirements of the subpart relate to. The text inside these curly braces is for Government reference only and enables coordination of the requirements of this Section with the RMF process throughout the design and construction process. Text in curly braces are not contractor requirements.

This Section refers to Security Requirements Guide (SRGs) and Security Technical Implementation Guide (STIGs). STIGs and SRGs are available online at the Information Assurance Support Environment (IASE) website at https://public.cyber.mil/stigs/downloads/ and an SRG/STIG Applicability Guide and Collection Tool is available at https://public.cyber.mil/stigs/SCAP/. Not all control system components have applicable STIGs or SRGs. The "Control Systems SRG" does not apply to work performed under this Section; all requirements within this section to apply applicable SRGs DO NOT include the "Control Systems SRG".

1.1 CONTROL SYSTEM APPLICABILITY

There are multiple versions of this Section associated with this project. Different versions have requirements applicable to different control systems. This specific Section applies only to the following control systems:

UFGS Section Reference	Device	AIR FORCE PIT Level	Network Connectivity & Communication Protocol	Drawing/ Specification Cross-Reference	C-I-A Impact Ratings
21 13 13 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	FACU	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-LOW-LOW

UFGS Section Reference	Device	AIR FORCE PIT Level	Network Connectivity & Communication Protocol	Drawing/ Specification Cross-Reference	C-I-A Impact Ratings
21 13 13 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Pull Station	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-LOW-LOW
21 13 13 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	LED Text Signs	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-LOW-LOW
21 13 13 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Speaker/Strobe	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-LOW-LOW
21 13 13 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Strobe Only	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-LOW-LOW

UFGS Section Reference	Device	AIR FORCE PIT Level	Network Connectivity & Communication Protocol	Drawing/ Specification Cross-Reference	C-I-A Impact Ratings
21 13 13 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Smoke Detection	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-LOW-LOW
21 13 13 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Addressable Input/Output Module	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-LOW-LOW
28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Monaco Radio Communications Interface Card	1A	Serial over EIA 422 pinouts over Standard Copper Cables	FA501 FA502 FA503	LOW-LOW-LOW
21 13 13 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Waterflow Devices	0A	Relay Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-LOW-LOW

1.2 RELATED REQUIREMENTS

This section does not contain sufficient requirements to procure a control system and must be used in conjunction with other Sections which specify control systems. This Section adds cybersecurity requirements to the control systems specified in other Sections, and as these requirements are conditioned on the control system being provided, there may be requirements in this Section that will not apply to this project. All

Sections containing facility-related control systems or control system components are related to the requirements of this Section. Review all specification sections to determine related requirements.

In cases where a requirement is specified in both this Section and in another Section, the more stringent requirement must be met. In cases where a requirement in this Section conflicts with the requirements of another Section such that both requirements cannot be met at the same time, request direction from the Contracting Officer to determine which requirement applies to the project.

1.3 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST FIPS 140-2	(2001) Security Requirements for Cryptographic Modules
NIST FIPS 201-2	(2013) Personal Identity Verification (PIV) of Federal Employees and Contractors

U.S. DEPARTMENT OF DEFENSE (DOD)

DODI 8551.01	(2014) Ports, Protocols, and Services Management (PPSM)
DTM 08-060	(2008) Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement

1.4 DEFINITIONS

1.4.1 Administrator Account

An administrator account is an account with full permissions to a device, application, or operating system, including the ability to create and modify other user accounts.

Note that the operating system Administrator Account may be different than Administrator Accounts for applications hosted on that operating system. Also, most controllers will not have any support for accounts and will therefore not have an 'Administrator Account'.

1.4.2 Computer

A computer is one of the following:

a. a device running a non-embedded desktop or server version of Microsoft Windows

b. a device running a non-embedded version of MacOS

c. a device running a non-embedded version of Linux

d. a device running a version or derivative of the Android Operating

System, where Android is considered separate from Linux

e. a device running a version of Apple iOS

Unless otherwise indicated or clear from context use of the word "device" in this Section includes computers.

1.4.3 Controller

A device other than a computer or Ethernet switch. For Fire Protection systems this includes fire alarm control panels, remote operating consoles, and remote annunciators.

1.4.4 Mission Space

A device or media is in mission space if physical access to the device or media is controlled by the organization served by the device. For example, a variable air volume (VAV) box controller in a suspended ceiling is in mission space if the VAV box serves that room; an electrical switchgear in an electrical room or an air handling unit (AHU) in a mechanical room or on a rooftop may still be considered to be in mission space if the organization (mission) served by that switchgear or AHU controls access to the electrical room, mechanical room or rooftop.

1.4.5 Network

A network is a group of two or more devices that can communicate using a network protocol. Network protocols must provide a method for addressing devices on the network; a communication method that does not provide an addressing scheme is not a networked form of communication. Devices that communicate using a method of communication that does not support device addressing are not using a network. Addresses may be other than IP addresses, and addressing may be at either Open Systems Interconnection (OSI) layer 2 or layer 3.

1.4.6 Network Connected

A component is network connected (or "connected to a network") only when the device has a network transceiver which is directly connected to the network and implements the network protocol. A device lacking a network transceiver (and accompanying protocol implementation) can never be considered network connected. Note that (unlike many IT definitions of "Network Connected") a device connected to a non-IP network is still considered network connected (an IP connection or IP address is not required for a device to be network connected).

1.4.6.1 Wireless Network Connected

Any device that supports wireless network communication is network connected to a wireless network, regardless of whether the device is communicating using wireless. Unless physically disabled, devices with wireless transceivers support wireless, it is not sufficient to disable the wireless in software.

1.4.7 Network Media

The thing that provides the communication channel between the devices on a network. Typically wire, but might include wireless, fiber optic, or even power line (some network protocols allow sending network signals over

power wiring).

1.4.8 User Account Support Levels

The support for user accounts is categorized in this Section as one of three levels:

1.4.8.1 FULLY Supported

Device supports configurable individual accounts. Accounts can be created, deleted, modified, etc. Privileges can be assigned to accounts. These devices support user-based (as opposed to role-based) authentication.

1.4.8.2 MINIMALLY Supported

Device supports a small, fixed number of accounts (perhaps only one). Accounts cannot be modified. A device with only a "User" and an "Administrator" account would fit this category. Similarly, a device with two PINs for logon - one for restricted and one for unrestricted rights would fit here (in other words, the accounts do not have to be the traditional "username and password" structure). These devices typically only support role-based authentication.

Examples of devices which MINIMALLY support accounts are a) a variable frequency drive with a single account which requires a PIN for access to configuration; and b) a room lighting control touchpad interface that has a single account.

1.4.8.3 NOT Supported

Device does not support any Access Enforcement therefore the whole concept of "account" is meaningless.

1.4.9 Manual Local Input

Manual Local Inputs are system analog or binary inputs that are adjustable by a person but are, by intrinsic hardware design, very limited in potential capabilities. Manual Local Inputs do not have touch screens or full keyboards, but may have a few buttons or dials to allow input. Manual Local Inputs do not have full graphic screens or dot-matrix displays, but may have simple lights (LEDs) or 7-segment displays. Manual Local Inputs do not have any sort of menu structure, each button has a single well-defined function.

Examples of Manual Local Inputs are H-O-A switches, simple thermostats, and disconnect switches.

1.4.10 Card Reader

A card reader is an input/output device whose primary function is to assist in two-factor authentication. A card reader must have an interface to read data from a card and may be able to write data to a card. A card reader may have a means (such as buttons, keypad, touchscreen, etc.) for a user to input a PIN or password, as well as a limited display.

1.4.11 User Interface

A User Interface (UI) is something other than a Manual Local Input or Card Reader that allows a person to interact with the system or device. Note

that while a Card Reader is not by itself a User Interface, a User Interface may contain a Card Reader in order for it to authenticate its user. Within control systems, there are a wide range of User Interfaces.

Two important distinctions are 1) whether the user interface is Local or Remote, and 2) the effective capabilities of the User Interface to alter data, which is the "privilege" of the user interface (where effective privilege available to a specific user at a specific user interface is the combination of the greatest privilege offered by the user interface and the specific account the user is logged into).

1.4.11.1 Local User Interface

A Local User Interface is a user interface where the physical hardware the user interacts with (keyboard, buttons, display, etc.) is physically part of the device being affected. All of the relevant characteristics of the user interface are embodied within a single device.

Note that a Local UI may be able to access data in a different device, Local versus Remote in this context refers to the user interface itself; the capability to access data in a different device is covered under "Full User Interface".

1.4.11.2 Remote User Interface

A Remote User Interface implements a Client/Server model where the physical hardware the user interacts with (Client) is physically distinct from the device being affected (Server). Most or all of the security and functionality characteristics of the user interface are defined by the Server, not the Client. The Client and Server communicate via a network connection. A common example of a remote user interface is a web-based interface where the browser (client) is generally on different hardware than the web server (server). A Remote UI remains a Remote UI even if the user happens to be at a Client on the same hardware as the Server. What is important is that a) the Client may be on different hardware than the Server and b) the majority of the security and functional characteristics of the interface are defined at the Server.

Note that this definition of "remote" is consistent with that generally used in the control industry but is not aligned with the NIST 800-53 definition of "Remote", which refers to "outside the system". The term "Remote" here better aligns with the NIST 800-53 definition of "Network" (remote from within the system) Access.

1.4.11.3 Types of User Interface (by capability)

User interfaces are also categorized by their capabilities as being Read Only, Limited, or Full.

1.4.11.3.1 Read-Only User Interface

A Read Only User Interface (also referred to as a View-Only User Interface) is a user interface that only allows for reading data, it does not allow (have the capability to) modify data. A Read Only User Interface may be either Local or Remote. A User Interface that is configured to be Read Only (by some other means than the interface itself, such as using configuration software on a laptop) is a Read-Only Interface. Note a Read Only User Interface may have buttons (or touch screen, etc.) allowing the user to navigate through the presentation of

data.

Examples of a Read Only User Interfaces are a) a publicly viewable "energy dashboard" showing weather data and energy usage within a building and b) digital wayfinding signage.

1.4.11.3.2 Limited User Interface

A Limited User Interface is a user interface that - by design - can only alter information local to the user interface. Note that the determination of "alter" includes only direct interactions, it explicitly excludes interactions that might occur as secondary effects. For example, an interface changing the flow setpoint in a pump controller is a direct interaction, the subsequent change in flow (as well as any subsequent downstream changes in valve position) are not direct interactions.

Two examples of LIMITED UIs are: a) a variable speed drive has a Limited Local User Interface which allows the user to change properties within the drive, but does not allow affecting things outside the drive; and b) a typical home WiFi Router has a Limited Remote User Interface which allows configuration of the Router, but does not allow direct interaction with other devices.

1.4.11.3.3 Full User Interface

A Full User Interface can alter information in devices outside the device with the user interface. For example, a typical Local Display Panel is a Full Local User Interface while a browser-based front end is a Full Remote User Interface.

1.4.11.3.4 View-Only User Interface

See Read-Only User Interface

1.4.11.4 Other User Interface Terminology

In addition to defining whether a user interface is a Hardware Limited, Read-Only, Limited or Full, and whether it is Local or Remote, user interfaces are classified by whether they are writable or privileged.

1.4.11.4.1 Writable User Interface

Any User Interface that is not Read-Only is Writable. (Limited User Interfaces and Full User Interfaces are both writable user interfaces (as they are capable of changing a value)).

1.4.11.4.2 Privileged User Interface

A Privileged UI is a UI that has sufficient capabilities or functionality that it requires specific cybersecurity measures to be put in place to limit its unauthorized use. Ultimately, whether a specific user interface is considered a Privileged User Interface must be determined by usage. Unless otherwise specified, user interfaces can be determined to be privileged or not using the following:

a. Read-Only User Interfaces are not privileged user interfaces.

b. User Interfaces that can inhibit or force the activation of a fire suppression system (e.g. such as for a pre-action or deluge system)

are always privileged user interfaces. Other Full User interfaces for Fire Alarm Systems are privileged user interfaces as indicated and shown, or when another requirement of this Section establishes they are privileged. For all other systems, Full User Interfaces are privileged user interfaces.

c. User interfaces that allow for configuration of auditing or allows for modification or deletion of audit logs are privileged user interface.

d. User interfaces that allow for reprogramming a network connected device is a privileged user interface.

e. Except as specified above, a Limited User Interface must be determined to be privileged or not based on the specific capabilities and use case of the user interface. In general however, user interfaces that do not offer significant capabilities above and beyond those available at that location via other means (e.g. such as a disconnect switch, breaker, or hand-off-auto switch, or physical attack) are not privileged.

1.4.12 Wireless Network

Any network that communicates without using wires or fiber optics as the communication media. Wireless networks include: WiFi, Bluetooth, ZigBee, cellular, satellite, long and short wave radio, 2.4 GHz, free space optical, point-to-point laser, microwave, and IR.

1.4.13 Wired Broadcast Network

Wired Broadcast Networks are any network, such as powerline carrier networks and modem (wired telephony), that use wire-based technologies where there is not a clearly defined boundary for signal propagation.

1.5 ADMINISTRATIVE REQUIREMENTS

1.5.1 Points of Contact

Coordinate with the following Points of Contact as indicated in this Section and as required. Not all projects will require coordination with all Points of Contact. When coordination is required and no Point of Contact is indicated, coordinate with the Contracting Officer (KO).

a. Government Computer Access Point of Contact: Contracting Office (KO)

b. HTTPS Certificate Point of Contact: Contracting Officer (KO)

c. Email Address Point of Contact: Contracting Officer (KO)

d. Password Point of Contact: Contracting Officer (KO)

e. Mobile Code Point of Contact: Contracting Officer (KO)

1.5.2 Coordination

Coordinate the execution of this Section with the execution of all other Sections related to control systems as indicated in the paragraph RELATED REQUIREMENTS. Items that must be considered when coordinating project efforts include but are not limited to:

a. If requesting permission for wireless or wired broadcast communication, the Wireless and Wired Broadcast Communication Request submittal must be approved prior to control system device selection and installation.

b. If requesting permission for alternate account lock permissions, the Device Account Lock Exception Request must be approved prior to control system device selection and installation.

c. If requesting permission for the use of a device with multiple physical connections to IP networks, the Multiple IP Connection Device Request must be approved prior to control system device selection and installation.

d. Wireless testing may be required as part of the control system testing. See requirements for the Wireless Communication Test Report submittal.

e. If the Device Audit Record Upload Software is to be installed on a computer not being provided as part of the control system, coordination is required to identify the computer on which to install the software.

f. The Cybersecurity Interconnection Schedule must be coordinated with other work that will be interconnected to, and interconnections must be approved by the Government before relying on them for system functionality.

g. Cybersecurity testing support must be coordinated across control systems and with the Government cybersecurity testing schedule.

h. Passwords must be coordinated with the indicated contact for the project site.

i. If applicable, HTTPS web server certificates must be obtained from the indicated HTTPS Certificate Point of Contact.

j. Contractor Computer Cybersecurity Compliance Statements must be provided for each contractor using contractor owned computers.

1.6 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Device Account Lock Exception Request; G

Contractor Computer Cybersecurity Compliance Statements; G

Contractor Temporary Network Cybersecurity Compliance Statements; G

Cybersecurity Interconnection Schedule; G

Proposed STIG and SRG Applicability Report; G

Pre-Construction Control System Inventory Report; G

SD-02 Shop Drawings

Network Communication, Ports, Protocols and Services Report; G

Cybersecurity Network (Riser) Diagram; G

SD-03 Product Data

Control System Cybersecurity Documentation; G

SD-06 Test Reports

Control System Cybersecurity Testing Procedures; G

Control System Cybersecurity Testing Report; G

SD-07 Certificates

Software Licenses; G

SD-11 Closeout Submittals

Confidential Password Report; G

Enclosure Keys; G

Software and Configuration Backups; G

System Maintenance Tool Software; G

Control System Scanning Tools; G

STIG, SRG and Vendor Guide Compliance Result Report; G

Final Control System Inventory Report; G

Integrity Verification Software; G

1.7 CYBERSECURITY DOCUMENTATION

{For Government Reference Only: This subpart (and its subparts) relates to PL-7; CCI-003071}

1.7.1 Proposed STIG and SRG Applicability Report

For each model of network connected or network infrastructure device, use the DISA SRG/STIG Applicability Guide and Collection Tool (available at https://public.cyber.mil/stigs/SCAP/to identify applicable STIGs or SRGs and provide a report indicating applicable STIGs and SRGs for each model. Provide the Proposed STIG and SRG Applicability Report concurrently with the Pre-Construction Control System Inventory Report.

1.7.2 Cybersecurity Interconnection Schedule

{For Government Reference Only: This subpart relates to CA-3(b), PL-8, SC-7(9), SC-7(11); CCI-000258, CCI-003072, CCI-003073, CCI-003075, CCI-002398, CCI-002399, CCI-002401, CCI-002402, CCI-002403. For MODERATE

Impact systems, this subpart also relates to SC-7; CCI-001126, CCI-001109}

Provide a completed Cybersecurity Interconnection Schedule documenting network connections between the installed system and other systems. Provide the following information for each device directly communicating between systems: Device Identifier, Device Manufacturer, Device Description, Transport layer Protocol, Network Address, Port (if applicable), MAC (Layer 2) address (if applicable), Media, Application Protocol, Service (if applicable), Descriptive Purpose of communication. For communication with other authorized systems also provide the Foreign Destination and POC for Destination. For MODERATE Impact Systems: Also describe the impact of loss of the connection on the control system. If other control system Sections used on this project include submittals documenting this information, provide copies of those submittals to meet this requirement.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Cybersecurity Interconnection Schedule as an editable Microsoft Excel file (a template Cybersecurity Interconnection Schedule in Excel format is available at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-1

1.7.3 Network Communication, Ports, Protocols and Services Report

{For Government Reference Only: This subpart (and its subparts) relates to CA-9, PL-8; CCI-002102, CCI-002103, CCI-002104, CCI-002105, CCI-003072, CCI-003073, CCI-003075 and also the submittal requirements associated with CM-6, CM-7, including CM-7(3), CCI-000388.}

Provide a Network Communication, Ports, Protocols and Services Report. For each networked device, document device identifier and the communication characteristics of the device including communication protocols, services used, encryption employed, and a general description of what information is communicated over the network. For each device using IP communication, document all TCP and UDP ports used. For each device using non-IP communication, document communication protocol and media used. If other control system Sections used on this project include submittals documenting this information, provide copies of those submittals to meet this requirement.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Network Communication, Ports, Protocols and Services Report as an editable Microsoft Excel file.

1.7.4 Control System Inventory Reports

{For Government Reference Only: This subpart (and its subparts) relates to CM-8(a), SI-17, IA-3; CCI-000389, CCI-000392, CCI-000398, CCI-002773, CCI-002774, CCI-002775, CCI-000777, CCI-000778, CCI-001958}

Provide a Pre-Construction Control System Inventory Report report and a Final Control System Inventory Report, using the Inventory Spreadsheet listed under this Section at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-1 In the Control System Inventory Reports, document all networked devices, including network infrastructure devices. For each device provide all applicable information for which there is a field on the spreadsheet in accordance with the instructions on the spreadsheet.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Control System Inventory Reports as editable Microsoft Excel files. Provide the Pre-Construction Control System Inventory Report concurrently with the Proposed STIG and SRG Applicability Report

1.7.5 Software and Configuration Backups

{For Government Reference Only: This subpart (and its subparts) relates to CP-10; CCI-000550, CCI-000551, CCI-000552}

For all controllers, provide a backup of the controller configuration and the source code for all loaded application programs (all software that is not common to every controller of the same manufacturer and model).

If any or all of these are provided under another Section, provide documentation indicating this and referencing those submittals.

1.7.6 Cybersecurity Network (Riser) Diagram

{For Government Reference Only: This subpart (and its subparts) relates to PL-2(a), PL-8; CCI-003051, CCI-003053, CCI-003072, CCI-003073, CCI-003075}

Provide a cybersecurity network (riser) diagram of the complete control system including all network and device hardware. For each device, include the device identifier, device type, and manufacturer. If the control system specifications require a riser diagram submittal, provide a copy of that submittal as the cybersecurity riser diagram. Otherwise, provide a riser diagram in one-line format overlayed on a facility schematic.

1.7.7 STIG, SRG and Vendor Guide Compliance Result Report

For every component (device or software) with an applicable STIG or SRG in the Proposed STIG and SRG Applicability Report, document compliance with the STIG or SRG requirements.

a. For components which are scannable by the Evaluate-STIG tool (available online at (CAC Required), include the Evaluate-STIG report and raw scan results in addition to the final, manually reviewed and revised, documentation of compliance with STIG and SRG requirements. Checklist files should not contain any findings with a Not Reviewed (NR) status after manual reviews.

b. For components which do not support automated scanning, a manual review using the General Purpose STIG option should be done. A completed Checklist file should not contain any findings with a Not Reviewed (NR) status after manual reviews

For every component (device or software) with manufacturer provided cybersecurity documentation, procedure, or method for secure configuration or installation, provide a report documenting how the component was configured and any deviation from the manufacturer instructions.

1.7.8 Control System Cybersecurity Documentation

{For Government Reference Only: This subpart (and its subparts) relates

to SA-5(a),SA-5(b),SA-5(c), SA-22(b); CCIs: CCI-003124, CCI-003125, CCI-003126, CCI-003127, CCI-003128, CCI-003129, CCI-003130, CCI-003131, CCI-003374}

Provide a Control System Cybersecurity Documentation submittal containing the indicated information for each device and software application.

1.7.8.1 Default Requirements for Control System Devices

For control system devices where Control System Cybersecurity Documentation requirements are not otherwise indicated in this Section, provide:

a. Documentation that describes secure configuration of the device {For Government Reference Only: relates to CCI-003124}

b. Documentation that describes secure installation of the device {For Government Reference Only: relates to CCI-003125}

c. Documentation that describes secure operation of the device {For Government Reference Only: relates to CCI-003124}

d. Documentation that describes effective use and maintenance of security functions or mechanisms for the device {For Government Reference Only: relates to CCI-003127}

e. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device {For Government Reference Only: relates to CCI-003128}

f. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms {For Government Reference Only: relates to CCI-003129}

g. Documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

h. Documentation that describes user responsibilities in maintaining the security of the device {For Government Reference Only: relates to CCI-003131}

i. Documentation of the published last date of support by the manufacturer or indication that a published date is not available. {For Government Reference Only: relates to CCI-003374}

1.8 SOFTWARE LICENSING

{For Government Reference Only: This subpart (and its subparts) relates to SI-2(a), SI-2(c), SI-7(14); CCI-001227, CCI-002605, CCI-002737}

For all software provided that has not already been licensed to the government or project site, provide a license to the Government for a period of no less than 5 years, and the license must also include the following software updates:

a. Security and bug-fix patches issued by the software manufacturer.

b. Security patches to address any vulnerability identified in the National Vulnerability Database at http://nvd.nist.gov with a Common Vulnerability Scoring System (CVSS) severity rating of MEDIUM or higher.

Provide a single Software Licenses submittal with documentation of the software licenses for all software provided

1.9 CYBERSECURITY DURING CONSTRUCTION

{For Government Reference Only: This subpart (and its subparts) relates to AC-18, CA-3; CCI-000258}

In addition to the control system cybersecurity requirements indicated in this section, meet following requirement throughout the construction process.

1.9.1 Contractor Computer Equipment

Contractor owned computers may be used for construction. Contractor computers connected to the control system, control system network, or a control system component at any point during construction must meet the following requirements:

1.9.1.1 Operating System

The operating system must be an operating system currently supported by the manufacturer of the operating system. The operating system must be current on security patches and operating system manufacturer required updates.

1.9.1.2 Anti-Malware Software

The computer must run anti-malware software from a reputable software manufacturer. Anti-malware software must be a version currently supported by the software manufacturer, must be current on all patches and updates, and must use the latest definitions file. Computers used on this project must perform a full antivirus scan at least once per day. Computers which have connected to any other network since the last full antivirus scan must perform a full antivirus scan prior to connection to the control system network or to the temporary contractor-installed IP network. Perform an antivirus scan on all removable media (e.g., external hard drives, CDs, DVDs, USB flash drives) prior to connecting to the control system environment.

1.9.1.3 Passwords and Passphrases

The passwords and passphrases for computers, applications, and web-based applications supporting passwords must be changed from their default values. Passwords must be a minimum of eight characters with a minimum of one uppercase letter, one lowercase letter, one number and one special character.

1.9.1.4 User-Based Authentication

Each user must have a unique account; sharing of a single account between multiple users is prohibited.

1.9.1.5 Demonstration of Compliance

The Government has the right to require demonstration of computer compliance with these requirements at any time during the project.

1.9.1.6 Contractor Computer Cybersecurity Compliance Statements

Provide a single submittal containing completed Contractor Computer Cybersecurity Compliance Statements for each company using contractor owned computers. Contractor Computer Cybersecurity Compliance Statements must use the template published at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-1 Each Statement must be signed by a cybersecurity representative for the relevant company.

1.9.2 Temporary IP Networks

Temporary contractor-installed IP networks may be used during construction. When used, temporary contractor-installed IP networks connected to the control system, control system network, or a control system component at any point during construction must meet the following requirements:

1.9.2.1 Network Boundaries and Connections

The network must not extend outside the project site and must not connect to any IP network other than those specifically provided or furnished for this project. Any and all access to the network from outside the project site is prohibited.

1.9.3 Government Access to Network

Government personnel must be allowed to have complete and immediate access to the network at any time in order to verify compliance with this specification.

1.9.4 Temporary Wireless IP Networks

In addition to the other requirements on temporary IP networks, temporary wireless IP (WiFi) networks, when permitted, must not interfere with existing wireless networks, must use WPA2 security and must not broadcast the network name (SSID). Network names (SSID) for wireless networks must be changed from their default values.

1.9.5 Passwords and Passphrases

The passwords and passphrases for all network devices and network access must be changed from their default values. Passwords must be a minimum 8 characters with a minimum of one uppercase letter, one lowercase letter, one number and one special character.

1.9.6 Contractor Temporary Network Cybersecurity Compliance Statements

Provide a single submittal containing completed Contractor Temporary Network Cybersecurity Compliance Statements for each company implementing a temporary IP network. Contractor Temporary Network Cybersecurity Compliance Statements must use the template published at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-1

Each Statement must be signed by a cybersecurity representative for the relevant company. If no temporary IP networks will be used, provide a single copy of the Statement indicating this.

1.10 CYBERSECURITY DURING WARRANTY PERIOD

All work performed on the control system after acceptance must be performed using Government Furnished Equipment or equipment specifically and individually approved by the Government.

PART 2 PRODUCTS

All products used on this project must meet the indicated requirements, but not all products specified here will be required by every project.

2.1 ETHERNET SWITCH

Not Applicable

2.2 DAISY CHAIN IP CONTROLLERS

Not Applicable

2.3 DATABASE AND WEB SERVER SOFTWARE FOR MODERATE IMPACT SYSTEMS

Not Applicable

PART 3 EXECUTION

3.1 CYBERSECURITY HARDENING AND CONFIGURATION GUIDES

Install, configure, and harden all hardware and software furnished on this project in accordance with manufacturer provided documentation, procedures, or methods for secure configuration or installation. Do not implement specific hardening actions if that action would conflict with required functionality or another requirement of this Section.

3.2 NETWORK REQUIREMENTS

3.2.1 Wireless and Wired Broadcast Communication for Fire Protection Systems

The use of wireless and wired broadcast communication for fire protection systems within a facility is prohibited. Wireless communication may be used to provide communication from the fire protection system in a facility to the central monitoring station.

3.2.2 Non-IP Control Networks

When control system specifications require particular communication protocols, use only those communication protocols and only as specified. Do not implement any other communication protocol.

When control system specifications do not indicate requirements for communication protocols, use only those protocols required for operation of the system as specified.

3.2.3 IP Control Networks

{For Government Reference Only: This subpart relates to CM-6(a), CM-7(a), CM-7(b), CM-7(1)(b), SC-41; CCI-001588, CCI-000381, CCI-000380, CCI-000381, CCI-000382, CCI-001761, CCI-001762, CCI-002544, CCI-002545, CCI-002546. For Moderate Impact Systems, this subpart (and its subparts) also relates to SC-5(1), SC-5(2); CCI-001094 CCI-001095}

IP Networks must be Ethernet networks and must use switches which are Ethernet Switches or Daisy Chain IP Controllers as defined in this Section. Do not use nonsecure functions, ports, protocols and services as defined in DODI 8551.01 unless those ports, protocols and services are specifically required by the control system specifications or otherwise specifically authorized by the Government. Do not use ports, protocols and services that are not specified in the control system specifications or required for operation of the control system.

For MODERATE Impact Systems, unless explicitly authorized, do not use IP networks if the same control functionality is available through the use of non-IP networks.

3.2.3.1 IP Network Routers

Do not install any device that performs IP routing.

3.2.4 Device Identification and Authentication

{For Government Reference Only: This subpart (and its subparts) relates to IA-3; CCI-000777, CCI-000778, CCI-001958. For MODERATE Impact systems, this subpart (and its subparts) also relates to SC-23, SC-23(5); CCI-001184, CCI-002470.}

3.2.4.1 Default Requirements for Control System Devices

For control system devices where Device Identification and Authentication requirements are not otherwise indicated in this Section: Devices using HTTP as a control protocol must use HTTPS instead.

3.2.5 Cryptographic Module Authentication

{For Government Reference Only: This subpart (and its subparts) relates to IA-7; CCI-000803}

For devices (including but not limited to NIST FIPS 140-2 compliant radios) that have STIG/SRGs related to cryptographic module authentication (CCI-000803), comply with the requirements of those STIG/SRGs.

3.3 ACCESS CONTROL REQUIREMENTS

3.3.1 User Accounts

{For Government Reference Only: This subpart (and its subparts) relate to AC-2(a), AC-3, AC-6(1), AC-6(10), AC-6(2), AC-6(9), CM-11(2), and IA-2; CCI-002110, CCI-000213, CCI-001558, CCI-002221, CCI-002222, CCI-002223, CCI-002235, CCI-000039, CCI-001419, CCI-002234, CCI-001812, and CCI-000764. For MODERATE Impact systems, this subpart (and its subparts) also relate to AC-2 (2), AC-2(3), AC-2(4), AC-6(1), and CM-5(1); CCI-001361, CCI-000017, CCI-000217, CCI-000018, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-001683, CCI-001684, CCI-001685, CCI-001686, CCI-002132,

CCI-001558, CCI-002221, CCI-002222, CCI-002223, CCI-001813.}

Any user interface supporting user accounts (either FULLY or MINIMALLY) must limit access according to specified limitations for each account. Install and configure any device having a STIG or SRG in accordance with that STIG or SRG.

All user interfaces FULLY supporting accounts must implement user-based authentication where each account is uniquely assigned to a specific user. User interfaces FULLY supporting accounts must implement at least three (3) levels of user account privilege including: 1) an account with read-only permissions 2) an account with full permissions including account creation and modification and 3) an account with greater permissions than read-only but without account creation and modification. Disable any unnecessary or unused accounts. Disable any "guest-level" accounts that are created on the system by default.

3.3.1.1 Controllers

For user interfaces provided by controllers, provide access control in accordance with the User Interface Requirements table for the applicable control system and user interface type.

a. For table entries of "NA": NA means Not Applicable, there are no interfaces in this category.

b. For table entries of "None Required": The user interface is not required to support user accounts.

c. For table entries of "MINIMALLY": The user interface must at least MINIMALLY support user accounts.

d. For table entries of "FULLY": The user interface must at FULLY support user accounts.

e. For table entries of "KEY": The user interface must have physical security in the form of either a key lock on the interface itself or be furnished inside a lockable enclosure. Where this is required for a read only interface, the lockable enclosure must prevent viewing of data on the interface; for other interfaces, this lockable enclosure must prevent using the interface to alter data.

f. For table entries of "Physical Security": For Local FULL interfaces, the interface must be located inside mission space. For Local Limited (not FULL) interfaces, the user interface must either a) be located within mission space or b) be protected by physical security at least as good as the control devices (and equipment controlled by the control devices) affected by the interface. For purposes of this requirement, 'affected' includes controllers with data that can be directly altered by the interface, as well as mechanical and/or electrical equipment directly controlled by those controllers, but does not include other interactions.

g. Entries of the form "X and Y" must meet both the requirement indicated for X and the requirement indicated for Y. For example, an entry of "MINIMALLY and Physical Security" indicates the user interface must both MINIMALLY support accounts and have physical security.

h. Entries of the form "X or Y" must meet either the requirement

indicated for X or the requirement indicated for Y.

3.3.1.1.1 Fire Protection Systems

User Interface Requirements for MODERATE Impact Fire Protection Systems	
User Interface Type	**Access Control Requirement** (See note 2)
Local Read Only	None Required
Local Limited, Non-privileged	KEY or MINIMALLY
Local Limited, Privileged	FULLY
Local Full	KEY
Remote Read Only	MINIMALLY
Remote Limited, Non-Privileged	FULLY
Remote Limited, Privileged AND Remote Full	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Devices outside mission space require physical security protections as indicated (in "PHYSICAL SECURITY IN MODERATE IMPACT SYSTEMS")	

3.3.1.2 Additional User Account Expiration Requirements In MODERATE Impact Systems:

In addition to other user account requirements, user account expiration and auditing must be configured as indicated.

3.3.1.2.1 For Other Control System Devices FULLY Supporting Accounts

If temporary accounts are supported, expire temporary accounts 72 hours after creation. Expire all other accounts after 365 days of inactivity.

3.3.2 Unsuccessful Logon Attempts

{For Government Reference Only: This subpart (and its subparts) relate to AC-7 (a), AC-7 (b); CCI-000043, CCI-000044, CCI-001423, CCI-002236, CCI-002237, CCI-002238}

Except for high availability user interfaces indicated as exempt, devices must meet the indicated requirements for handling unsuccessful logon attempts. If a device cannot meet these requirements, document device capabilities to protect from subsequent logon attempts and propose alternate protections in a Device Account Lock Exception Request submittal. Do not implement alternate protection measures in lieu of the indicated requirements without explicit permission from the Government. If no Device Account Lock Exceptions are requested, provide a document stating that no approval is being requested as the Device Account Lock Exception Request.

3.3.2.1 Devices MINIMALLY Supporting Accounts

For MODERATE Impact Systems: Devices which MINIMALLY (but not FULLY) support accounts must lock the user accountafter five consecutive failed login attempts and must unlock the user account after 60 minutes have elapsed without an unsuccessful login attempt or by a successful login to a separate administrator account.

3.3.2.2 Devices FULLY Supporting Accounts

Devices which FULLY support accounts must meet the following requirements.

a. It must lock the user account when three unsuccessful logon attempts occur within a 15 minute interval.

b. Once an account is locked, the account must stay locked until unlocked by an administrator. If the account being locked is the sole administrator account on the device, the account must stay locked for 1 hour and then automatically unlock.

c. Once the indicated number of unsuccessful logon attempts occurs, delay further logon prompts by 5 seconds.

3.3.2.3 High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements

There are no high availability interfaces which are exempt from unsuccessful logon attempts requirements.

3.3.3 System Use Notification

{For Government Reference Only: This subpart (and its subparts) relates to AC-8; CCI-000048, CCI-002247, CCI-002243, CCI-002244, CCI-002245, CCI-002246, CCI-000050, CCI-002248}

3.3.3.1 System Use Notification for Remote User Interfaces

Remote user interfaces must display a warning banner meeting the requirements of DTM 08-060 on screen.

3.3.3.2 System Use Notification for Local User Interfaces

Devices which are connected to a network and have a local user interface must display a warning banner meeting the requirements of DTM 08-060 on the user interface screen if capable of doing so and must have a permanently affixed label with an approved banner from DTM 08-060 if unable to display the warning banner on the screen. Where it is impractical (perhaps due to device size) to affix the label to the device, affix the label to the device enclosure.

Labels must be machine printed or engraved, plastic or metal, designed for permanent installation, must use a font no smaller than 14 point, and must provide a high contrast between font and background colors.

3.3.4 Session Lock and Session Termination Requirements In MODERATE Impact Systems:

{For Government Reference Only: This subpart (and its subparts) relates to AC-11(a), AC-11(b), AC-11(1), AC-12, SC-10; AC-10; CCI-000058, CCI-000059, CCI-000056, CCI-000057, CCI-000060, CCI-002360, CCI-002361, CCI-001133, CCI-001134, CCI-000054, CCI-000055, CCI-002252}

3.3.4.1 Session Termination

When session termination is required for a User Interface, the User Interface must implement session termination a) based on manual initiation, or b) based on lack of activity, or c) based on either manual initiation or lack of activity, as indicated.

Session Termination must result in logging out the user. A logged out User Interface may only perform actions as indicated in the "Permitted Actions Without Identification or Authentication" subpart of this Section or display a publicly viewable image or blank screen. User Interfaces must remain logged out (session terminated) until a user enters correct authentication information, which must initiate a new session. All User Interfaces running on computers and all Remote User Interfaces must also terminate network connections as part of session termination.

3.3.4.2 Session Lock

When session lock is required for a User Interface, the User Interface must implement session lock a) based on manual initiation, or b) based on lack of activity, or c) based on either manual initiation or lack of activity, as indicated.

Session lock must result in the User Interface being suspended and the user interface must display a publicly viewable image or blank screen. No interaction with the user interface must be possible until either a) the same user enters valid authentication information, in which case that session must be continued, or b) until a different user enters valid authentication information at which point the first session must be terminated and a new session initiated for the new user.

3.3.4.3 Session Lock and Termination for Controllers

Except as shown in the Session Lock and Session Termination Exception Table, Writable Remote User Interfaces must support requirements for Session Termination, and must both be capable of being initiated by the user and initiated by lack of activity. Session Termination must initiate after 30 minutes of inactivity.

Except as shown in the Session Lock and Session Termination Exception Table, Local User Interfaces supporting accounts must support manual initiation of Session Termination. Privileged Local User Interfaces must also support timed initiation of Session Termination, unless otherwise indicated in the Session Lock and Termination Exceptions table, with Session Termination initiated at 30 minutes of inactivity.

3.3.4.4 Session Lock and Termination Exceptions

Table: Session Lock and Termination Exceptions

Device	Location	Session Lock and Termination Requirements for Device (or "none" to indicate session lock or session termination is not required)
FACU	TBD	Return to user logon screen

3.3.5 Permitted Actions Without Identification or Authentication

{For Government Reference Only: This subpart (and its subparts) relates to AC-14; CCI-000061, CCI-000232}

The control system must require identification and authentication before allowing any actions except read-only actions by a user acting from a user interface which MINIMALLY or FULLY supports accounts.

3.3.6 Physical Security in MODERATE Impact Systems

{For Government Reference Only: This subpart relates to PE-3(1), PE-4, PE-5, SC-7(a), SC-7(c), SC-8, SC-8(1); CCI-000928, CCI-002926, CCI-000936, CCI-002930, CCI-002931, CCI-000937, CCI-001097, CCI-001109, CCI-002418, CCI-002419, CCI-002421.}

3.3.6.1 Physical Security for Media

3.3.6.1.1 Physical Security for Media Inside Mission Space

Install all non-IP network media located inside of the mission space in conduit. Install all IP network media located inside of the mission space in intermediate metallic conduit.

3.3.6.1.2 Physical Security for Media Outside Mission Space

Install all network media (both IP and non-IP) located outside of the mission space in rigid metallic conduit.

3.3.6.1.3 Physical Security for Non-Network Media in Fire Protection Systems

For Fire Suppression Systems which can be inhibited or forced to activate by manipulation of non-network wiring, install all non-network media outside of mission space, including analog and binary instrumentation wiring and power wiring, in rigid metallic conduit.

3.3.6.2 Physical Security for Devices

Install all devices (computers and controllers) which are located outside of mission space in lockable enclosures. (Recall that per definition of mission space, a room controlled by the mission is mission space regardless of whether it is contiguous with other mission space.)

Install all controllers connected to an IP network in lockable enclosures (both inside and outside of mission space).

3.3.6.2.1 Physical Security for Devices in Fire Protection Systems

For Fire Suppression systems with a release panel, install all components of the suppression system either inside mission space, or within locked enclosures. Components of these systems include: release panel, any relay or interface panels, analog and binary inputs or outputs, control valves, manual valves.

3.3.6.3 Physical Security for User Interfaces

Physical security requirements for User Interfaces are specified in the preceding paragraphs of this Section.

3.3.7 Enclosures

Prior to final acceptance of the system, lock all lockable enclosures. Submit an Enclosure Keys submittal with all copies of keys for all enclosures and a key inventory list documenting all keys. Label each key with the matching enclosure identifier.

3.4 USER IDENTIFICATION AND AUTHENTICATION

{For Government Reference Only: This subpart (and its subparts) relates to IA-2, IA-2(1),IA-2(12), IA-5 IA-5(b), IA-5(c), IA-5(e), IA-5(g), IA-5(1), IA-5(11); CCI-000764, CCI-000765, CCI-001953, CCI-001954, CCI-001544, CCI-001989, CCI-000182, CCI-001610, CCI-000192, CCI-000193, CCI-000194, CCI-000205, CCI-001619, CCI-001611, CCI-001612, CCI-001613, CCI-001614, CCI-000195, CCI-001615, CCI-000196, CCI-000197, CCI-000199, CCI-000198, CCI-001616, CCI-001617, CCI-000200, CCI-001618, CCI-002041, CCI-002002, CCI-002003. For MODERATE Impact systems, this subpart also relates to AC-6 (1), AC-6(10), AC-6(2), AC-6(9)-IA-2(4), IA-5(13); CCI-001558, CCI-002221, CCI-002222, CCI-002223, CCI-002235, CCI-000039, CCI-001419, CCI-002234, CCI-000768, CCI-002007.}

This subpart indicates requirements for specific methods of identification and authentication for users and user accounts. Where these requirements conflict apply the following order of precedence: 1) If present, Device Specific Requirements take precedence over any other requirements; and then 2) multifactor authentication requirements take precedence over password requirements.

3.4.1 User Identification and Authentication for All System Types

Unless otherwise indicated, all user interfaces supporting accounts (either FULLY or MINIMALLY) must implement Identification and Authorization via passwords.

3.4.2 User Identification and Authentication for Specific System Types

System specific requirements are in addition to and supersede those indicated for all system types. When no additional requirements are indicated for a specific system type the requirements for all systems still apply to that system type.

3.4.3 User Identification and Authentication for Specific Devices

There are no additional device specific user interface requirements

3.4.4 Implementation of Identification and Authorization Requirements

Identification and Authorization must be met by one of the following methods:

a. Direct implementation in the user interface.

b. For remote interfaces: an implementation shared between the remote user interface server and the remote user interface client. For example, a requirement for PIV authentication may be met on a remote user interface by a PIV reader on a web browser client which sends the authentication information via HTTPS to the remote server.

3.4.5 Password-Based Authentication Requirements

3.4.5.1 Passwords for Controllers FULLY Supporting Accounts

All controllers FULLY supporting accounts and supporting password-based authentication must enforce the following requirements:

a. Minimum password length of 15 characters

b. Password must contain at least one uppercase character.

c. Password must contain at least one lowercase character.

d. Password must contain at least one numeric character.

e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.

f. Password must have a maximum lifetime of sixty (60) days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.

g. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters.

h. Passwords must be cryptographically protected during storage and transmission.

3.4.5.2 Passwords for Remote Interfaces

Passwords for connecting to a Remote User Interface supporting password-based authentication must enforce the following requirements:

a. Minimum password length of 15 characters

b. Password must contain at least one uppercase character.

c. Password must contain at least one lowercase character.

d. Password must contain at least one numeric character.

e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.

f. Password must have a maximum lifetime of 60 days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.

g. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters (where location is significant, a character may be reused if it is in a different position).

h. Passwords must be cryptographically protected during storage and transmission.

3.4.5.3 Passwords for Devices Minimally Supporting Accounts

Devices MINIMALLY supporting accounts must support passwords with a minimum length of four characters.

3.4.5.4 Password Configuration and Reporting

For all devices with a password, change the password from the default password. Coordinate selection of passwords with the Password Point of Contact. Do not use the same password for more than one device unless specifically instructed to do so. Provide a Confidential Password Report documenting the password for each device and describing the procedure to change the password for each device.

Do not provide the Password Summary Report in electronic format. Provide two hardcopies of the Password Summary Report, each copy in its own sealed envelope.

3.4.6 Authenticator Feedback

{For Government Reference Only: This subpart relates to IA-6; CCI-000206}

Devices must never show authentication information, including passwords, on a display. Devices that momentarily display a character as it is entered, and then obscure the character, are acceptable. For devices that have STIGs or SRGs related to obscuring of authenticator feedback (CCI-000206), comply with the requirements of those STIGS/SRGs.

3.5 CYBERSECURITY AUDITING

Where an auditing requirement exists for email notification, notify via email the application administrator and Information System Security Officer (ISSO) of the event. Coordinate with the Email Address Point of Contact for email addresses. If outgoing email is not available to the system, disable email notifications.

3.5.1 Audit Events, Content of Audit Records, and Audit Generation

{For Government Reference Only: This subpart (and its subparts) relates to AU-2(a), AU-2(c), AU-2(d), AU-3, AU-10, AU-12, AU-14(b), AU-14(1), AU-14(2), AU-14(3), CM-5(1), SC-7 (9); CCI-000123, CCI-001571, CCI-000125, CCI-001485, CCI-000130, CCI-000131, CCI-000132, CCI-001230, CCI-000133, CCI-000134, CCI-001487, CCI-000166, CCI-001899, CCI-000169, CCI-001459, CCI-000171, CCI-000172, CCI-001910, CCI-001914, CCI-001919, CCI-001464, CCI-001462, CCI-001920, CCI-001814, CCI-002400. For MODERATE Impact systems, this subpart (and its subparts) also relates to AU-3 (1);

CCI-000135, CCI-001488}

For devices that have STIG/SRGs related to audit events, content of audit records or audit generation, comply with the requirements of those STIG/SRGs.

If auditing requirements can be met using existing control system alarm or event capabilities, those existing capabilities may be used to meet these requirements.

3.5.1.1 Default Requirements for Control System Controllers

For control system controllers where Audit Events, Content of Audit Records, and Audit Generation are not otherwise indicated in this Section:

3.5.1.1.1 Controllers Which FULLY Support Accounts

For each controller which FULLY supports accounts, provide the capability to select audited events and the content of audit logs. Configure controllers to audit the indicated events, and to record the indicated information for each auditable event.

3.5.1.1.1.1 Audited Events

Configure each controller to audit the following events:

a. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels)

b. Successful and unsuccessful logon attempts

c. Successful logouts

d. Concurrent logons from different workstations

e. All account creations, modifications, disabling, and terminations. For MODERATE Impact Systems, also provide email notification when these audit events occur.

f. All kernel module load, unload, and restart

g. For privileged user interfaces in MODERATE Impact Systems: All user commands.

3.5.1.1.1.2 Audit Event Information To Record

Configure each controller to record, for each auditable event, the following information (where applicable to the event):

a. what type of event occurred

b. when the event occurred

c. where the event occurred

d. the source of the event

e. the outcome of the event

f. the identity of any individuals or subjects associated with the event

g. For privileged user interfaces in MODERATE Impact Systems: Full text recording of the executed command and the user executing the command.

For MODERATE Impact Systems: Audit records must provide sufficient detail to reconstruct events to determine cause of compromise and magnitude of damage, malfunction, or security violation

3.5.1.1.2 Controllers Which Do Not FULLY Support Accounts

For each controller which does not FULLY support accounts configure the controller to audit all controller shutdown and startup events and to record for each event the type of event and when the event occurred.

3.5.2 Audit Time Stamps

{For Government Reference Only: This subpart (and its subparts) relates to AU-8; CCI-000159, CCI-001889, CCI-001890. For MODERATE Impact systems, this subpart (and its subparts) also relates to AU-8 (1); CCI-001891, CCI-001892, CCI-002046.}

Any device (computer or controller) generating audit records must have an internal clock capable of providing time with a resolution of one second. Clocks must not drift more than 10 seconds per day. Configure the system so that each device (computer or controller) generating audit records maintains accurate time to within 1 second. Note that if the control system specifications include requirement for clocks, the most stringent requirement applies.

3.5.3 Audit Storage Capacity and Audit Upload

{For Government Reference Only: This subpart (and its subparts) relates to AU-4; CCI-001848, CCI-001849}

The creation of audit records must never interfere with normal device operation. Devices must cease collection of auditing information if required to maintain normal operation.

a. For devices that have STIG/SRGs related to audit storage capacity (CCI-001848 or CCI-001849) comply with the requirements of those STIG/SRGs.

b. For controllers capable of generating audit records, provide 60 days worth of secure local storage, assuming 10 auditable events per day.

3.5.3.1 Audit Log Storage Notification In MODERATE Impact Systems

{For Government Reference Only: This subpart (and its subparts) relates to AU-5(1); CCI-001855.}

Controllers storing audit logs must provide notification when audit logs reach 75 percent of capacity either directly through email or indirectly by sending a notification to a computer, and the computer sending an email. Computers storing audit logs must provide notification when audit logs reach 75 percent of capacity directly through email.

3.6 REQUIREMENTS FOR LEAST FUNCTIONALITY

{For Government Reference Only: This subpart (and its subparts), along with the Network Communication, Ports, Protocols and Services Report submittal specified elsewhere in this section, relates to CM-6(a), CM-6(c), CM-7, CM-7(1)(b), SC-41; CCI-000363, CCI-000364, CCI-000365, CCI-001588, CCI-001755, CCI-000381, CCI-000380, CCI-000382, CCI-001761, CCI-001762, CCI-002544, CCI-002545, CCI-002546. For MODERATE Impact systems, this subpart (and its subparts) also relates to CM-7(2), CM-7(5)(a), CM-7(5)(b); CCI-000381, CCI-000380, CCI-000382, CCI-001761, CCI-001762}

For devices that have a STIG or SRG related to Requirements for Least Functionality (such as configuration settings and port and device I/O access for least functionality), install and configure the device in accordance with that STIG or SRGs.

3.6.1 Device Capabilities

Do not provide devices with remote user interfaces or full user interfaces where one was not required. Do not use a networked sensor or actuator where a non-networked sensor or actuator would suffice.

For all MODERATE Impact Systems: Unless specifically required by the government, do not provide a capability to update device firmware over the network.

3.6.2 Software

For software that has a STIG or SRG related to Requirements for Least Functionality (such as configuration settings and port access for least functionality), install and configure the software in accordance with that STIG or SRG.

Do not install software that is not specifically required to meet a contract requirement. Remove any previously installed that is not specifically required to meet a contract requirement. Do not implement functionality within software
that is not specifically required to meet contract requirements.

3.7 SYSTEM AND COMMUNICATION PROTECTION

3.7.1 Denial of Service Protection and Application Partitioning In MODERATE Impact Systems:

{For Government Reference Only: This subpart relates to SC-5, SC-12, SC-7(a); CCI-001093, CCI-002385, CCI-002386, CCI-002430, CCI-001097. For MODERATE Impact systems, this subpart also relates to SC-2; CCI-001082.}

To the greatest extent practical, implement control logic without reliance on the network. Except when required to meet the requirements of the control system Section (where the requirement can only be met using computer hardware), do not implement control logic in computers. For MODERATE Impact systems, do not implement control logic in a device providing (i.e. acting as a server for) a Full Remote User Interface.

3.7.1.1 Default Requirements for MODERATE Impact Control Systems

Except for networked input and outputs on input-output buses specifically

designed to provide high reliability or redundancy, sensors and actuators must not rely on the network to exchange data with the controller executing the sequence of operation which uses the sensor value or determines the actuator command.

Sensor values required by multiple devices may be shared over the network provided they are connected to a controller requiring the value for execution of the sequence and that controller shares the value on the network.

3.7.2 Mobile Code In MODERATE Impact Systems:

{For Government Reference Only: This subpart relates to SC-18(a), SC-18(b),
SC-18(c), SC-18(1), SC-18(3), SC-18(4); CCI-001160, CCI-001161, CCI-001162, CCI-001163, CCI-001164, CCI-001165, CCI-001166, CCI-001662, CCI-002457, CCI-002458, CCI-001169, CCI-001695, CCI-001170, CCI-002469}

Devices with STIGs/SRGs related to Mobile Code and to Security Control SC-18 must be installed in accordance with the relevant STIGs/SRGs. All remote user interfaces must meet the requirements of the "Web Browsers and Application SRG".

Mobile code may only be downloaded from a specifically authorized mobile code repository. Coordinate with the Mobile Code Point of Contact for the location of a repository.

3.7.3 Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems

{For Government Reference Only: This subpart relates to SC-7(a), SC-7(c), SC-7(4)(a), SC-7(4)(c), SC-7(5), SC-7(7), SC-7(9)(a), SC-7(11), SC-7(13), SC-7(13), SC-7(18); CCI-001097, CCI-001098, CCI-001102, CCI-002396, CCI-001109, CCI-002397, CCI-002398, CCI-002399, CCI-002403, CCI-001120, CCI-001119, CCI-001126}

3.7.3.1 Radio Interfaces for Fire Protection Systems

When radios interfacing a local fire protection system to a supervisory system are not NIST FIPS 140-2 validated, use a relay panel interface between the local fire protection system and the radio. Install and configure the relay panel to prohibit initiating any action within the local fire protection system other than causing the system to play a pre-recorded message or causing the system to play a live audio message.

3.7.3.2 Fire Suppression System Network Isolation

For fire suppression systems including a release panel, any network used in these systems must be dedicated to these systems and must be isolated from any other network, including other components of the Fire Alarm and Fire Suppression systems. Use only dry contacts and relays to transfer signals from these systems to any other systems.

3.8 SAFE MODE AND FAIL SAFE OPERATION

{For Government Reference Only: This subpart (and its subparts) relates to CP-12, SI-10(3), SI-17; CCI-002855, CCI-002856, CCI-002857, CCI-002754, CCI-002773, CCI-002774, CCI-002775}

For all control system components with an applicable STIG or SRG, configure the component in accordance with all applicable STIGs and SRGs.

3.9 SYSTEM MAINTENANCE TOOL SOFTWARE

{For Government Reference Only: This subpart (and its subparts) relates to MA-3; CCI-000865.}

Submit and license to the Government all software required to operate, maintain and modify the control system such the Government or their agents are able to perform repair, replacement, upgrades, and expansions of the system without subsequent or future dependence on the Contractor, Vendor or Manufacturer. Submit hard copies of user manuals for each software with the software submittal. Provide any hardware keys or dongles, software keys, license numbers, and other information required to enable the Government to access or change the system.

For software provided and licensed to the Government under the requirements of another Section, submit a statement indicating the Section and Submittal under which the software was provided. For software provided to meet the requirements of this Section and not provided and licensed under another Section, submit software and software user manuals on DVD or CD as a Technical Data Package and submit one hard copy of the software user manual for each piece of software.

3.10 DEVICE POWER

{For Government Reference Only: This subpart (and its subparts) relates to PE-11, PE-11(1); CCI-002955, CCI-000961. For MODERATE Impact systems, this subpart (and its subparts) also relates to PE-9, PE-9(1); CCI-000952, CCI-002953, CCI-002954.}

For MODERATE Impact Systems: Provide control system with power supply meeting or exceeding the reliability of the controlled equipment. Powering control system devices using the same power source as the equipment controlled by the device is a permissible method of meeting this requirement. Without explicit approval from the government, do not install local uninterruptible power supplies (UPSes) as a source of device power.

3.10.1 Device Behavior on Loss of Power In MODERATE Impact Systems:

Application programs and configuration settings must be stored in devices in manner such that a loss of power does not result in a loss of the application program or configuration settings: Loss of power must never result in the loss of application programs, regardless of the length of time power is lost; and loss of power for less than 2,500 hours must not result in the loss of configured settings.

In the event of a loss of power, when power is restored, controllers and computers executing control logic (and the underlying equipment) must recover and resume their normal sequences of operation. Note that the sequence of operation may require specific actions (e.g. startup sequences) upon recovery from loss of power.

3.11 VULNERABILITY SCANNING

{For Government Reference Only: This subpart (and its subparts) relates to RA-5 RA-5(a),RA-5(b),RA-5(c),RA-5(d); CCI-001054, CCI-001055,

CCI-000156, CCI-001641, CCI-001643, CCI-001057, CCI-001058, CCI-001059. For MODERATE Impact systems, this subpart (and its subparts) also relates to RA-5(1), RA-5(5); CCI-001062, CCI-001067, CCI-001645, CCI-002906.}

All IP devices must be scannable, such that the device can be scanned by industry standard IP network scanning utilities without harm to the device, application, or functionality.

3.11.1 Controllers

Provide controllers that are scannable by standard control system discovery tools or control system browsers and return meaningful status information including the network inputs and outputs for the controller. This information must contain sufficient detail to detect vulnerabilities or exploits of the controller.

Provide all software needed to scan the control system as the Control System Scanning Tools submittal. If the software required to scan the system is already installed at the project site or is provided under a separate section instead provide a statement indicating this.

3.12 FIPS 201-2 REQUIREMENT

{For Government Reference Only: This subpart (and its subparts) relates to SA-4 (10); CCI-003116}

Devices in the following systems which implement PIV must be on the NIST FIPS 201-2 approved product list (https://www.idmanagement.gov/approved-products-list/): NONE.

3.13 SYSTEM AND INTEGRATION INTEGRITY

3.13.1 Software, Firmware, and Information Integrity In MODERATE Impact Systems:

{For Government Reference Only: This subpart relates to CM-5(3); CCI-001749, CCI-002704, CCI-002726}

If there exists Integrity Verification Software that can check boot process, software, firmware, or information in the control system and verify its integrity, provide it. If no such software exists, provide a statement to this affect in lieu of the software.

3.14 CONTROL SYSTEM CYBERSECURITY TESTING

{For Government Reference Only: For MODERATE Impact systems, this subpart (and its subparts) relates to SA-11(a), SA-11(b), SA-11(c), SA-11(d), SA-11(e); CCI-003171, CCI-003172, CCI-003173, CCI-003174, CCI-003175, CCI-003176, CCI-003177, CCI-003178.}

3.14.1 Control System Cybersecurity Testing Procedures

Prepare and submit Control System Cybersecurity Testing Procedures explaining step-by-step, the actions and expected results that will demonstrate that the control system meets the requirements of this Section. The Control System Cybersecurity Testing Procedures may be submitted as a Technical Data Package.

3.14.2 Control System Cybersecurity Testing Execution

Using the Control System Cybersecurity Testing Procedures verify that the control system meets the requirements of this Section. UNLESS GOVERNMENT WITNESSING OF A TEST IS SPECIFICALLY WAIVED BY THE GOVERNMENT, PERFORM ALL TESTS WITH A GOVERNMENT WITNESS. If testing reveals deficiencies in the system, correct the deficiency and retest until successful.

3.14.3 Control System Cybersecurity Testing Report

Prepare and submit a Control System Cybersecurity Testing Report documenting all tests performed and their results. Include all tests in the Control System Cybersecurity Testing Procedures and any additional tests performed during testing. Document test failures and repairs conducted with the test results. The Control System Cybersecurity Testing Report may be submitted as a Technical Data Package

3.15 FIELD QUALITY CONTROL, CYBERSECURITY VALIDATION SUPPORT

In addition to testing and testing support required by other Sections, provide a minimum of 16 hours of technical support for cybersecurity testing of control systems to support the DoD Risk Management Framework process Cybersecurity assessment of the control system. This support is independent of (and in addition to) the Control System Cybersecurity Testing specified in this section.

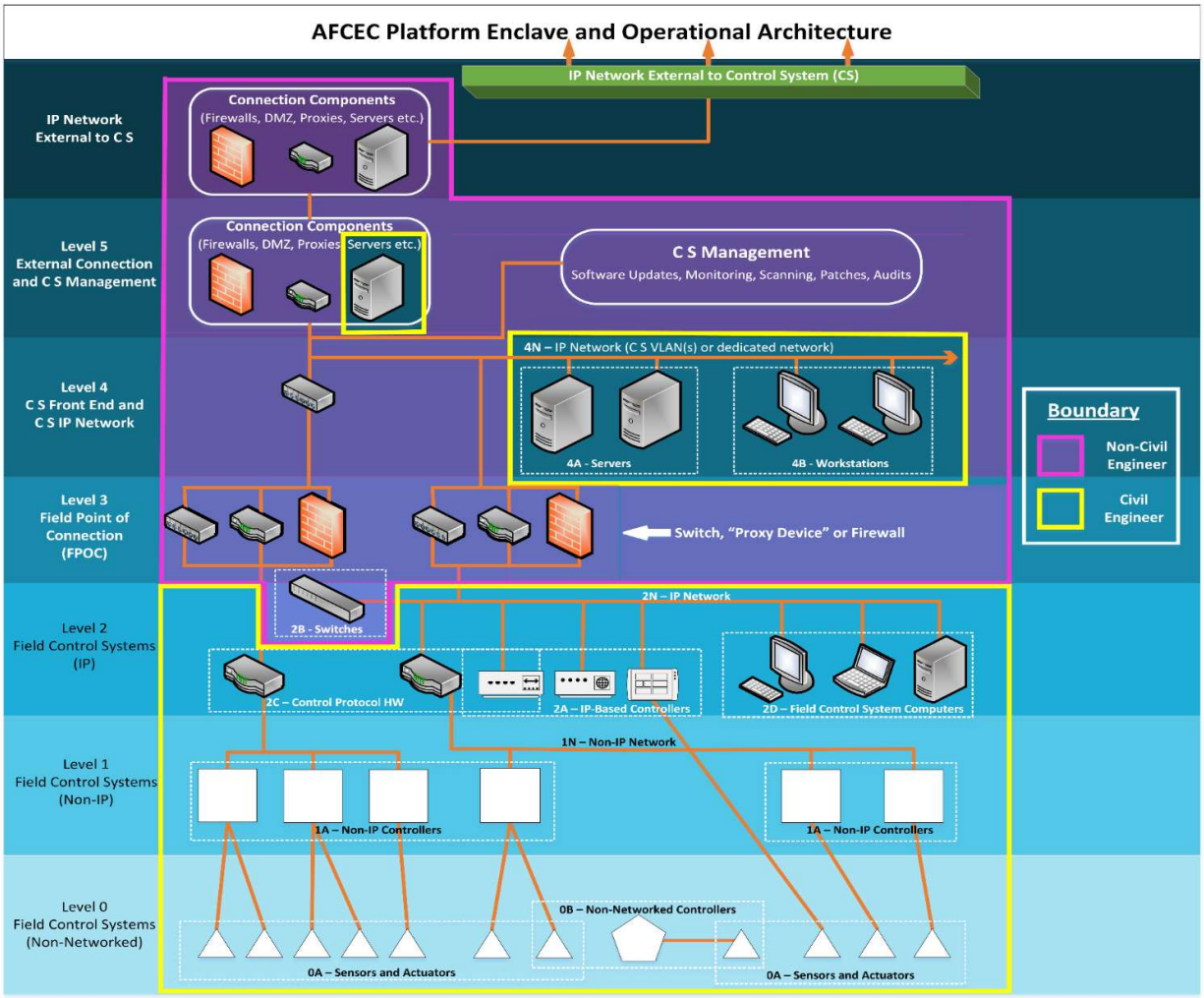
3.16 CYBERSECURITY TRAINING

Provide eight hours of classroom and hands-on training for six Government personnel on the cybersecurity operation and maintenance of the control system provided. This training is in addition to and must be coordinated with control system training specified in other Sections.

The Government will provide the training location. Training must cover, at a minimum: (a) applying software and firmware updates, (b) user account creation, modification and deletion, (c) audit log upload procedures and (d) identification of privileged user interfaces and system impact of those interfaces. Training session must include a question and answer period during which government staff questions about cybersecurity aspects of the control system are answered.

-- End of Section --

Project Name:	SF NC ANG 145
[redacted]	
Designer:	AECOM
Date:	5/28/2025



PROJECT NAME:	AGENCY:		DATE:	CONTROL SYSTEM:				BUILDING:
60637899	AFCEC		5/28/2025	MECHANICAL				Security Forces Building
UFGS SPECIFICATION REFERENCE	DEVICE	PIT LEVEL	NETWORK CONNECTIVITY & COMMUNICATION PROTOCOL	DRAWING/ SPECIFICATION CROSS-REFERENCE	C-I-A IMPACT	SYSTEM OWNER	AUTHORIZING OFFICIAL	COMMENTS
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS	Microprocessor Based HVAC DDC	2A	BACnet/IP over Ethernet	M701 M801 M802	LOW-LOW-LOW	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
22 00 00 PLUMBING, GENERAL PURPOSE 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS	Electric Water Heater	2A	BACnet/IP over Ethernet	M701	LOW-LOW-LOW	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS	Thermostatic Mixing Valve (TMV)	2A	BACnet/IP over Ethernet	M701	LOW-LOW-LOW	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS	Packaged Rooftop Unit	2A	BACnet/IP over Ethernet	M701 M801 M802	LOW-LOW-LOW	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC	Fan Coils	0A	Dry Contacts over Copper Cables	M701 M801 M802	LOW-LOW-LOW	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC	Heat Pump	0A	Dry Contacts over Copper Cables	M701 M801 M802	LOW-LOW-LOW	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC	Fan	0A	Dry Contacts over Copper Cables	M701 M801 M802	LOW-LOW-LOW	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC	Unit Heater	0A	Analog and Discrete I/O over Copper Cables to DDC	M801	LOW-LOW-LOW	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC	VAV for Rooftop Unit	0A	Analog and Discrete I/O over Copper Cables to DDC	M801	LOW-LOW-LOW	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
22 00 00 PLUMBING, GENERAL PURPOSE	Water Meter to DDC	0A	4-20 mA (Analog) or Pulse Counter over Copper Cables	M701 M802	LOW-LOW-LOW	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
26 20 00 - INTERIOR DISTRIBUTION SYSTEM	Electrical Meter to DDC	2A	Ethernet (Per Client Comment) to DDC/UMCS	E601 M802	LOW-LOW-LOW	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
26 20 00 - INTERIOR DISTRIBUTION SYSTEM	Generator	0A	Analog and Discrete I/O over Copper Cables to DDC	E601 M802	LOW-LOW-LOW	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	

PROJECT NAME:	AGENCY:		DATE:	CONTROL SYSTEM:				BUILDING:
60637899	AFCEC		5/28/2025	FIRE & LIFE SAFETY				Security Forces Building
UFGS SPECIFICATION REFERENCE	DEVICE	PIT LEVEL	NETWORK CONNECTIVITY & COMMUNICATION PROTOCOL	DRAWING/ SPECIFICATION CROSS-REFERENCE	C-I-A IMPACT	SYSTEM OWNER	AUTHORIZING OFFICIAL	COMMENTS
21 13 13.00 10 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	FACU	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-MOD-MOD	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
21 13 13.00 10 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Pull Station	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-MOD-MOD	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
21 13 13.00 10 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	LED Text Signs	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-MOD-MOD	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
21 13 13.00 10 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Speaker/Strobe	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-MOD-MOD	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
21 13 13.00 10 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Strobe Only	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-MOD-MOD	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
21 13 13 - WET PIPE SPRINKLER SYSTEMS, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Smoke Detection	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-MOD-MOD	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
21 13 13.00 10 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Addressable Input/Output Module	1A	Proprietary Serial and Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-MOD-MOD	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Monaco Radio Communications Interface Card	1A	Serial over EIA 422 pinouts over Standard Copper Cables	FA501 FA502 FA503	LOW-MOD-MOD	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	
21 13 13.00 10 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE	Waterflow Devices	0A	Relay Contacts over Standard Copper Cables	FA501 FA502 FA503	LOW-MOD-MOD	145th Airlift Wing - North Carolina Air National Guard Base PWD	DAF CE CS	

CCI List & Tailoring Information

Mechanical-HVAC

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-1(a)	2107	The organization defines the personnel or roles to be recipients of the access control policy necessary to facilitate the implementation of the access control policy and associated access controls.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-1(a)	CCI-002108	The organization defines the personnel or roles to be recipients of the procedures necessary to facilitate the implementation of the access control policy and associated access controls.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-1(a)(1)	CCI-000001	The organization develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization being inspected/assessed develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization conducting the inspection/assessment obtains and examines the access control policy to ensure the organization being inspected/assessed develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-1(a)(1)	CCI-000002	The organization disseminates the access control policy to organization-defined personnel or roles.	The organization being inspected/assessed disseminates via an information sharing capability to all personnel. DoD has defined the personnel or roles as all personnel.	The organization conducting the inspection/assessment examines the access control policy via the organization's information sharing capability to ensure the organization being inspected/assessed disseminates the policy to all personnel. DoD has defined the personnel or roles as all personnel.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-1(a)(2)	CCI-000004	The organization develops and documents procedures to facilitate the implementation of the access control policy and associated access controls.	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of the access control policy and associated access controls.	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the access control policy and associated access controls to ensure the organization being inspected/assessed develops and documents procedures to facilitate the implementation of the access control policy and associated access controls.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-1(a)(2)	CCI-000005	The organization disseminates the procedures to facilitate access control policy and associated access controls to the organization-defined personnel or roles .	The organization being inspected/assessed disseminates via an information sharing capability to all personnel the procedures to facilitate access control policy and associated access controls. DoD has defined the personnel or roles as all personnel.	The organization conducting the inspection/assessment examines the procedures to facilitate access control policy and associated access controls via the organization's information sharing capability to ensure the organization being inspected/assessed disseminates the procedures to all personnel. DoD has defined the personnel or roles as all personnel.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-1(b)(1)	CCI-000003	The organization reviews and updates the access control policy in accordance with organization-defined frequency.	The organization being inspected/assessed annually reviews and updates the access control policy. The organization must maintain review and update activity as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed annually reviews and updates the access control policy. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-1(b)(1)	CCI-001545	The organization defines a frequency for reviewing and updating the access control policy.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AC-1(b)(2)	CCI-000006	The organization reviews and updates the access control procedures in accordance with organization-defined frequency.	The organization being inspected/assessed annually reviews and updates the access control procedures. The organization must maintain review and update activity as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed annually reviews and updates the access control procedures. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-1(b)(2)	CCI-001546	The organization defines a frequency for reviewing and updating the access control procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AC-10(b)	CCI-002332	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store or transmit organization-controlled information using the external information systems.	The organization being inspected/assessed establishes and documents the terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store or transmit organization-controlled information using the external information systems.	The organization conducting the inspection/assessment obtains and examines the documented terms and conditions to ensure the organization being inspected/assessed establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store or transmit organization-controlled information using the external information systems.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-2(a)	CCI-001227	The organization corrects information system flaws.	The organization being inspected/assessed corrects information system flaws within the time period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs). The organization documents the corrections on their POA&M. DoD has defined the time period as within the time period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines the information system POA&M and examines the information system to ensure the organization being inspected/assessed corrects information system flaws.	LOW	X		X	X				1.10 SOFTWARE LICENSING		CCI requirements are addressed within subparagraph "Software Licensing" of UFGS 25 05 11.
N/A	SI-2(c)	CCI-002605	The organization installs security-relevant software updates within organization-defined time period of the release of the updates	The organization being inspected/assessed configures the information system to install security-relevant software updates within 30 days of the release of the updates For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2605. DoD has defined the time period as 30 days.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to install security-relevant software updates within 30 days of the release of the updates. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2605. DoD has defined the time period as 30 days.	LOW			X					1.10 SOFTWARE LICENSING		CCI requirements are addressed within subparagraph "Software Licensing" of UFGS 25 05 11.
N/A	AC-17(a)	CCI-000063	The organization defines allowed methods of remote access to the information system.	The organization being inspected/assessed defines and documents the allowed methods of remote access to the information system. The methods should be defined IAW ports, protocols, and service requirements, as well as access control requirements for any STIGs applicable to the technology in use. DoD has determined the allowed methods of remote access are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented methods to ensure the organization being inspected/assessed defines allowed methods of remote access to the information system. DoD has determined the allowed methods of remote access are not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(a)	CCI-002310	The organization establishes and documents usage restrictions for each type of remote access allowed.	The organization being inspected/assessed establishes and documents usage restrictions for each type of remote access allowed.	The organization conducting the inspection/assessment obtains and examines the documented usage restrictions to ensure the organization being inspected/assessed establishes and documents usage restrictions for each type of remote access allowed.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(a)	CCI-002311	The organization establishes and documents configuration/connection requirements for each type of remote access allowed.	The organization being inspected/assessed establishes and documents configuration/connection requirements for each type of remote access allowed.	The organization conducting the inspection/assessment obtains and examines the documented requirements to ensure the organization being inspected/assessed establishes and documents configuration/connection requirements for each type of remote access allowed.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(a)	CCI-002312	The organization establishes and documents implementation guidance for each type of remote access allowed.	The organization being inspected/assessed establishes and documents implementation guidance for each type of remote access allowed.	The organization conducting the inspection/assessment obtains and examines the documented implementation guidance to ensure the organization being inspected/assessed establishes and documents implementation guidance for each type of remote access allowed.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(b)	CCI-000065	The organization authorizes remote access to the information system prior to allowing such connections	The organization being inspected/assessed authorizes remote access to the information system prior to allowing such connections. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes remote access to the information system prior to allowing such connections.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
CA-3	CA-3(b)	CCI-000258	The organization documents, for each interconnection, the interface characteristics.	The organization being inspected/assessed will document the interface characteristics for each interconnection. Use of external reporting databases for these characteristics when tied to the specific interconnection is acceptable (e.g., ports, protocols, and services). Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	The organization conducting the inspection/assessment obtains and examines interconnection security agreement documentation. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	LOW	X	X	X					1.9.2 Cybersecurity Interconnection Sched… 1.11 CYBERSECURITY DURING CONSTRUCTION		Cybersecurity requirements will be documented by the contractor in the Cybersecurity Interconnection Schedule and is addressed withing Sub-Paragraphs "Cybersecurity During Construction" and "Cybersecurity Interconnection Schedule" within Part 1.
CA-9	CA-9(a)	CCI-002102	The organization defines the information system components or classes of components that that are authorized internal connections to the information system.	The organization being inspected/assessed defines and documents the information system components or classes of components that that are authorized internal connections to the information system. DoD has determined the information system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components or classes of components that that are authorized internal connections to the information system. DoD has determined the information system components are not appropriate to define at the Enterprise level.	LOW		X						1.9.3 Network Communication Report		Cybersecurity requirements will be documented by the contractor and required for submission of the Network Communication Report. This is documented within Sub-Paragraph "Network Communication Report" withing Part 1

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
CA-9	CA-9(b)	CCI-002103	The organization documents, for each internal connection, the interface characteristics.	The organization being inspected/assessed documents, for each internal connection, the interface characteristics.	The organization conducting the inspection/assessment obtains and examines the documented interface characteristics as well as the network topology to ensure the organization being inspected/assessed documents, for each internal connection, the interface characteristics.	LOW		X						1.9.3 Network Communication Report		Cybersecurity requirements will be documented by the contractor and required for submission of the Network Communication Report. This is documented within Sub-Paragraph "Network Communication Report" withing Part 1
CA-9	CA-9(b)	CCI-002104	The organization documents, for each internal connection, the security requirements.	The organization being inspected/assessed documents, for each internal connection, the security requirements.	The organization conducting the inspection/assessment obtains and examines the documented security requirements as well as the network topology to ensure the organization being inspected/assessed documents, for each internal connection, the security requirements.	LOW		X						1.9.3 Network Communication Report		Cybersecurity requirements will be documented by the contractor and required for submission of the Network Communication Report. This is documented within Sub-Paragraph "Network Communication Report" withing Part 1
N/A	AC-19(a)	CCI-000082	The organization establishes usage restrictions for organization controlled mobile devices.	The organization being inspected/assessed establishes and documents usage restrictions for organization controlled mobile devices.	The organization conducting the inspection/assessment obtains and examines the documented usage restrictions to ensure the organization being inspected/assessed establishes usage restrictions for organization controlled mobile devices.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-19(a)	CCI-000083	The organization establishes implementation guidance for organization controlled mobile devices.	The organization being inspected/assessed establishes and documents implementation guidance for organization controlled mobile devices.	The organization conducting the inspection/assessment obtains and examines the documented implementation guidance to ensure the organization being inspected/assessed establishes implementation guidance for organization controlled mobile devices.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-19(a)	CCI-002325	The organization establishes configuration requirements for organization controlled mobile devices.	DoD is automatically compliant with this CCI because existing STIGs establish configuration requirements for approved mobile devices.	DoD is automatically compliant with this CCI because existing STIGs establish configuration requirements for approved mobile devices.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-19(a)	CCI-002326	The organization establishes connection requirements for organization controlled mobile devices.	The organization being inspected/assessed establishes and documents connection requirements for organization controlled mobile devices.	The organization conducting the inspection/assessment obtains and examines the documented connection requirements to ensure the organization being inspected/assessed establishes connection requirements for organization controlled mobile devices.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-19(b)	CCI-000084	The organization authorizes connection of mobile devices to organizational information systems.	The organization being inspected/assessed authorizes connection of mobile devices to organizational information systems. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes connection of mobile devices to organizational information systems.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
CA-9	CA-9(b)	CCI-002105	The organization documents, for each internal connection, the nature of the information communicated.	The organization being inspected/assessed documents, for each internal connection, the nature of the information communicated.	The organization conducting the inspection/assessment obtains and examines the documented nature of information communication as well as the network topology to ensure the organization being inspected/assessed documents, for each internal connection, the nature of the information communicated.	LOW		X						1.9.3 Network Communication Report		Cybersecurity requirements will be documented by the contractor and required for submission of the Network Communication Report. This is documented within Sub-Paragraph "Network Communication Report" withing Part 1
N/A	AC-2(a)	CCI-002111	The organization identifies and selects the organization-defined information system account types of information system accounts which support organizational missions/business functions.	The account types are defined per AC-2, CCI 2110.	The account types are defined per AC-2, CCI 2110.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(b)	CCI-002112	The organization assigns account managers for information system accounts.	The organization being inspected/assessed documents personnel responsible for the management of system accounts.	The organization conducting the inspection/assessment obtains and examines the documented appointment of management personnel to ensure that the organization being inspected/assessed has documented personnel responsible for the management of system accounts.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(c)	CCI-000008	The organization establishes conditions for group membership.	The organization being inspected/assessed documents conditions for adding accounts as members of groups.	The organization conducting the inspection/assessment obtains and examines the documented conditions for adding accounts as members of groups to ensure that the conditions are established.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(c)	CCI-002113	The organization establishes conditions for role membership.	The organization being inspected/assessed documents conditions for adding accounts as members of roles.	The organization conducting the inspection/assessment obtains and examines the documented conditions for adding accounts as members of roles to ensure that the conditions are established.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(d)	CCI-002115	The organization specifies authorized users of the information system.	The organization being inspected/assessed documents authorized users of the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of authorized users for a sampling of information system accounts to ensure that the authorized users are specified.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(d)	CCI-002116	The organization specifies authorized group membership on the information system.	The organization being inspected/assessed documents authorized group membership on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of authorized groups for a sampling of information system accounts to ensure that the authorized groups are specified.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(d)	CCI-002117	The organization specifies authorized role membership on the information system.	The organization being inspected/assessed documents authorized role membership on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of authorized roles for a sampling of information system accounts to ensure that the authorized roles are specified	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(d)	CCI-002118	The organization specifies access authorizations (i.e., privileges) for each account on the information system.	The organization being inspected/assessed documents access authorizations (i.e., privileges) for each account on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of access authorizations for a sampling of information system accounts to ensure that the access authorizations are specified.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(d)	CCI-002119	The organization specifies other attributes for each account on the information system.	The organization being inspected/assessed documents other attributes for each account on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of other attributes for a sampling of information system accounts to ensure that other attributes are specified.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-2(e)	CCI-000010	The organization requires approvals by organization-defined personnel or roles for requests to create information system accounts.	The organization being inspected/assessed implements a process for the ISSM or ISSO to approve information system account requests. The organization being inspected/assessed maintains an audit trail of approvals. DoD has defined the personnel or roles as the ISSM or ISSO.	The organization conducting the inspection/assessment obtains and examines the audit trail of approvals to ensure that the organization being inspected/assessed implements a process for the ISSM or ISSO to approve information system account requests. DoD has defined the personnel or roles as the ISSM or ISSO.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(e)	CCI-002120	The organization defines the personnel or roles authorized to approve the creation of information system accounts.	DoD has defined the personnel or roles as the ISSM or ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSM or ISSO.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(f)	CCI-000011	The organization creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions.	The organization being inspected/assessed implements account maintenance processes to create, enable, modify, disable, and remove information system accounts in accordance with procedures or conditions defined in AC-2, 2121. The organization being inspected/assessed maintains an audit trail of account maintenance activities.	The organization conducting the inspection/assessment obtains and examines the audit trail of account maintenance activities to ensure the organization being inspected/assessed implements account maintenance processes to create, enable, modify, disable, remove, and track information system accounts in accordance with procedures or conditions defined in AC-2, 2121.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(f)	CCI-002121	The organization defines the procedures or conditions to be employed when creating, enabling, modifying, disabling, and removing information system accounts.	The organization being inspected/assessed defines and documents the procedures or conditions to be employed when creating, enabling, modifying, disabling, and removing information system accounts. DoD has determined the procedures or conditions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented procedures or conditions to ensure the organization being inspected/assessed defines the procedures or conditions to be employed when creating, enabling, modifying, disabling, and removing information system accounts. DoD has determined the procedures or conditions are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(g)	CCI-002122	The organization monitors the use of information system accounts.	The organization being inspected/assessed implements a process to monitor the use of information system accounts.	The organization conducting the inspection/assessment obtains and examines the audit trail to ensure that the organization being inspected/assessed implements a process to monitor the use of information system accounts.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(h)(1)	CCI-002123	The organization notifies account managers when accounts are no longer required.	The organization being inspected/assessed implements a process to notify account managers when accounts are no longer required. The organization being inspected/assessed maintains an audit trail of notifications.	The organization conducting the inspection/assessment obtains and examines the audit trail of notifications to ensure the organization being inspected/assessed implements a process to notify account managers when accounts are no longer required.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(h)(2)	CCI-002124	The organization notifies account managers when users are terminated or transferred.	The organization being inspected/assessed implements a process to notify account managers when users are terminated or transferred. The organization being inspected/assessed maintains an audit trail of notifications.	The organization conducting the inspection/assessment obtains and examines the audit trail of notifications to ensure the organization being inspected/assessed implements a process to notify account managers when users are terminated or transferred.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(h)(3)	CCI-002125	The organization notifies account managers when individual information system usage or need-to-know changes.	The organization being inspected/assessed implements a process to notify account managers when individual information system usage or need-to-know changes. The organization being inspected/assessed maintains an audit trail of notifications.	The organization conducting the inspection/assessment obtains and examines the audit trail of notifications to ensure the organization being inspected/assessed implements a process to notify account managers when individual information system usage or need-to-know changes.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(i)(1)	CCI-002126	The organization authorizes access to the information system based on a valid access authorization.	The organization being inspected/assessed authorizes access to the information system based on the access authorization process. The organization being inspected/assessed maintains an audit trail of approved access.	The organization conducting the inspection/assessment obtains and examines the audit trail of approved access to ensure the organization being inspected/assessed authorizes access to the information system based on the access authorization process.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(i)(2)	CCI-002127	The organization authorizes access to the information system based on intended system usage.	The organization being inspected/assessed authorizes access to the information system based on intended system usage. The organization being inspected/assessed maintains an audit trail of approved access.	The organization conducting the inspection/assessment obtains and examines the audit trail of approved access to ensure the organization being inspected/assessed authorizes access to the information system based on intended system usage.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(i)(3)	CCI-002128	The organization authorizes access to the information system based on other attributes as required by the organization or associated missions/business functions.	The organization being inspected/assessed authorizes access to the information system based on other attributes as required by the organization or associated missions/business functions. The organization being inspected/assessed maintains an audit trail of approved access.	The organization conducting the inspection/assessment obtains and examines the audit trail of approved access to ensure the organization being inspected/assessed authorizes access to the information system based on other attributes as required by the organization or associated missions/business functions.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-2(j)	CCI-000012	The organization reviews information system accounts for compliance with account management requirements per organization-defined frequency.	The organization being inspected/assessed implements a process to review information system accounts for compliance with account management requirements at a minimum, annually. The organization being inspected/assessed maintains an audit trail of reviews. DoD has defined the frequency as at a minimum, annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organization being inspected/assessed implements a process to review information system accounts for compliance with account management requirements at a minimum, annually. DoD has defined the frequency as at a minimum, annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(j)	CCI-001547	The organization defines the frequency on which it will review information system accounts for compliance with account management requirements.	DoD has defined the frequency as at a minimum, annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at a minimum, annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AC-2(k)	CCI-002129	The organization establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	The organization being inspected/assessed includes in the account management procedures a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	The organization conducting the inspection/assessment obtains and examines the account management procedures to ensure the organization being inspected/assessed includes in the account management procedures a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-20(a)	CCI-000093	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems.	The organization being inspected/assessed establishes and documents terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems.	The organization conducting the inspection/assessment obtains and examines the documented terms and conditions to ensure the organization being inspected/assessed establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-21(a)	CCI-000098	The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information circumstances where user discretion is required.	The organization being inspected/assessed documents and implements a process to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for information circumstances defined in AC-21, CCI 1470 where user discretion is required.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed determines whether access authorizations assigned to the sharing partner match the access restrictions on the information for information circumstances defined in AC-21, CCI 1470 where user discretion is required.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-21(a)	CCI-001470	The organization defines information sharing circumstances where user discretion is required.	The organization being inspected/assessed defines and documents information sharing circumstances where user discretion is required. DoD has determined the information sharing circumstances are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information sharing circumstances to ensure the organization being inspected/assessed defines information sharing circumstances where user discretion is required. DoD has determined the information sharing circumstances are not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-21(b)	CCI-001471	The organization employs organization defined automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions.	The organization being inspected/assessed implements the process defined in AC-21, CCI 1472 to assist users in making information sharing/collaboration decisions.	The organization conducting the inspection/assessment obtains and examines the documented process defined per AC-21, CCI 1472 to ensure the organization being inspected/assessed assists users in making information sharing/collaboration decisions.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-21(b)	CCI-001472	The organization defines the automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions.	The organization being inspected/assessed defines and documents the automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions. DoD has determined the automated mechanisms or manual processes are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented automated mechanisms to ensure the organization being inspected/assessed defines the automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions. DoD has determined the automated mechanisms or manual processes are not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-22(a)	CCI-001473	The organization designates individuals authorized to post information onto a publicly accessible information system.	The organization being inspected/assessed identifies and documents individuals authorized to post information onto a publicly accessible information system.	The organization conducting the inspection/assessment obtains and examines the list of individuals to ensure the organization being inspected/assessed designates individuals authorized to post information onto a publicly accessible information system.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS is not publically accessible."	
N/A	AC-22(b)	CCI-001474	The organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information.	The organization being inspected/assessed documents and implements a process to train authorized individuals to ensure that publicly accessible information does not contain nonpublic information. The organization must maintain an audit trail of the training conducted.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of the training conducted to ensure the organization being inspected/assessed trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS is not publically accessible."	
N/A	AC-22(c)	CCI-001475	The organization reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.	The organization being inspected/assessed	The organization conducting the inspection/assessment obtains and examines	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS is not publically accessible."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-22(d)	CCI-001476	The organization reviews the content on the publicly accessible information system for nonpublic information on an organization-defined frequency.	The organization being inspected/assessed documents and implements a process to review the content on the publicly accessible information system for nonpublic information on an organization-defined frequency. The organization must maintain an audit trail of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reviews to ensure the organization being inspected/assessed reviews the content on the publicly accessible information system for nonpublic information on an organization-defined frequency.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS is not publically accessible."	
N/A	AC-22(d)	CCI-001477	The organization defines a frequency for reviewing the content on the publicly accessible information system for nonpublic information.	DoD has defined the frequency as every 90 days or as new information is posted.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 90 days or as new information is posted.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS is not publically accessible."	
N/A	AC-22(e)	CCI-001478	The organization removes nonpublic information from the publicly accessible information system, if discovered.	The organization being inspected/assessed documents and implements a process to remove nonpublic information from the publicly accessible information system, if discovered.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed removes nonpublic information from the publicly accessible information system, if discovered.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS is not publically accessible."	
CM-8	CM-8(a)(1)	CCI-000389	The organization develops and documents an inventory of information system components that accurately reflects the current information system.	The organization being inspected/assessed documents inventory of information system components that accurately reflects the current information system.	The organization conducting the inspection/assessment obtains and examines the documented inventory and examines a sampling of information system components to ensure inventory accurately reflects the current information system.	LOW		X						1.9.4 Control System Inventory Report		Cybersecurity design requires the contractor to document the inventory of components within the control system through the submission of a Control System Inventory Report. This design requirement is captured in Sub-Paragraph "Control System Inventory Report" within Part 1.
CM-8	CM-8(a)(2)	CCI-000392	The organization develops and documents an inventory of information system components that includes all components within the authorization boundary of the information system.	The organization being inspected/assessed documents inventory of information system components that includes all components within the authorization boundary of the information system.	The organization conducting the inspection/assessment obtains and examines the documented inventory and examines a sampling of information system components to ensure inventory includes all components within the authorization boundary of the information system.	LOW		X						1.9.4 Control System Inventory Report		Cybersecurity design requires the contractor to document the inventory of components within the control system with components through the submission of a Control System Inventory Report. This design requirement is captured in Sub-Paragraph "Control System Inventory Report" within Part 1.
CM-8	CM-8(a)(4)	CCI-000398	The organization defines information deemed necessary to achieve effective information system component accountability.	DoD has defined the information as hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information as hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name.	LOW		X	X	X	X			1.9.4 Control System Inventory Report		Cybersecurity design requires the contractor to document the inventory of components within the control system and submit a Control System Inventory Report. This design requirement is captured in Sub-Paragraph "Control System Inventory Report" within Part 1.
IA-3	IA-3	CCI-000777	The organization defines a list of specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system.	DoD has defined the value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	LOW	X	X		X	X			1.9.4 Control System Inventory Report 3.2.7 Device Identification and Authentic...		Cybersecurity requirement is met by requiring the contractor to document the inventory of components within the control system and submit a Control System Inventory Report. This design requirement is captured in Sub-Paragraph "Control System Inventory Report" within Part 1 and "Device Identification and Authentication" within Part 3
IA-3	IA-3	CCI-000778	The information system uniquely identifies an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.	The organization being inspected/assessed configures the network infrastructure to identify all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 778. DoD has defined the value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	The organization conducting the inspection/assessment examine a sampling of the network infrastructure device configurations to ensure devices connecting to the infrastructure are uniquely identified. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 778.	LOW	X	X		X				1.9.4 Control System Inventory Report 3.2.7 Device Identification and Authentic...		Cybersecurity requirement is met by requiring the contractor to document the inventory of components within the control system and submit a Control System Inventory Report. This design requirement is captured in Sub-Paragraph "Control System Inventory Report" within Part 1 and "Device Identification and Authentication" within Part 3
IA-3	IA-3	CCI-001958	The information system authenticates an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.	The organization being inspected/assessed configures the network infrastructure to authenticate all mobiles devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1958. DoD has defined the value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	The organization conducting the inspection/assessment examine a sampling of the network infrastructure device configurations to ensure devices connecting to the infrastructure are uniquely authenticated. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1958.	LOW	X	X		X				1.9.4 Control System Inventory Report 3.2.7 Device Identification and Authentic...		Cybersecurity requirement is met by requiring the contractor to identify and document all components within the control system through the Control System Inventory Report. This CCI is further enforced through requiring the contractor to provide 802.1x capable switches when design requires switches. This design requirement is captured in Sub-Paragraph "Control System Inventory Report" within Part 1 and Device Identification and Authentication within Part 3

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-17	CCI-002773	The organization defines the fail-safe procedures to be implemented by the information system when organization defined failure conditions occur.	The organization being inspected/assessed defines and documents the fail-safe procedures to be implemented by the information system when organization-defined failure conditions occur. DoD has determined the fail-safe procedures are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented fail-safe procedures to ensure the organization being inspected/assessed defines the fail-safe procedures to be implemented by the information system when organization-defined failure conditions occur. DoD has determined the fail-safe procedures are not appropriate to define at the Enterprise level.	LOW		X						1.9.4 Control System Inventory Report 3.8 SAFE MODE AND FAIL SAFE OPERATION		Cybersecurity design requires the contractor to document the inventory of components within the control system and submit a Control System Inventory Report. This design requirement is captured in Sub-Paragraphs "Control System Inventory Report" within Part 1 and "SAFE MODE AND FAIL SAFE OPERATION" within Part 3
N/A	SI-17	CCI-002774	The organization defines the failure conditions which, when they occur, will result in the information system implementing organization-defined fail-safe procedures.	The organization being inspected/assessed defines and documents the failure conditions which, when they occur, will result in the information system implementing organization-defined fail-safe procedures. DoD has determined the failure conditions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented failure conditions to ensure the organization being inspected/assessed defines the failure conditions which, when they occur, will result in the information system implementing organization-defined fail-safe procedures. DoD has determined the failure conditions are not appropriate to define at the Enterprise level.	LOW		X						1.9.4 Control System Inventory Report 3.8 SAFE MODE AND FAIL SAFE OPERATION		Cybersecurity design requires the contractor to document the inventory of components within the control system and submit a Control System Inventory Report. This design requirement is captured in Sub-Paragraphs "Control System Inventory Report" within Part 1 and "SAFE MODE AND FAIL SAFE OPERATION" within Part 3
N/A	SI-17	CCI-002775	The information system implements organization-defined fail-safe procedures when organization-defined failure conditions occur.	The organization being inspected/assessed configures the information system to implement fail-safe procedures defined in SI-17, CCI 2773 when failure conditions defined in SI-17, CCI 2774 occur. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2775.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement fail-safe procedures defined in SI-17, CCI 2773 when failure conditions defined in SI-17, CCI 2774 occur. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2775.	LOW		X						1.9.4 Control System Inventory Report 3.8 SAFE MODE AND FAIL SAFE OPERATION		Cybersecurity design requires the contractor to document the inventory of components within the control system and submit a Control System Inventory Report. This design requirement is captured in Sub-Paragraphs "Control System Inventory Report" within Part 1 and "SAFE MODE AND FAIL SAFE OPERATION" within Part 3
N/A	CP-10	CCI-000550	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption.	The organization being inspected/assessed provides automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a disruption. The organization must identify the selected method in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it identifies the recovery and reconstitution method for its information system to a known state after a disruption.	LOW	X	X	X					1.9.5 Software and Configuration Backups		Cybersecurity Requirements are met by requiring the contractor to submit a "Software and Configuration Backups" report with Part 1
N/A	CP-10	CCI-000551	The organization provides for the recovery and reconstitution of the information system to a known state after a compromise.	The organization being inspected/assessed provides automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a compromise. The organization must identify the selected method in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it identifies the recovery and reconstitution method for its information system to a known state after a compromise.	LOW	X	X	X					1.9.5 Software and Configuration Backups		Cybersecurity Requirements are met by requiring the contractor to submit a "Software and Configuration Backups" report with Part 1
N/A	CP-10	CCI-000552	The organization provides for the recovery and reconstitution of the information system to a known state after a failure.	The organization being inspected/assessed provides automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a failure. The organization must identify the selected method in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it identifies the recovery and reconstitution method for its information system to a known state after a failure.	LOW	X	X	X					1.9.5 Software and Configuration Backups		Cybersecurity Requirements are met by requiring the contractor to submit a "Software and Configuration Backups" report with Part 1
N/A	PL-2(a)(2)	CCI-003051	The organization's security plan for the information system explicitly defines the authorization boundary for the system.	The organization being inspected/assessed explicitly defines within the security plan the authorization boundary for the system.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed explicitly defines within the security plan the authorization boundary for the system.	LOW	X	X	X					1.9.6 Cybersecurity Riser Diagram		Cybersecurity Requirements are met by requiring the contractor to submit a "Cybersecurity Riser Diagram" report with Part 1
N/A	PL-2(a)(4)	CCI-003053	The organization's security plan for the information system provides the security categorization of the information system including supporting rationale.	The organization being inspected/assessed defines within the security plan the security categorization of the information system including supporting rationale.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed defines within the security plan the security categorization of the information system including supporting rationale.	LOW		X	X					1.9.6 Cybersecurity Riser Diagram		Cybersecurity Requirements are met by requiring the contractor to submit a "Cybersecurity Riser Diagram" report with Part 1
N/A	AC-8(c)(1)	CCI-001384	The information system, for publicly accessible systems, displays system use information organization-defined conditions before granting further access.	The organization being inspected/assessed configures the information system to display the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," March 2013 before granting further access for publicly accessible systems For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1384. DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," March 2013.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," March 2013 before granting further access for publicly accessible systems For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1384. DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," March 2013.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS is not publically accessible."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-5(a)(1)	CCI-003126	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure operation of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure operation of the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure operation of the system, component, or service.	LOW		X	X					1.9.8 Control System Cybersecurity Docume...		Requirement is met in "Control System Cybersecurity Documentation"
N/A	AC-8(c)(2)	CCI-001385	The information system, for publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.	The organization being inspected/assessed configures the information system to display references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1385.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1385.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS is not publically accessible."	
N/A	AC-8(c)(2)	CCI-001386	The information system for publicly accessible systems displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.	The organization being inspected/assessed configures the information system to display references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1386.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1386.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS is not publically accessible."	
N/A	AC-8(c)(2)	CCI-001387	The information system for publicly accessible systems displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.	The organization being inspected/assessed configures the information system to display references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1387.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1387.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS is not publically accessible."	
N/A	AC-8(c)(3)	CCI-001388	The information system, for publicly accessible systems, includes a description of the authorized uses of the system.	The organization being inspected/assessed configures the information system to include a description of the authorized uses of the system for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1388.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to include a description of the authorized uses of the system for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1388.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS is not publically accessible."	
N/A	AT-1(a)	CCI-002048	The organization defines the personnel or roles to whom the security awareness and training policy is disseminated.	DoD has defined the roles as organizational personnel with security awareness and training responsibilities. DoD disseminates DoDD 8570.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with security awareness and training responsibilities.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-1(a)	CCI-002049	The organization defines the personnel or roles to whom the security awareness and training procedures are disseminated.	DoD has defined the roles as organizational personnel with security awareness and training responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with security awareness and training responsibilities.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AT-1(a)(1)	CCI-000100	The organization develops and documents a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. Comment: DoDD 8570.01 will be updated with DoDD 8140 once signed. The organization's use of their higher command policy/procedures meets this requirement if more stringent.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. Comment: The organization's use of their higher command policy/procedures meets this requirement if more stringent.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-1(a)(1)	CCI-000101	The organization disseminates a security awareness and training policy to organization-defined personnel or roles.	DoD disseminates DoDD 8570.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-1(a)(2)	CCI-000103	The organization develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	DoD develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls within DoDD 8570.01. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-1(a)(2)	CCI-000104	The organization disseminates security awareness and training procedures to organization-defined personnel or roles.	DoD disseminates DoDD 8570.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. DoD has defined the roles as organizational personnel with security awareness and training responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. DoD has defined the roles as organizational personnel with security awareness and training responsibilities.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-1(b)(1)	CCI-000102	The organization reviews and updates the current security awareness and training policy in accordance with organization-defined frequency.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-1(b)(1)	CCI-001564	The organization defines the frequency of security awareness and training policy reviews and updates.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-1(b)(2)	CCI-000105	The organization reviews and updates the current security awareness and training procedures in accordance with organization-defined frequency.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. DoD has defined the frequency as annually.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-1(b)(2)	CCI-001565	The organization defines the frequency of security awareness and training procedure reviews and updates.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-2	CCI-001480	The organization defines the frequency for providing refresher security awareness training to all information system users (including managers, senior executives, and contractors).	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level (DoDD 8570.01). DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AT-2(a)	CCI-000106	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-2(b)	CCI-000112	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) when required by information system changes.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-2(c)	CCI-001479	The organization provides refresher security awareness training to all information system users (including managers, senior executives, and contractors) in accordance with the organization-defined frequency.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-3(a)	CCI-000108	The organization provides role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the information system or performing assigned duties	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT for privileged users is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT for privileged users is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-3(b)	CCI-000109	The organization provides role-based security training to personnel with assigned security roles and responsibilities when required by information system changes.	Privileged user type Security-related education/training available through DISA IASE (e.g. VTE, Skill Soft, other professional sources) meets the provision of this control. The organization being inspected/assessed may define specific requirements within the above listed sources for their personnel.	The organization conducting the inspection/assessment obtains and examines documented records (IAW AT-4) of their privileged users training.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-3(c)	CCI-000110	The organization provides refresher role-based security training to personnel with assigned security roles and responsibilities in accordance with organization-defined frequency.	Privileged user type Security-related education/training available through DISA IASE (e.g. VTE, Skill Soft, other professional sources) meets the provision of this control. The organization being inspected/assessed may define specific requirements within the above listed sources for their personnel.	The organization conducting the inspection/assessment obtains and examines documented records (IAW AT-4) of their privileged users training.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-3(c)	CCI-000111	The organization defines a frequency for providing refresher role-based security training.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-4(a)	CCI-000113	The organization documents individual information system security training activities, including basic security awareness training and specific information system security training.	The organization being inspected/assessed identifies and documents training activities to include basic security awareness training (per AT-2) and role-based security related training (per AT-3) IAW DoD 8570.01M.	The organization conducting the inspection/assessment obtains and examines the security awareness training activities to ensure the organization being inspected/assessed documents training activities to include basic security awareness training (per AT-2) and role-based security related training (per AT-3) IAW DoD 8570.01M.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-4(a)	CCI-000114	The organization monitors individual information system security training activities, including basic security awareness training and specific information system security training.	The organization being inspected/assessed maintains and monitors records identifying personnel who have received training and the date the training was received	The organization conducting the inspection/assessment obtains and examines records identifying personnel who have received training and the date the training was received	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-4(b)	CCI-001336	The organization retains individual training records for an organization-defined time period.	The organization being inspected/assessed will maintain records training records for at least 5 years or 5 years after completion of a specific training program. DoD has defined the frequency as at least 5 years or 5 years after completion of a specific training program.	The organization conducting the inspection/assessment obtains and examines training records to ensure records have been maintained for at least 5 years or 5 years after completion of a specific training program. DoD has defined the frequency as at least 5 years or 5 years after completion of a specific training program.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-4(b)	CCI-001337	The organization defines a time period for retaining individual training records.	DoD has defined the frequency as at least 5 years or 5 years after completion of a specific training program.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least 5 years or 5 years after completion of a specific training program.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-1(a)	CCI-001930	The organization defines the organizational personnel or roles to whom the audit and accountability policy is to be disseminated.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO or ISSM, to whom the audit and accountability policy is to be disseminated. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles to whom the audit and accountability policy is to be disseminated to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-1(a)	CCI-001931	The organization defines the organizational personnel or roles to whom the audit and accountability procedures are to be disseminated.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO or ISSM, to whom the audit and accountability procedures are to be disseminated. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles to whom the audit and accountability procedures are to be disseminated to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-1(a)(1)	CCI-000117	The organization develops and documents an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization being inspected/assessed develops and documents an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization conducting the inspection/assessment obtains and examines the audit and accountability policy to ensure that the audit and accountability policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-1(a)(1)	CCI-001832	The organization disseminates the audit and accountability policy to organization-defined personnel or roles.	The organization being inspected/assessed disseminates, via an information sharing capibility, to the ISSO and ISSM and others as the local organization deems appropriate an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the audit and accountability procedures via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-1(a)(2)	CCI-000120	The organization develops and documents procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The organization conducting the inspection/assessment obtains and examines the audit and accountability procedures to ensure that the procedures facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-1(a)(2)	CCI-001834	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The organization being inspected/assessed disseminates, via an information sharing capibility, to the ISSO and ISSM and others as the local organization deems appropriate audit and accountability procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the audit and accountability procedures via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-1(b)(1)	CCI-000119	The organization reviews and updates the audit and accountability policy on an organization-defined frequency.	The organization being inspected/assessed reviews and updates the audit and accountability policy annually. The organization must maintain an audit trail of reviews and updates. Any changes or acceptance of the document without change must be captured in the audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the audit and accountability policy annually. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-1(b)(1)	CCI-001569	The organization defines the frequency on which it will review and update the audit and accountability policy.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-1(b)(2)	CCI-000122	The organization reviews and updates the audit and accountability procedures on an organization-defined frequency.	The organization being inspected/assessed reviews and updates the audit and accountability procedures annually. The organization must maintain an audit trail of reviews and updates. Any changes or acceptance of the document without change must be captured in the audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the audit and accountability procedures annually. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-1(b)(2)	CCI-001570	The organization defines the frequency on which it will review and update the audit and accountability procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-11	CCI-000167	The organization retains audit records for an organization defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	The organization being inspected/assessed will take action to ensure it retains audit records for 5 years for SAMI; otherwise for at least 1 year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. DoD has defined the time period as 5 years for SAMI; otherwise for at least 1 year.	The organization conducting the inspection/assessment reviews the information system audit records and any other relevant documents or records to ensure the organization being inspected/assessed retains its audit records for 5 years for SAMI; otherwise for at least 1 year. DoD has defined the time period as 5 years for SAMI; otherwise for at least 1 year.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-11	CCI-000168	The organization defines the time period for retention of audit records which is consistent with its records retention policy, to provide support for after-the-fact investigations of security incidents, and meet regulatory and organizational information retention requirements.	DoD has defined the time period as 5 years for SAMI; otherwise for at least 1 year.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 5 years for SAMI; otherwise for at least 1 year.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-5(a)(1)	CCI-003124	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure configuration of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.2.1 HVAC Control System Devices FULLY S... 1.9.8.2.2 All Other HVAC Control System Devic... 1.9.8.3.1 Lighting Control System Devices FUL... 1.9.8.3.2 All Other Lighting Control System D... 1.9.8.5 Default Requirements for Control Sy...		Requirement is met in "Control System Cybersecurity Documentation"
N/A	SA-5(a)(2)	CCI-003127	The organization obtains administrator documentation for the information system, system component, or information system services that describes effective use and maintenance of security functions/mechanisms.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe effective use and maintenance of security functions/mechanisms.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe effective use and maintenance of security functions/mechanisms.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.1 Software Applications 1.9.8.2.1 HVAC Control System Devices FULLY S... 1.9.8.2.2 All Other HVAC Control System Devic... 1.9.8.3.1 Lighting Control System Devices FUL... 1.9.8.3.2 All Other Lighting Control System D... 1.9.8.5 Default Requirements for Control Sy...		Requirement is met in "Control System Cybersecurity Documentation"
N/A	SA-5(b)(2)	CCI-003130	The organization obtains user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.1 Software Applications 1.9.8.2.1 HVAC Control System Devices FULLY S... 1.9.8.2.2 All Other HVAC Control System Devic... 1.9.8.3.1 Lighting Control System Devices FUL... 1.9.8.3.2 All Other Lighting Control System D... 1.9.8.5 Default Requirements for Control Sy...		Requirement is met in "Control System Cybersecurity Documentation"
N/A	SA-5(a)(3)	CCI-003128	The organization obtains administrator documentation for the information system, system component, or information system services that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.1 Software Applications 1.9.8.2.1 HVAC Control System Devices FULLY S... 1.9.8.3.1 Lighting Control System Devices FUL... 1.9.8.5 Default Requirements for Control Sy...		Requirement is met in "Control System Cybersecurity Documentation"
N/A	SA-5(b)(1)	CCI-003129	The organization obtains user documentation for the information system, system component, or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide user documentation for the information system, system component or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.1 Software Applications 1.9.8.2.1 HVAC Control System Devices FULLY S... 1.9.8.3.1 Lighting Control System Devices FUL... 1.9.8.5 Default Requirements for Control Sy...		Requirement is met in "Control System Cybersecurity Documentation"

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-5(a)(1)	CCI-003125	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure installation of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure installation of the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure installation of the system, component, or service.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.5 Default Requirements for Control Sy...		Requirement is met in "Control System Cybersecurity Documentation"
N/A	SA-5(b)(3)	CCI-003131	The organization obtains user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.1 Software Applications		Requirement is met in "Control System Cybersecurity Documentation"
N/A	AU-2(b)	CCI-000124	The organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.	The organization being inspected/assessed documents and implements within the audit and accountability policy and procedures, a process to coordinate the additional auditable events. The objective is to enhance mutual support and to help guide the selection of auditable events. The organization must maintain artifacts of the coordination.	The organization conducting the inspection/assessment obtains and examines the audit and accountability policy and procedures as well as artifacts of the coordination to determine if coordination is necessary and if necessary, whether it has been performed.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-11	CCI-002955	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to long-term alternate power in the event of a primary power source loss.	The organization being inspected/assessed implements an uninterruptible power supply with sufficient capacity to support orderly shutdown of the system or transition the system to long-term alternate power in the event of a primary power source loss.	The organization conducting the inspection/assessment obtains and examines documentation identifying the capacity of the implemented uninterruptible power supply, documentation identifying the power requirements of the system, and documentation identifying the contingency plan in the event of primary power source loss to ensure the organization being inspected/assessed provides uninterruptible power supply with sufficient capacity to support orderly shutdown of the system or transition the system to long-term alternate power in the event of a primary power source loss.	LOW	X	X		X			NIST 800-53 does not have this in a LOW baseline. NIST 800-82 included it with the rationale "ICS may support critical activities....". By definition, a CS supporting "critical activities" is not a LOW system.	3.10 DEVICE POWER		CCI requirements are addressed within subparagraph "Device Power" of UFGS 25 05 11.
N/A	AU-2(d)	CCI-000126	The organization determines that the organization-defined subset of the auditable events defined in AU-2 are to be audited within the information system.	The organization conducting the inspection/assessment reviews the documented audit process as well as audit logs to ensure that the organization being inspected/assessed audits all auditable events defined in AU-2 (a) per occurrence. DoD has defined the actions as all auditable events defined in AU-2 (a) per occurrence.	The organization conducting the inspection/assessment reviews the documented audit process as well as audit logs to ensure that the organization being inspected/assessed audits all auditable events defined in AU-2 (a) per occurrence. DoD has defined the actions as all auditable events defined in AU-2 (a) per occurrence.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-2(d)	CCI-001484	The organization defines frequency of (or situation requiring) auditing for each identified event.	DoD has defined the frequency as all auditable events defined in AU-2 (a) per occurrence.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as all auditable events defined in AU-2 (a) per occurrence.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PE-11(1)	CCI-000961	The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	The organization being inspected/assessed will: 1. implement alternate power supply capable of supporting minimal operational capability over the long term. 2. Provide a list of physical IT assets within the boundary of the information system that require a long term alternate power supply. This list may come from the inspected organization's security plan, continuity plan, or other documentation.	The organization conducting the inspection/assessment obtains and examines the list of physical IT assets within the boundary of the information system that require a long term alternate power supply. Physically inspect a sample from the list to ensure that long term power supply capability supporting minimal operational capability has been provided.	LOW	X	X					NIST 800-53 does not have this in a LOW baseline. NIST 800-82 included it with the rationale "ICS may support critical activities....". By definition, a CS supporting "critical activities" is not a LOW system.	3.10 DEVICE POWER		CCI requirements are addressed within subparagraph "Device Power" of UFGS 25 05 11.
RA-5	RA-5(a)	CCI-001054	The organization scans for vulnerabilities in the information system and hosted applications on an organization-defined frequency.	The organization being inspected/assessed will define, document, and implement procedures for vulnerability scans of the information system and hosted applications; and scan for vulnerabilities in the information system and hosted applications every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). This control is not targeted at security control compliance scanning. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines the organization's vulnerability scanning procedures and results for the 90 days preceding the inspection/assessment. If the system in question has not been operational for more than 90 days the organization will provide all available scan(s).	LOW	X	X	X					3.11 VULNERABILITY SCANNING		CCI requirements are addressed within subparagraph "VULNERABILITY SCANNING" of UFGS 25 05 11.
RA-5	RA-5(a)	CCI-001055	The organization defines a frequency for scanning for vulnerabilities in the information system and hosted applications.	DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	LOW	X	X		X	X			3.11 VULNERABILITY SCANNING		CCI requirements are addressed within subparagraph "VULNERABILITY SCANNING" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
RA-5	RA-5(a)	CCI-001641	The organization defines the process for conducting random vulnerability scans on the information system and hosted applications.	DoD has defined the requirement for vulnerability scanning periodicity of every 30 days. If the organization being inspected/assessed has determined a requirement for random scanning they must document that process. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines random vulnerability process documentation (if applicable) to validate the organization has clearly defined and documented a process for conducting random vulnerability scans on the information system and hosted applications. If the organization being inspected/assessed has determined they have no requirement for random scanning, there is no requirement for a process.	LOW	X	X	X	X				3.11 VULNERABILITY SCANNING		CCI requirements are addressed within subparagraph "VULNERABILITY SCANNING" of UFGS 25 05 11.
RA-5	RA-5(a)	CCI-001643	The organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined process for random scans.	The organization being inspected/assessed will conduct random vulnerability scans every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs). The organization will document the vulnerability scans as an audit trail for future reference. The audit trail must be maintained IAW DoD, CYBERCOM, or component policies. DoD has defined the frequency as every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs). .	The organization conducting the inspection/assessment obtains and examines the vulnerability scanning results every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs) to verify compliance with the organization being inspected/assessed random vulnerability scanning process. DoD has defined the frequency as every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs).	LOW	X	X	X					3.11 VULNERABILITY SCANNING		CCI requirements are addressed within subparagraph "VULNERABILITY SCANNING" of UFGS 25 05 11.
RA-5	RA-5(b)	CCI-001057	The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: enumerating platforms, software flaws, and improper configurations; formatting checklists and test procedures; and measuring vulnerability impact.	The organization being inspected/assessed employs the DoD Enterprise scanning tool.	The organization conducting the inspection/assessment obtains and examines the software list or vulnerability scanning procedures to ensure the organization being inspected/assessed employs the DoD Enterprise scanning tool.	LOW	X	X	X	X				3.11 VULNERABILITY SCANNING		CCI requirements are addressed within subparagraph "VULNERABILITY SCANNING" of UFGS 25 05 11.
RA-5	RA-5(c)	CCI-001058	The organization analyzes vulnerability scan reports and results from security control assessments.	The organization being inspected/assessed analyzes vulnerability scan reports and security control assessment results with the intent of identifying legitimate vulnerabilities and the relationship between vulnerabilities and security controls.	The organization conducting the inspection/assessment will interview organizational personnel with security control assessment and vulnerability scanning responsibilities. The purpose of the reviews and interviews is to validate the organization is conducting an analysis of the vulnerability scan reports and results from the security control assessments.	LOW	X	X	X					3.11 VULNERABILITY SCANNING		CCI requirements are addressed within subparagraph "VULNERABILITY SCANNING" of UFGS 25 05 11.
RA-5	RA-5(d)	CCI-001059	The organization remediates legitimate vulnerabilities in organization-defined response times in accordance with an organizational assessment risk.	The organization being inspected/assessed takes corrective actions as appropriate on legitimate vulnerabilities identified in RA-5, CCI 001058 IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). Audit records of actions must be maintained IAW applicable DoD, CYBERCOM, and/or component policies. DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines audit records to validate the organization is taking action to remediate legitimate vulnerabilities within the required response times (IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). The organization conducting the inspection/assessment may conduct independent vulnerability scans to compare those scan results with audit records of remediation actions. DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	LOW	X	X	X	X				3.11 VULNERABILITY SCANNING		CCI requirements are addressed within subparagraph "VULNERABILITY SCANNING" of UFGS 25 05 11.
N/A	SA-4(10)	CCI-003116	The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.	The organization being inspected/assessed employs DoD approved PKI tokens for identity verification.	The organization conducting the inspection/assessment examines the information system to ensure DoD approved PKI tokens are implemented for identity verification.	LOW	X	X		X				3.12 FIPS 201-2 REQUIREMENT		CCI requirements are addressed within subparagraph "FIPS 201-2 Requirement" of UFGS 25 05 11.
N/A	AU-4(1)	CCI-001850	The organization defines the frequency on which the information system off-loads audit records onto a different system or media than the system being audited.	DoD has defined the frequency as at a minimum, real-time for interconnected systems and weekly for stand-alone systems.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at a minimum, real-time for interconnected systems and weekly for stand-alone systems.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-4(1)	CCI-001851	The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.	The organization being inspected/assessed configures the information system to off-load audit records at a minimum, in real-time for interconnected systems and weekly for stand-alone systems onto a different system or media than the system being audited. DoD has defined the frequency as at a minimum, real-time for interconnected systems and weekly for stand-alone systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1851.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to off-load audit records at a minimum, in real-time for interconnected systems and weekly for stand-alone systems onto a different system or media than the system being audited. DoD has defined the frequency as at a minimum, real-time for interconnected systems and weekly for stand-alone systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1851.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-3(c)(1)	CCI-001241	The organization configures malicious code protection mechanisms to perform periodic scans of the information system on an organization defined frequency.	The organization being inspected/assessed configures malicious code protection mechanisms to perform periodic scans of the information system on every 7 days. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1241. DoD has defined the frequency as every 7 days.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform periodic scans of the information system on every 7 days. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1241. DoD has defined the frequency as every 7 days.	LOW	X	X	X					3.13.1 Malicious Code Protection	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-5(a)	CCI-001572	The organization defines the personnel or roles to be alerted in the event of an audit processing failure.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the SCA and ISSO, who shall be alerted in the event of audit processing failure. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as at a minimum, the SCA and ISSO.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles who should be alerted in the event of audit processing failure to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles. DoD has defined the personnel or roles as at a minimum, the SCA and ISSO.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-3(c)(1)	CCI-002623	The organization defines the frequency for performing periodic scans of the information system for malicious code.	DoD has defined the frequency as every 7 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 7 days.	LOW		X		X	X			3.13.1 Malicious Code Protection	FRCS has no computers	
SI-4	SI-4(a)(1)	CCI-001253	The organization defines the objectives of monitoring for attacks and indicators of potential attacks on the information system.	DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	LOW	X	X		X	X			3.13.3 Information System Monitoring	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-6(a)	CCI-000148	The organization reviews and analyzes information system audit records on an organization defined frequency for indications of organization-defined inappropriate or unusual activity.	The organization being inspected/assessed documents and implements a process to review and analyze information system audit records every seven days or more frequently if required by an alarm event or anomaly for indications of activity defined in AU-6, CCI 1862. The organization must maintain an audit trail of the reviews. DoD has defined the frequency as every seven days or more frequently if required by an alarm event or anomaly.	The organization conducting the inspection/assessment obtains and examines the documented process for audit trail reviews as well as the audit trail showing the reviews to ensure the organization being inspected/assessed reviews and analyzes information system audit records every seven days or more frequently if required by an alarm event or anomaly for indications of activity defined in AU-6, CCI 1862. DoD has defined the frequency as every seven days or more frequently if required by an alarm event or anomaly.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-6(a)	CCI-000151	The organization defines the frequency for the review and analysis of information system audit records for organization-defined inappropriate or unusual activity.	DoD has defined the frequency as every seven days or more frequently if required by an alarm event or anomaly.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every seven days or more frequently if required by an alarm event or anomaly.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-6(a)	CCI-001862	The organization defines the types of inappropriate or unusual activity to be reviewed and analyzed in the audit records.	The organization being inspected/assessed defines and documents the types of inappropriate or unusual activity to be reviewed and analyzed in the audit records. DoD has determined that the types of inappropriate or unusual activity are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented types of inappropriate or unusual activity to ensure they have been defined. DoD has determined that the types of inappropriate or unusual activity are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-6(b)	CCI-000149	The organization reports any findings to organization-defined personnel or roles for indications of organization-defined inappropriate or unusual activity.	The organization being inspected/assessed documents and implements a process for reporting any findings of inappropriate or unusual activity as defined in AU-6, CCI 1862 to at a minimum, the ISSO and ISSM. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines the documented process for reporting findings as well as a sampling of historical reports to ensure the organization being inspected/assessed reports any findings of inappropriate or unusual activity as defined in AU-6, CCI 1862 to at a minimum, the ISSO and ISSM. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-6(b)	CCI-001863	The organization defines the personnel or roles to receive the reports of organization-defined inappropriate or unusual activity.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO and ISSM, who shall receive the reports of inappropriate or unusual activity defined in AU-6, CCI 1862. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles who should receive the reports of inappropriate or unusual activity defined in AU-6, CCI 1862 to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
SI-4	SI-4(b)	CCI-002645	The organization defines the techniques and methods to be used to identify unauthorized use of the information system.	The organization being inspected/assessed defines and documents the techniques and methods to be used to identify unauthorized use of the information system. DoD has determined the techniques and methods are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being inspected/assessed defines the techniques and methods to be used to identify unauthorized use of the information system. DoD has determined the techniques and methods are not appropriate to define at the Enterprise level.	LOW	X	X	X					3.13.3 Information System Monitoring	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-8(b)	CCI-001888	The organization defines the granularity of time measurement for time stamps generated for audit records.	DoD has defined the granularity of time measurement as one second.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the granularity of time measurement as one second.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
AC-18	AC-18(a)	CCI-001438	The organization establishes usage restrictions for wireless access.	The organization being inspected/assessed establishes and documents usage restrictions for wireless access.	The organization conducting the inspection/assessment obtains and examines documented usage restrictions to ensure the organization being inspected/assessed establishes usage restrictions for wireless access.	LOW		X	X					3.2.3 Wireless and Wired Broadcast Commun...		CCI requirements are addressed in "Wireless and Wired Broadcast Communication" subparagraph
AC-18	AC-18(a)	CCI-001439	The organization establishes implementation guidance for wireless access.	The organization being inspected/assessed establishes and documents implementation guidance for wireless access.	The organization conducting the inspection/assessment obtains and examines the documented implementation guidance to ensure the organization being inspected/assessed establishes implementation guidance for wireless access.	LOW		X	X					3.2.3 Wireless and Wired Broadcast Commun...		CCI requirements are addressed in "Wireless and Wired Broadcast Communication" subparagraph
N/A	AU-9	CCI-000162	The information system protects audit information from unauthorized access.	The organization being inspected/assessed configures the information system to disallow unauthorized access to audit information. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 162.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized access to audit information. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 162.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-9	CCI-000163	The information system protects audit information from unauthorized modification.	The organization being inspected/assessed configures the information system to disallow unauthorized modification of audit information. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 163.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized modification of audit information. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 163.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-9	CCI-000164	The information system protects audit information from unauthorized deletion.	The organization being inspected/assessed configures the information system to disallow unauthorized deletion of audit information. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 164.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized deletion of audit information. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 164.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-9	CCI-001493	The information system protects audit tools from unauthorized access.	The organization being inspected/assessed configures the information system to disallow unauthorized access to audit tools. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1493.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized access to audit tools. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1493.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-9	CCI-001494	The information system protects audit tools from unauthorized modification.	The organization being inspected/assessed configures the information system to disallow unauthorized modification of audit tools. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1494.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized modification of audit tools. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1494.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-9	CCI-001495	The information system protects audit tools from unauthorized deletion.	The organization being inspected/assessed configures the information system to disallow unauthorized deletion of audit tools. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1495.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized deletion of audit tools. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1495.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system… The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CA-1(a)	CCI-002061	The organization defines the personnel or roles to whom security assessment and authorization policy is to be disseminated.	DoD has defined the personnel or roles as all personnel. DoD disseminates DoDI 8510.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/ins1.html	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-1(a)	CCI-002062	The organization defines the personnel or roles to whom the security assessment and authorization procedures are to be disseminated.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-1(a)(1)	CCI-000239	The organization develops and documents a security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01.	LOW			X		X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-1(a)(1)	CCI-000240	The organization disseminates to organization-defined personnel or roles a security assessment and authorization policy.	DoD disseminates DoDI 8510.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/ins1.html	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-1(a)(2)	CCI-000242	The organization develops and documents procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.	The organization being inspected/assessed develops and documents, IAW DoDI 8510.01, procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.	The organization conducting the inspection/assessment obtains and examines the procedures to ensure the organization being inspected/assessedd evelops and documents procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls IAW DoDI 8510.01	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-1(a)(2)	CCI-000243	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.	The organization being inspected/assessed will require all personnel to register at the DTIC website to receive update notifications to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls. DoD has defined the personnel or roles as all personnel.	The organization conducting the inspection/assessment obtains and examines the AUP (Acceptable Use Policy), appointment orders, or written policy requiring that all personnel register at the DTIC website to receive update notifications. DoD has defined the personnel or roles as all personnel.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-1(b)(1)	CCI-000238	The organization defines the frequency to review and update the current security assessment and authorization policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CA-1(b)(1)	CCI-000241	The organization reviews and updates the current security assessment and authorization policy in accordance with organization-defined frequency.	DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CA-1(b)(2)	CCI-000244	The organization reviews and updates the current security assessment and authorization procedures in accordance with organization-defined frequency.	The organization being inspected/assessed reviews and updates, IAW DoDI 8510.01, the current security assessment and authorization procedures annually. The organization must maintain an audit trail of review and update activity. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of review and update activity to ensure the organization being inspected/assessed reviews and updates, IAW DoDI 8510.01, the current security assessment and authorization procedures annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-1(b)(2)	CCI-001578	The organization defines the frequency to review and update the current security assessment and authorization procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CA-2(a)	CCI-000245	The organization develops a security assessment plan for the information system and its environment of operation. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will document these security assessment plan requirements as part of the DoD approved Security Plan. Security plan templates are provided through eMASS and the Knowledge Service. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment obtains and examines the Security Plan to validate *security assessment blocks* are complete.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-2(a)(1)	CCI-000246	The organization's security assessment plan describes the security controls and control enhancements under assessment. IG&VP WG Note *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will ensure the Security Plan identifies the security controls and control enhancements under assessment. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment obtains the security assessment plan to verify the plan identifies the security controls and those control enhancements under assessment.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-2(a)(2)	CCI-000247	The organization's security assessment plan describes assessment procedures to be used to determine security control effectiveness. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The implementation guidance and validation procedures posted on the Knowledge Service constitutes assessment procedures for DoD. If organizations being inspected/assessed use assessment procedures other than those posted on the Knowledge Service, those procedures must be documented. *Comment* The items required within this CCI are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	DoD components are automatically compliant with this CCI if using the implementation guidance and validation procedures on the Knowledge Service. If the organization being inspected/assessed is using alternative implementation guidance and validation procedures, the organization conducting the inspection/assessment will obtain and examine those procedures.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CA-2(a)(3)	CCI-000248	The organization's security assessment plan describes assessment environment. *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will provide a description of the authorization boundary in their Security Plan. Authorization boundary can be described via one or more of the following: network diagrams, data flow diagrams, system design documents, or a list of information system components. Authorization boundary as defined in CNSSI 4009. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment obtains and examines the organization's authorization boundary. Authorization boundary can be described via one or more of the following: network diagrams, data flow diagrams, system design documents, or a list of information system components.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-2(a)(3)	CCI-002070	The organization's security assessment plan describes assessment team, assessment roles and responsibilities.	The organization being inspected/assessed lists their assessment team members and their associated assessment roles and responsibilities in the security assessment plan.	The organization conducting the inspection/assessment obtains and examines the security assessment plan to ensure the organization being inspected/assessed lists their assessment team members and their associated assessment roles and responsibilities in the security assessment plan.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-2(b)	CCI-000251	The organization assesses, on an organization-defined frequency, the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	In accordance with DoD's published guidance, the organization being inspected/assessed will utilize the implementation guidance and validation procedures published on the Knowledge Service to evaluate the implementation status of the applicable controls. DoD has defined the frequency as annually for technical controls, annually for a portion of management and operational controls, such that all are reviewed in a 3 year period, except for those requiring more frequent review as defined in other site or overarching policy. (NOTE: Technical, Management and Operational is IAW NIST SP 800-53 Table 1-1). *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	See CA-2 c "The organization conducting the inspection/assessment obtains and examines the security assessment report to verify that it includes the compliance/non-compliance status of all controls and specific deficiencies for all non-compliant controls."	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CA-2(b)	CCI-000252	The organization defines the frequency on which the security controls in the information system and its environment of operation are assessed. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	DoD has defined the frequency as annually for technical controls, annually for a portion of management and operation controls such that all are reviewed in a 3 year period except for those requiring more frequent review as defined in other site or overarching policy. NOTE: Technical, Management and Operational is IAW NIST SP 800-53 Table 1-1. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually for technical controls, annually for a portion of management and operation controls such that all are reviewed in a 3 year period except for those requiring more frequent review as defined in other site or overarching policy. NOTE: Technical, Management and Operational is IAW NIST SP 800-53 Table 1-1.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CA-2(c)	CCI-000253	The organization produces a security assessment report that documents the results of the assessment against the information system and its environment of operation. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will develop a SAR that includes the compliance/non-compliance status of all controls and specific deficiencies for all non-compliant controls using the template available on the Knowledge Service. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment obtains and examines the SAR to verify that it includes the compliance/non-compliance status of all controls and specific deficiencies for all non-compliant controls.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-2(d)	CCI-000254	The organization provides the results of the security control assessment against information system and its environment of operation to organization-defined individuals or roles. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will provide the SAR to at a minimum, the ISSO and ISSM. DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment interviews at a minimum, the ISSO and ISSM to ensure the SAR has been received. DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-2(d)	CCI-002071	The organization defines the individuals or roles to whom the results of the security control assessment is to be provided.	DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CA-3(a)	CCI-000257	The organization authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements.	The organization being inspected/assessed will develop and certify, by appropriate signatures (e.g. AO, network managers), Interconnection Security Agreements (e.g., MOU, MOA, SLA) authorizing the connection of its information systems to other information systems. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	The organization conducting the inspection/assessment obtains and examines documentation of the Interconnection Security Agreements to include appropriate signatures. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
AC-18	AC-18(a)	CCI-002323	The organization establishes configuration/connection requirements for wireless access.	The organization being inspected/assessed establishes and documents configuration/connection requirements for wireless access.	The organization conducting the inspection/assessment obtains and examines the documented configuration/connection requirements to ensure the organization being inspected/assessed establishes configuration/connection requirements for wireless access.	LOW		X	X					3.2.3 Wireless and Wired Broadcast Commun...		CCI is addressed within "Wireless and Wired Broadcast Communication"
N/A	CA-3(b)	CCI-000259	The organization documents, for each interconnection, the security requirements.	The organization being inspected/assessed will, for each interconnection, identify and document any additional security controls to be implemented to protect the confidentiality, integrity, and availability of the connected systems and the data passing between them. Controls should be appropriate for the systems to be connected and the environment in which the interconnection will operate. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	The organization conducting the inspection/assessment obtains and examines interconnection security agreement documentation, specifically looking at any additional security controls identified for implementation. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CA-3(b)	CCI-000260	The organization documents, for each interconnection, the nature of the information communicated.	The organization being inspected/assessed will document in the interconnection security agreement the type of information being transferred/transmitted. Characteristics will include but are not limited to: classification, information type (e.g. PII, HIPAA, FOUO, financial data, etc.) Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	The organization conducting the inspection/assessment obtains and examines the interconnection security agreement documentation, specifically to identify the type of information being transferred/transmitted. Characteristics will include but are not limited to: classification, information type (e.g. PII, HIPAA, FOUO, financial data, etc.) Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system… The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CA-3(c)	CCI-002083	The organization reviews and updates Interconnection Security Agreements on an organization-defined frequency.	The organization being inspected/assessed reviews and updates Interconnection Security Agreements at least annually. The organization must maintain an audit trail of reviews and updates. DoD has defined the frequency as at least annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates Interconnection Security Agreements at least annually. DoD has defined the frequency as at least annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-3(c)	CCI-002084	The organization defines the frequency that reviews and updates to the Interconnection Security Agreements must be conducted.	DoD has defined the frequency as at least annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CA-5(a)	CCI-000264	The organization develops a plan of action and milestones for the information system to document the organizations planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.	The organization being inspected/assessed will develop a security POA&M in accordance with DoDI 8510.01 Enclosure 6. POA&M templates are available on the Knowledge Service.	The organization conducting the inspection/assessment obtains and examines the security POA&M for compliance with DoDI 8510.01.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-5(b)	CCI-000265	The organization defines the frequency to update existing plan of action and milestones for the information system.	DoD has defined the frequency as at least every 90 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least every 90 days.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CA-5(b)	CCI-000266	The organization updates, on an organization-defined frequency, existing plan of action and milestones based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	The organization being inspected/assessed will update the POA&M at least every 90 days. The updates are to be based upon the assessment of the identified vulnerabilities and weaknesses, prioritization of the vulnerabilities and weaknesses, progress being made in addressing and resolving the security weaknesses and vulnerabilities found in programs and systems, and continuous monitoring activities. DoD has defined the frequency as at least every 90 days.	The organization conducting the inspection/assessment obtains and examines current POA&M. The objective is to validate the organization is providing updates to the POA&M at least every 90 days. Review of POA&M without change must be documented (i.e., adding review date to the POA&M header information). DoD has defined the frequency as at least every 90 days.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-6(a)	CCI-000270	The organization assigns a senior-level executive or manager as the authorizing official for the information system.	The organization being inspected/assessed will assign a senior-level executive or manager as the official role, and the responsibility, for authorizing the information system(s). Assignment must be in writing and IAW with DoDI 8510.01 (i.e. Appointment memorandum).	The organization conducting the inspection/assessment obtains and examines the written appointment memorandum.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-6(b)	CCI-000271	The organization ensures the authorizing official authorizes the information system for processing before commencing operations.	The organization being inspected/assessed will ensure that an authorization document (e.g. authorization to operate (ATO), interim authorization to operate (IATO)) has been issued by the authorizing official (AO) prior to placing the information system into an operational status.	The organization conducting the inspection/assessment obtains and examines the authorization document to ensure the information system is authorized prior to being placed into operational status.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-6(c)	CCI-000272	The organization updates the security authorization on an organization-defined frequency.	The organization being inspected/assessed updates the security authorization at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates. DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.	The organization conducting the inspection/assessment obtains and examines the security authorization documentation to confirm the security authorization has been updated within the last three years, when there was a significant change to the system, or if there was a change to the environment in which the system operates. DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CA-6(c)	CCI-000273	The organization defines the frequency of updating the security authorization.	DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CA-7	CCI-000274	The organization develops a continuous monitoring strategy.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-7(a)	CCI-002087	The organization establishes and defines the metrics to be monitored for the continuous monitoring program.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-7(b)	CCI-002088	The organization establishes and defines the frequencies for continuous monitoring.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-7(b)	CCI-002089	The organization establishes and defines the frequencies for assessments supporting continuous monitoring.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-7(c)	CCI-000279	The organization implements a continuous monitoring program that includes ongoing security control assessments in accordance with the organizational continuous monitoring strategy.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-7(d)	CCI-002090	The organization implements a continuous monitoring program that includes ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-7(e)	CCI-002091	The organization implements a continuous monitoring program that includes correlation and analysis of security-related information generated by assessments and monitoring.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-7(f)	CCI-002092	The organization implements a continuous monitoring program that includes response actions to address results of the analysis of security-related information.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-7(g)	CCI-000280	The organization implements a continuous monitoring program that includes reporting the security status of organization and the information system to organization-defined personnel or roles on an organization-defined frequency.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-7(g)	CCI-000281	The organization defines the frequency to report the security status of organization and the information system to organization-defined personnel or roles.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-7(g)	CCI-001581	The organization defines personnel or roles to whom the security status of organization and the information system should be reported.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-9(a)	CCI-002101	The organization authorizes internal connections of organization-defined information system components or classes of components to the information system.	The organization being inspected/assessed authorizes internal connections of information system components defined in CA-9, CCI 2102 or classes of components to the information system. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes internal connections of information system components defined in CA-9, CCI 2102 or classes of components to the information system.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
AC-18	AC-18(b)	CCI-001441	The organization authorizes wireless access to the information system prior to allowing such connections.	The organization being inspected/assessed authorizes wireless access to the information system prior to allowing such connections. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes wireless access to the information system prior to allowing such connections.	LOW		X	X					3.2.3 Wireless and Wired Broadcast Commun...		CCI requirements are addressed in "Wireless and Wired Broadcast Communication" subparagraph
CM-6	CM-6(a)	CCI-001588	The organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for ensuring security configuration checklists reflect the most restrictive mode consistent with operational requirements. DoD Components are automatically compliant with this CCI because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for ensuring security configuration checklists reflect the most restrictive mode consistent with operational requirements. DoD Components are automatically compliant with this CCI because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	LOW		X	X	X	X			3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT... 3.2.3 IP Control Networks		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-7(1)(b)	CCI-001761	The organization defines the functions, ports, protocols and services within the information system that are to be disabled when deemed unnecessary and/or nonsecure.	The organization being inspected/assessed must define and document in the system security plan, the functions, ports, protocols and services within the information system that are to be disabled when deemed unnecessary. DoD has determined that it is not appropriate to define unnecessary functions, ports, protocols and service at the Enterprise level. Nonsecure functions, ports, protocols and services are defined in DoDI 8551.01.	The organization conducting the inspection/assessment obtains and examines the system security plan to ensure the organization being inspected/assessed defines the functions, ports, protocols and services within the information system that are to be disabled when deemed unnecessary. DoD has determined that it is not appropriate to define unnecessary functions, ports, protocols and service at the Enterprise level. Nonsecure functions, ports, protocols and services are defined in DoDI 8551.01.	LOW		X						3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT... 3.2.3 IP Control Networks		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.
N/A	CM-7(1)(b)	CCI-001762	The organization disables organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure.	The organization being inspected/assessed must disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure as defined in CM-7 (1), CCI 1761.	The organization conducting the inspection/assessment inspects the information system to ensure the organization being inspected/assessed disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure as defined in CM-7 (1), CCI 1761.	LOW		X		X				3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT... 3.2.3 IP Control Networks		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.
N/A	CM-1(a)	CCI-001821	The organization defines the organizational personnel or roles to whom the configuration management policy is to be disseminated.	DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(a)	CCI-001824	The organization defines the organizational personnel or roles to whom the configuration management procedures are to be disseminated.	DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	LOW			X		X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(a)(1)	CCI-000287	The organization develops and documents a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization being inspected/assessed develops and documents a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization conducting the inspection/assessment obtains and examines the configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(a)(1)	CCI-001822	The organization disseminates the configuration management policy to organization defined personnel or roles.	The organization being inspected/assessed disseminates a configuration management policy via an information sharing capability (e.g. portal, intranet, email, etc.) to all stakeholders in the configuration management process. DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	The organization conducting the inspection/assessment obtains and examines the configuration management policy via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(a)(2)	CCI-000290	The organization develops and documents procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(a)(2)	CCI-001825	The organization disseminates to organization defined personnel or roles the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization being inspected/assessed disseminates the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls via an information sharing capability (e.g. portal, intranet, email, etc.) to all stakeholders in the configuration management process. DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(b)(1)	CCI-000286	The organization defines a frequency to review and update the configuration management policies.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW			X		X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(b)(1)	CCI-000289	The organization reviews and updates, on an organization defined frequency, the configuration management policy.	The organization being inspected/assessed reviews and updates, annually, the configuration management policy. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the configuration management policy to ensure annual review and necessary updates are occurring. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-1(b)(2)	CCI-000292	The organization reviews and updates, on an organization defined frequency, the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization being inspected/assessed reviews and updates, annually, the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls to ensure annual review and necessary updates are occurring. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(b)(2)	CCI-001584	The organization defines the frequency to review and update configuration management procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW			X		X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(a)	CCI-001726	The organization uses software in accordance with contract agreements.	The organization being inspected/assessed uses software in accordance with contract agreements.	The organization conducting the inspection/assessment obtains and examines a sampling of contract agreements and supporting evidence concerning the usage of software to ensure compliance with the contract agreements.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(a)	CCI-001727	The organization uses software documentation in accordance with contract agreements.	The organization being inspected/assessed uses software documentation in accordance with contract agreements.	The organization conducting the inspection/assessment obtains and examines a sampling of contract agreements associated with software documentation and supporting evidence concerning the usage of software documentation to ensure compliance with contract agreements.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(a)	CCI-001728	The organization uses software in accordance with copyright laws.	The organization being inspected/assessed uses software in accordance with copyright laws.	The organization conducting the inspection/assessment obtains and examines supporting evidence concerning the usage of software to ensure compliance with copyright laws.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(a)	CCI-001729	The organization uses software documentation in accordance with copyright laws.	The organization being inspected/assessed uses software documentation in accordance with copyright laws.	The organization conducting the inspection/assessment obtains and examines supporting evidence concerning the usage of software documentation to ensure compliance with copyright laws.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(b)	CCI-001730	The organization tracks the use of software protected by quantity licenses to control copying of the software.	The organization being inspected/assessed tracks the use of software protected by quantity licenses to control copying of the software. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	The organization conducting the inspection/assessment obtains and examines the tracking records to ensure the organization being inspected/assessed tracks the use of software protected by quantity licenses to control copying of the software.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(b)	CCI-001731	The organization tracks the use of software documentation protected by quantity licenses to control distribution of the software documentation.	The organization being inspected/assessed tracks the use of software documentation protected by quantity licenses to control distribution of the software documentation. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	The organization conducting the inspection/assessment obtains and examines the tracking records to ensure the organization being inspected/assessed tracks the use of software documentation protected by quantity licenses to control distribution of the software documentation.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(b)	CCI-001802	The organization tracks the use of software documentation protected by quantity licenses to control copying of the software documentation.	The organization being inspected/assessed tracks the use of software documentation protected by quantity licenses to control copying of the software documentation. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	The organization conducting the inspection/assessment obtains and examines the tracking records to ensure the organization being inspected/assessed tracks the use of software documentation protected by quantity licenses to control copying of the software documentation.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(b)	CCI-001803	The organization tracks the use of software protected by quantity licenses to control distribution of the software.	The organization being inspected/assessed tracks the use of software protected by quantity licenses to control distribution of the software. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	The organization conducting the inspection/assessment obtains and examines the tracking records to ensure the organization being inspected/assessed tracks the use of software protected by quantity licenses to control distribution of the software.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(c)	CCI-001732	The organization controls the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	The organization being inspected/assessed reviews and authorizes in order to control the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. The organization must maintain an audit trail of peer-to-peer file sharing technology reviews and authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of peer-to-peer file sharing technology reviews and authorizations to ensure the organization being inspected/assessed controls the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-10(c)	CCI-001733	The organization documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	The organization being inspected/assessed documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	The organization conducting the inspection/assessment obtains and examines the documentation for the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system… The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CM-11(a)	CCI-001804	The organization defines the policies for governing the installation of software by users.	The organization being inspected/assessed must define policies governing the installation of software by users. DoD has determined the policies are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines policies governing the installation of software by users (e.g., user agreements, CM plan, etc.) to ensure the organization being inspected/assessed defines the policies for governing the installation of software by users. DoD has determined the policies are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-11(a)	CCI-001805	The organization establishes organization-defined policies governing the installation of software by users.	The organization being inspected/assessed documents their policies governing the installation of software by users (e.g., user agreements, CM plan, etc.).	The organization conducting the inspection/assessment obtains and examines documented policies governing the installation of software by users (e.g., user agreements, CM plan, etc.) to ensure the organization being inspected/assessed establishes policies governing the installation of software by users.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-11(b)	CCI-001806	The organization defines methods to be employed to enforce the software installation policies.	The organization being inspected/assessed must define and document the methods employed to enforce the software installation policies. DoD has determined the policies are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines documentation of the methods employed to ensure the organization being inspected/assessed defines methods to be employed to enforce the software installation policies. DoD has determined the policies are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-11(b)	CCI-001807	The organization enforces software installation policies through organization-defined methods.	The organization being inspected/assessed must enforce software installation policies as defined in CM-11, CCI 1804 through methods defined in CM-11, CCI 1806.	The organization conducting the inspection/assessment obtains and examines software installation policies defined in CM-11, CCI 1804 and inspects the methods defined in CM-11, CCI 1806 to verify they are properly implemented.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-11(c)	CCI-001808	The organization defines the frequency on which it will monitor software installation policy compliance.	DoD has defined the frequency as at least monthly.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least monthly.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-11(c)	CCI-001809	The organization monitors software installation policy compliance per organization-defined frequency.	The organization being inspected/assessed must monitor software installation policy compliance at least monthly. The organization must maintain audit trails of monitoring activity. DoD has defined the frequency as at least monthly.	The organization conducting the inspection/assessment obtains and examines the audit trails of monitoring activities to ensure the organization being inspected/assessed monitors software installation policy compliance at least monthly. DoD has defined the frequency as at least monthly.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
CM-2	CM-2	CCI-000293	The organization develops and documents a current baseline configuration of the information system.	The organization being inspected/assessed develops and documents a current baseline configuration of the information system.	The organization conducting the inspection/assessment obtains and examines the documented baseline configuration.	LOW		X						---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-2	CCI-000295	The organization maintains under configuration control, a current baseline configuration of the information system.	The organization being inspected/assessed maintains a current baseline configuration of the information system.	The organization conducting the inspection/assessment obtains and examines the current baseline to ensure the current configuration matches the current documented baseline.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-4	CCI-000333	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	The organization being inspected/assessed analyzes changes to the information system to determine potential security impacts prior to change implementation. The organization must maintain records of analysis of changes to the information system.	The organization conducting the inspection/assessment obtains and examines the records of analyses to ensure the organization is conducting a security impact analysis of changes to the information system(s) prior to their implementation.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
CM-7	CM-7(a)	CCI-000381	The organization configures the information system to provide only essential capabilities.	The organization being inspected/assessed documents in the security plan, essential capabilities which the information system must provide. The organization being inspected/assessed configures the information system to provide only those documented essential capabilities.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed has identified essential capabilities. The organization conducting the inspection/assessment inspects the information system to ensure that it provides only those documented essential capabilities.	LOW		X						3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT… 3.2.3 IP Control Networks		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.
CM-7	CM-7(b)	CCI-000380	The organization defines for the information system prohibited or restricted functions, ports, protocols, and/or services.	DoD has defined the information system prohibited or restricted functions, ports, protocols, and/or services as IAW DoDI 8551.01.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system prohibited or restricted functions, ports, protocols, and/or services as IAW DoDI 8551.01.	LOW		X						3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT… 3.2.3 IP Control Networks		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.
CM-7	CM-7(b)	CCI-000382	The organization configures the information system to prohibit or restrict the use of organization-defined functions, ports, protocols, and/or services.	The organization being inspected/assessed configures the information system to prohibit or restrict the use of functions, ports, protocols, and/or services IAW DoDI 8551.01. DoD has defined the information system prohibited or restricted functions, ports, protocols, and/or services as IAW DoDI 8551.01.	The organization conducting the inspection/assessment inspects the information system to ensure the organization being inspected/assessed prohibits or restricts the use of functions, ports, protocols, and/or services IAW DoDI 8551.01. DoD has defined the information system prohibited or restricted functions, ports, protocols, and/or services as IAW DoDI 8551.01.	LOW		X						3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT… 3.2.3 IP Control Networks		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-41	CCI-002544	The organization defines the information systems or information system components on which organization-defined connection ports or input/output devices are to be physically disabled or removed.	The organization being inspected/assessed defines and documents the information systems or information system components on which organization-defined connection ports or input/output devices are to be physically disabled or removed. DoD has determined the information systems or information system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information systems or information system components to ensure the organization being inspected/assessed defines the information systems or information system components on which organization-defined connection ports or input/output devices are to be physically disabled or removed. DoD has determined the information systems or information system components are not appropriate to define at the Enterprise level.	LOW	X	X	X					3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT... 3.2.3 IP Control Networks		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.
N/A	CM-6(b)	CCI-000366	The organization implements the security configuration settings.	The organization being inspected/assessed must develop and document a process for implementing DoD security configuration or implementation guidance (e.g. STIGs, NSA configuration guides, CTOs, DTMs etc.). DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, NSA configuration guides, CTOs, DTMs etc.).	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements DoD security configuration or implementation guidance (e.g. STIGs, NSA configuration guides, CTOs, DTMs etc.). The organization conducting the inspection/assessment tests a sampling of information system components to ensure they comply with the required settings. DoD has defined the security configuration checklists as DoD security configuration or implementation guidance	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-6(c)	CCI-000367	The organization identifies any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.	The organization being inspected/assessed documents in the security plan and POA&M, if applicable, the information system components as defined in CM-6, CCI 1755 which deviate from configuration settings, and which settings as defined in CM-6, CCI 1756.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed has documented deviations from configuration settings for information system components.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-6(c)	CCI-000368	The organization documents any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.	The organization being inspected/assessed documents in the security plan and POA&M, if applicable, all configurable information system components which deviate from configuration settings, and which settings as defined in CM-6, CCI 1756. DoD has defined the information system components as all configurable information system components.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed has documented deviations from configuration settings for information system components.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-6(c)	CCI-000369	The organization approves any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.	The organization being inspected/assessed manages and approves changes to the security plan documenting deviations IAW CM-3, CCI 314. The organization must maintain an audit trail of approved changes to the security plan.	The organization conducting the inspection/assessment obtains and examines the security plan and the audit trail of approved changes to ensure the deviations are approved IAW CM-3, CCI 314.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-41	CCI-002545	The organization defines the connection ports or input/output devices that are to be physically disabled or removed from organization-defined information systems or information system components.	The organization being inspected/assessed defines and documents the connection ports or input/output devices that are to be physically disabled or removed from organization-defined information systems or information system components. DoD has determined the connection ports or input/output devices are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented connection ports or input/output devices to ensure the organization being inspected/assessed defines the connection ports or input/output devices that are to be physically disabled or removed from organization-defined information systems or information system components. DoD has determined the connection ports or input/output devices are not appropriate to define at the Enterprise level.	LOW	X	X	X					3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT... 3.2.3 IP Control Networks		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.
N/A	CM-6(c)	CCI-001756	The organization defines the operational requirements on which the configuration settings for the organization-defined information system components are to be based.	The organization being inspected/assessed must define and document in the system security plan, the requirements which may deviate from the approved configuration settings on the information system components defined in CM-6, CCI 1755. DoD has determined that it is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the system security plan to ensure the organization being inspected/assessed defines the requirements which may deviate from the approved configuration settings on the information system components defined in CM-6, CCI 1755. DoD has determined that it is not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-6(d)	CCI-001502	The organization monitors changes to the configuration settings in accordance with organizational policies and procedures.	The organization being inspected/assessed develops and documents a process for monitoring changes to the configuration settings in accordance with organizational policies and procedures.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed monitors changes to the configuration settings in accordance with organizational policies and procedures.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-6(d)	CCI-001503	The organization controls changes to the configuration settings in accordance with organizational policies and procedures.	The organization being inspected/assessed develops and documents a process for controlling changes to the configuration settings in accordance with organizational policies and procedures.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed controls changes to the configuration settings in accordance with organizational policies and procedures.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-7(1)(a)	CCI-000384	The organization reviews the information system per organization defined frequency to identify unnecessary and nonsecure functions, ports, protocols, and services.	The organization being inspected/assessed documents and implements a process to review the information system every 30 days to identify unnecessary and nonsecure functions, ports, protocols, and services. The organization must maintain an audit trail of the reviews. DoD has defined the frequency as every 30 days.	The organization conducting the inspection/assessment obtains and examines the documented process and audit trail of reviews to ensure the organization being inspected/assessed reviews the information system every 30 days to identify unnecessary and nonsecure functions, ports, protocols, and services. DoD has defined the frequency as every 30 days.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-7(1)(a)	CCI-001760	The organization defines the frequency of information system reviews to identify unnecessary and/or nonsecure functions, ports, protocols, and services.	DoD has defined the frequency as every 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 30 days.	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-41	CCI-002546	The organization physically disables or removes organization-defined connection ports or input/output devices on organization-defined information systems or information system components.	The organization being inspected/assessed physically disables or removes connection ports or input/output devices defined in SC-41, CCI 2545 on information systems or information system components defined in SC-41, CCI 2544.	The organization conducting the inspection/assessment examines a sampling of devices to ensure the organization being inspected/assessed physically disables or removes connection ports or input/output devices defined in SC-41, CCI 2545 on information systems or information system components defined in SC-41, CCI 2544.	LOW		X		X				3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT… 3.2.3 IP Control Networks		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.
N/A	SC-13	CCI-002449	The organization defines the cryptographic uses, and type of cryptography required for each use, to be implemented by the information system.	DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography.	LOW	X	X		X	X		A LOW CS doesn't have any classified information	3.2.6 Cryptographic Protection	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-13	CCI-002450	The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	The organization being inspected/assessed configures the information system to implement, for, protection of classified information: NSA-approved cryptography; for provision of digital signatures and hashing: FIPS-validated cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2450. DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement, for, protection of classified information: NSA-approved cryptography; for provision of digital signatures and hashing: FIPS-validated cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2450. DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography.	LOW	X	X		X			A LOW CS doesn't have any classified information	3.2.6 Cryptographic Protection	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-7	CCI-000803	The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	The organization being inspected/assessed configures the information system to implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 803.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 803.	LOW	X	X		X				3.2.8 Cryptographic Module Authentication		Cybersecurity requirements are met in "Cryptographic Module Authentication"
AC-2	AC-2(a)	CCI-002110	The organization defines the information system account types that support the organizational missions/business functions.	The organization being inspected/assessed defines and documents the information system account types that support the organizational missions/business functions. DoD has determined the information system account types are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system account types to ensure the organization being inspected/assessed defines the information system account types that support the organizational missions/business functions. DoD has determined the information system account types are not appropriate to define at the Enterprise level.	LOW		X						3.3.1 User Accounts		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts" within Part 3
N/A	AC-3	CCI-000213	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	The organization being inspected/assessed configures the information system to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 213.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 213.	LOW		X						3.3.1 User Accounts		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts" within Part 3

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-2	CCI-000764	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	The organization being inspected/assessed configures the information system to uniquely identify and authenticate organiaztional users (or processes acting on behalf of organizational users). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 764.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 764.	LOW	X	X		X				3.3.1 User Accounts 3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION"within Part 3
N/A	CM-8(a)(3)	CCI-000395	The organization develops and documents an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting.	The organization being inspected/assessed documents inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting.	The organization conducting the inspection/assessment obtains and examines the documented inventory and examines a sampling of information system components to ensure inventory is at the level of granularity deemed necessary for tracking and reporting.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-7(a)	CCI-000043	The organization defines the maximum number of consecutive invalid logon attempts to the information system by a user during an organization-defined time period.	DoD has defined the maximum number as three.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the maximum number as three.	LOW		X		X	X			3.3.2 Unsuccessful Logon Attempts		Cybersecurity requirements are met for log in attempts within Sub-Paragraph "Unsuccessful Logon Attempts" within Part 3
N/A	CM-8(a)(4)	CCI-000399	The organization develops and documents an inventory of information system components that includes organization defined information deemed necessary to achieve effective information system component accountability.	The organization being inspected/assessed documents inventory of information system components that includes organization defined information deemed necessary to achieve effective information system component accountability.	The organization conducting the inspection/assessment obtains and examines the documented inventory and examines a sampling of information system components to ensure inventory includes organization defined information deemed necessary to achieve effective information system component accountability.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(b)	CCI-001779	The organization defines the frequency on which the information system component inventory is to be reviewed and updated	DoD has defined the frequency as at a minimum, annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at a minimum, annually.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(b)	CCI-001780	The organization reviews and updates the information system component inventory per organization-defined frequency.	The organization being inspected/assessed documents and implements a process to review and update the information system component inventory at a minimum, annually. The organization must maintain an audit trail of review and update activity. DoD has defined the frequency as at a minimum, annually.	The organization conducting the inspection/assessment obtains and examines the documented process for reviews and updates as well as the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the information system component inventory at a minimum, annually. DoD has defined the frequency as at a minimum, annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-1(a)(1)	CCI-000438	The organization develops and documents a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-1(a)(1)	CCI-000439	The organization disseminates a contingency planning policy to organization-defined personnel or roles.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html NIST disseminates NIST SP 800-34 via http://csrc.nist.gov/publications/PubsSPs.html	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-1(a)(1)	CCI-002825	The organization defines personnel or roles to whom the contingency planning policy is to be disseminated.	DoD has defined the personnel or roles as all stakeholders identified in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all stakeholders identified in the contingency plan.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-1(a)(2)	CCI-000441	The organization develops and documents procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-1(a)(2)	CCI-001597	The organization disseminates contingency planning procedures to organization-defined personnel or roles.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html NIST disseminates NIST SP 800-34 via http://csrc.nist.gov/publications/PubsSPs.html	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CP-1(a)(2)	CCI-002826	The organization defines personnel or roles to whom the contingency planning procedures are disseminated.	DoD has defined the personnel or roles as all stakeholders identified in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all stakeholders identified in the contingency plan.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-1(b)(1)	CCI-000437	The organization defines the frequency to review and update the current contingency planning policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-1(b)(1)	CCI-000440	The organization reviews and updates the current contingency planning policy in accordance with organization-defined frequency.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-1(b)(2)	CCI-001596	The organization defines the frequency to review and update the current contingency planning procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-1(b)(2)	CCI-001598	The organization reviews and updates the current contingency planning procedures in accordance with the organization-defined frequency.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-7(a)	CCI-000044	The information system enforces the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.	The organization being inspected/assessed configures the information system to limit invalid logon attempts by a user to three attempts during a 15 minute time period. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 44. DoD has defined the maximum number as three. DoD has defined the time period as 15 minutes.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to limit invalid logon attempts by a user to three attempts during a 15 minute time period. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 44. DoD has defined the maximum number as three. DoD has defined the time period as 15 minutes.	LOW		X						3.3.2 Unsuccessful Logon Attempts		Cybersecurity requirements are met for log in attempts within Sub-Paragraph "Unsuccessful Logon Attempts" within Part 3
N/A	AC-7(a)	CCI-001423	The organization defines the time period in which the organization-defined maximum number of consecutive invalid logon attempts occur.	DoD has defined the time period as 15 minutes.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 15 minutes.	LOW		X		X	X			3.3.2 Unsuccessful Logon Attempts		Cybersecurity requirements are met for log in attempts within Sub-Paragraph "Unsuccessful Logon Attempts" within Part 3
N/A	AC-7(b)	CCI-002236	The organization defines the time period the information system will automatically lock the account or node when the maximum number of unsuccessful attempts is exceeded.	DoD has defined the time period as until released by an administrator.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as until released by an administrator.	LOW		X		X	X			3.3.2 Unsuccessful Logon Attempts		Cybersecurity requirements are met for log in attempts within Sub-Paragraph "Unsuccessful Logon Attempts" within Part 3
N/A	AC-7(b)	CCI-002237	The organization defines the delay algorithm to be employed by the information system to delay the next login prompt when the maximum number of unsuccessful attempts is exceeded.	DoD has defined the delay algorithm as a minimum of 5 seconds.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the delay algorithm as a minimum of 5 seconds.	LOW		X		X	X			3.3.2 Unsuccessful Logon Attempts		Cybersecurity requirements are met for log in attempts within Sub-Paragraph "Unsuccessful Logon Attempts" within Part 3
N/A	AC-7(b)	CCI-002238	The information system automatically locks the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next login prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.	The organization being inspected/assessed configures the information system to automatically lock the account or node until the locked account is released by an administrator and delays the next login prompt for a minimum of 5 seconds when the maximum number of unsuccessful attempts is exceeded. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2238. DoD has defined the delay algorithm as a minimum of 5 seconds. DoD has defined the time period as until released by an administrator.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically lock the account or node until the locked account is released by an administrator and delays the next login prompt for a minimum of 5 seconds when the maximum number of unsuccessful attempts is exceeded. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2238. DoD has defined the delay algorithm as a minimum of 5 seconds. DoD has defined the time period as until released by an administrator.	LOW		X		X				3.3.2 Unsuccessful Logon Attempts		Cybersecurity requirements are met for log in attempts within Sub-Paragraph "Unsuccessful Logon Attempts" within Part 3

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-8(a)	CCI-000048	The information system displays an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The organization being inspected/assessed configures the information system to display the DoD Information Systems – Standard Consent Banner and User Agreement before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 48. DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display the DoD Information Systems – Standard Consent Banner and User Agreement before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 48. DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	LOW	X	X		X				3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3
N/A	CP-2(a)(1)	CCI-000443	The organization develops a contingency plan for the information system that identifies essential missions.	The organization being inspected/assessed must clearly and accurately document essential missions for its information system(s). Impact of loss of essential mission functions must be defined using CNSSI 1253.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents essential missions for its information system(s).	LOW			X				A LOW CS doesn't have any "essential" mission	---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(1)	CCI-000444	The organization develops a contingency plan for the information system that identifies essential business functions.	The organization being inspected/assessed must clearly and accurately document essential business functions for its information system(s). Impact of loss of essential business functions must be defined using CNSSI 1253.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents essential business functions for its information system(s).	LOW						X		---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(1)	CCI-000445	The organization develops a contingency plan for the information system that identifies associated contingency requirements.	The organization being inspected/assessed must clearly and accurately document associated contingency requirements for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents associated contingency requirements for its information system(s).	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(2)	CCI-000446	The organization develops a contingency plan for the information system that provides recovery objectives.	The organization being inspected/assessed must clearly and accurately document recovery objectives for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents recovery objectives for its information system(s).	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(2)	CCI-000447	The organization develops a contingency plan for the information system that provides restoration priorities.	The organization being inspected/assessed must clearly and accurately document restoration priorities for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents restoration priorities for its information system(s).	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(2)	CCI-000448	The organization develops a contingency plan for the information system that provides metrics.	The organization being inspected/assessed must clearly and accurately document metrics for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents metrics for its information system(s).	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(3)	CCI-000449	The organization develops a contingency plan for the information system that addresses contingency roles, responsibilities, assigned individuals with contact information.	The organization being inspected/assessed must clearly and accurately document contingency roles, responsibilities, assigned individuals with contact information for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents contingency roles, responsibilities, assigned individuals with contact information for its information system(s).	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(4)	CCI-000450	The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system disruption.	The organization being inspected/assessed must clearly and accurately document maintaining essential missions despite an information system disruption for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential missions despite an information system disruption for its information system(s).	LOW			X				A LOW CS doesn't have any "essential" mission	---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(4)	CCI-000451	The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system disruption.	The organization being inspected/assessed must clearly and accurately document maintaining business functions despite an information system disruption for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining business functions despite an information system disruption for its information system(s).	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS are not business systems."	
N/A	CP-2(a)(4)	CCI-000452	The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system compromise.	The organization being inspected/assessed must clearly and accurately document maintaining essential missions despite an information system compromise for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential missions despite an information system compromise for its information system(s).	LOW			X				A LOW CS doesn't have any "essential" mission	---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(4)	CCI-000453	The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system compromise.	The organization being inspected/assessed must clearly and accurately document maintaining business functions despite an information system compromise for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining business functions despite an information system compromise for its information system(s).	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS are not business systems."	
N/A	CP-2(a)(4)	CCI-000454	The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system failure.	The organization being inspected/assessed must clearly and accurately document maintaining essential missions despite an information system failure for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential missions despite an information system failure for its information system(s).	LOW			X				A LOW CS doesn't have any "essential" mission	---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(4)	CCI-000455	The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system failure.	The organization being inspected/assessed must clearly and accurately document maintaining business functions despite an information system failure for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining business functions despite an information system failure for its information system(s).	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS are not business systems."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CP-2(a)(5)	CCI-000456	The organization develops a contingency plan for the information system that addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.	The organization being inspected/assessed must clearly and accurately document eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented for its information system(s).	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(6)	CCI-000457	The organization develops a contingency plan for the information system that is reviewed and approved by organization-defined personnel or roles.	The organization being inspected/assessed reviews and approves the contingency plan by at a minimum, the ISSM and ISSO. The organization must maintain an audit trail of the review and approval activity. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization conducting the inspection/assessment obtains and examines the audit trail to ensure the contingency plan has been reviewed and approved by at a minimum, the ISSM and ISSO. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(6)	CCI-002830	The organization defines the personnel or roles who review and approve the contingency plan for the information system.	DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-2(b)	CCI-000458	The organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan.	DoD has defined the list as all stakeholders identified in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the list as all stakeholders identified in the contingency plan.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(b)	CCI-000459	The organization distributes copies of the contingency plan to an organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements.	The organization being inspected/assessed ensures the contingency plan is disseminated to all stakeholders identified in the contingency plan via an information sharing capibility. DoD has defined the list as all stakeholders identified in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(c)	CCI-000460	The organization coordinates contingency planning activities with incident handling activities.	The organization being inspected/assessed will coordinate the contingency plan and incident response plan (IR-8) to ensure they do not contradict each other's objectives or result in duplicate efforts/activities.	The organization conducting the inspection/assessment obtains and examines the contingency plan and the incident response plan (IR-8) to ensure they do not contradict each other's objectives or result in duplicate efforts/activities.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(d)	CCI-000461	The organization defines the frequency to review the contingency plan for the information system.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-2(d)	CCI-000462	The organization reviews the contingency plan for the information system in accordance with organization-defined frequency.	The organization being inspected/assessed annually reviews the contingency plan. The organization must maintain an audit trail of annual reviews.	The organization conducting the inspection/assessment obtains and examines the audit trail to ensure the contingency plan is reviewed annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(e)	CCI-000463	The organization updates the contingency plan to address changes to the organization.	The organization being inspected/assessed must clearly and accurately update the contingency plan to address organizational changes. The organization must document the update activities as an audit trail.	The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately updates the contingency plan to address organizational changes.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(e)	CCI-000464	The organization updates the contingency plan to address changes to the information system.	The organization being inspected/assessed must clearly and accurately update the contingency plan to address changes to the information system. The organization must document the update activities as an audit trail.	The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately updates the contingency plan to address information system changes.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(e)	CCI-000465	The organization updates the contingency plan to address changes to the environment of operation.	The organization being inspected/assessed must clearly and accurately revise the contingency plan to address changes to the environment of operation. The organization must document the update activities as an audit trail.	The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately revises the contingency plan to address changes to the environment of operation.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(e)	CCI-000466	The organization updates the contingency plan to address problems encountered during contingency plan implementation, execution, or testing.	The organization being inspected/assessed must clearly and accurately revise the contingency plan to address problems encountered during contingency plan implementation, execution, or testing. The organization must document the update activities as an audit trail.	The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately revises the contingency plan to address problems encountered during contingency plan implementation, execution, or testing.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(f)	CCI-000468	The organization communicates contingency plan changes to organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements.	The organization being inspected/assessed communicates contingency plan changes to all stakeholders identified in the contingency plan. DoD has defined the list as all stakeholders identified in the contingency plan.	The organization conducting the inspection/assessment examines the contingency plan via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure the most current version has been communicated.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CP-2(f)	CCI-002831	The organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to whom contingency plan changes are to be communicated.	DoD has defined the list as all stakeholders identified in the contingency plan	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the list as all stakeholders identified in the contingency plan	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(g)	CCI-002832	The organization protects the contingency plan from unauthorized disclosure and modification.	The organization being inspected/assessed documents and implements a process to protect the contingency plan from unauthorized disclosure and modification.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects the contingency plan from unauthorized disclosure and modification.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-3(a)	CCI-000486	The organization provides contingency training to information system users consistent with assigned roles and responsibilities within an organization-defined time period of assuming a contingency role or responsibility.	The organization being inspected/assessed provides initial contingency training to personnel with contingency roles and responsibilities IAW CP-2, CCI 449 at a maximum, 10 working days of assuming a contingency role or responsibility. The organization will maintain documentation of the training activity dates, location, and personnel for audit trail purposes and future reference (e.g., scheduling refresher training, etc.). DoD has defined the time period as at a maximum, 10 working days.	The organization conducting the inspection/assessment obtains and examines the list of contingency personnel and documentation of initial contingency training for the purpose of ensuring that all personnel with contingency roles and responsibilities have received initial contingency training at a maximum, 10 working days of assuming a contingency role or responsibility. DoD has defined the time period as at a maximum, 10 working days.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-3(a)	CCI-002833	The organization defines the time period that contingency training is to be provided to information system users consistent with assigned roles and responsibilities within assuming a contingency role or responsibility.	DoD has defined the time period as at a maximum, 10 working days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as at a maximum, 10 working days.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-3(b)	CCI-002834	The organization provides contingency training to information system users consistent with assigned roles and responsibilities when required by information system changes.	The organization being inspected/assessed will update contingency training materials when required by information system changes and provide that training to personnel with contingency roles and responsibilities IAW CP-2, CCI 449. The organization will maintain documentation of the training activity dates, location, and personnel for audit trail purposes and future reference (e.g., scheduling refresher training, etc.).	The organization conducting the inspection/assessment obtains and examines training materials and documentation of training activities to determine whether the materials are accurate in consideration of the state of the information system and content of the contingency plan. The organization ensures that training is provided to users consistent with assigned roles and responsibilities.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-3(c)	CCI-000485	The organization defines the frequency of refresher contingency training to information system users.	DoD has defined the frequency as at least annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-3(c)	CCI-000487	The organization provides refresher contingency training to information system users consistent with assigned roles and responsibilities in accordance with organization-defined frequency.	The organization being inspected/assessed provides refresher contingency training to personnel with contingency roles and responsibilities IAW CP-2, CCI 449 at least annually. The organization will maintain documentation of the training activity dates, location, and personnel for audit trail purposes and future reference (e.g., scheduling refresher training, etc.). DoD has defined the frequency as at least annually.	The organization conducting the inspection/assessment obtains and examines the list of contingency personnel and documentation of refresher contingency training for the purpose of ensuring that all personnel with contingency roles and responsibilities have received refresher contingency training at least annually. DoD has defined the frequency as at least annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-4(a)	CCI-000490	The organization defines the frequency to test the contingency plan for the information system.	DoD has defined the frequency as at least annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-4(a)	CCI-000492	The organization defines contingency plan tests to be conducted for the information system.	The organization being inspected/assessed defines and documents contingency plan tests to be conducted for the information system. DoD has determined the contingency plan tests are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented contingency plan tests to ensure the organization being inspected/assessed defines contingency plan tests to be conducted for the information system. DoD has determined the contingency plan tests are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-4(a)	CCI-000494	The organization tests the contingency plan for the information system in accordance with organization-defined frequency using organization-defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan.	The organization being inspected/assessed conduct tests defined in CP-4, 492 at least annually to determine the effectiveness of the plan and the organizational readiness to execute the plan. The organization must maintain a record of test results. DoD has defined the frequency as at least annually.	The organization conducting the inspection/assessment obtains and examines the record of test results to ensure the organization being inspected/assessed conduct tests defined in CP-4, 492 at least annually to determine the effectiveness of the plan and the organizational readiness to execute the plan. DoD has defined the frequency as at least annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CP-4(b)	CCI-000496	The organization reviews the contingency plan test results.	The organization being inspected/assessed will review the contingency plan test results. The organization must maintain an audit trail of issues identified during the reviews of the contingency plan test results.	The organization conducting the inspection/assessment obtains and examines the audit trail of issues identified during the reviews of the contingency plan test results to ensure the organization being inspected/assessed reviews the contingency plan test results.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-4(c)	CCI-000497	The organization initiates corrective actions, if needed, after reviewing the contingency plan test results.	The organization being inspected/assessed identifies and documents any corrective actions required after reviewing the contingency plan test results. The organization initiates corrective actions and tracks those actions within the POA&M.	The organization conducting the inspection/assessment obtains and examines the contingency plan test results as well as any documented corrective actions required and ensures the corrective actions are being implemented and tracked within the POA&M.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-9(a)	CCI-000534	The organization defines frequency of conducting user-level information backups to support recovery time objectives and recovery point objectives.	DoD has defined the frequency as at least weekly as defined in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least weekly as defined in the contingency plan.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-9(a)	CCI-000535	The organization conducts backups of user-level information contained in the information system per organization-defined frequency that is consistent with recovery time and recovery point objectives.	The organization being inspected/assessed must identify user level information within the backup strategy and configure the system to perform backups at least weekly as defined in the contingency plan.	The organization conducting the inspection/assessment obtains and reviews the backup strategy, and examines a sample of systems to ensure they are configured to perform back ups at least weekly as defined in the contingency plan.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-9(b)	CCI-000536	The organization defines frequency of conducting system-level information backups to support recovery time objectives and recovery point objectives.	DoD has defined the frequency as at least weekly and as required by system baseline configuration changes in accordance with the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least weekly and as required by system baseline configuration changes in accordance with the contingency plan.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-9(b)	CCI-000537	The organization conducts backups of system-level information contained in the information system per organization-defined frequency that is consistent with recovery time and recovery point objectives.	The organization being inspected/assessed must identify system-level information within the backup strategy and configure the system to perform backups at least weekly and as required by system baseline configuration changes in accordance with the contingency plan.	The organization conducting the inspection/assessment obtains and reviews the backup strategy, and examines a sample of systems to ensure they are configured to perform back ups at least weekly and as required by system baseline configuration changes in accordance with the contingency plan.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-9(c)	CCI-000538	The organization defines the frequency of conducting information system documentation backups including security-related documentation to support recovery time objectives and recovery point objectives.	DoD has defined the frequency as when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-9(c)	CCI-000539	The organization conducts backups of information system documentation including security-related documentation per organization-defined frequency that is consistent with recovery time and recovery point objectives.	The organization being inspected/assessed conducts backups of information system documentation including security-related documentation when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan.	The organization conducting the inspection/assessment obtains and examines the latest version of the information system documentation including security-related documentation to verify it is the same version as contained in backups.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-9(d)	CCI-000540	The organization protects the confidentiality, integrity, and availability of backup information at storage locations.	The organization being inspected/assessed will protect the confidentiality, integrity, and availability of backup information at the storage location IAW the system security plan.	The organization conducting the inspection/assessment obtains and examines the system security plan and ensures backup information at the storage location is protected IAW the system security plan.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-1(a)	CCI-001933	The organization defines the personnel or roles to be recipients of the identification and authentication policy and the procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	DoD has defined the roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate. DoDI 8520.02 and DoDI 8520.03 meet the DoD requirement for Identification and Authentication policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. DoD has defined the roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-1(a)	CCI-001934	The organization documents procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	DoD documents within DoDI 8520.02 and DoDI 8520.03 procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-1(a)(1)	CCI-000756	The organization develops and documents an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoD developed DoDI 8520.02 and DoDI 8520.03 as the identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-1(a)(1)	CCI-000757	The organization disseminates to organization defined personnel or roles an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoD disseminates the DoDI 8520.02 and DoDI 8520.03 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) to the ISSO and ISSM and others as the local organization deems appropriate as an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03. DoD has defined the personnel or roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. DoD has defined the personnel or roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-1(a)(1)	CCI-001932	The organization documents an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoD documents within DoDI 8520.02 and DoDI 8520.03 an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-1(a)(2)	CCI-000760	The organization develops and documents procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	DoD develops within DoDI 8520.02 and DoDI 8520.03, procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-1(a)(2)	CCI-000761	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	DoD disseminates the DoDI 8520.02 and DoDI 8520.03 to the ISSO and ISSM and others as the local organization deems appropriate via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html). DoDI 8520.02 and DoDI 8520.03 are procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. DoD has defined the personnel or roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-1(b)(1)	CCI-000758	The organization reviews and updates identification and authentication policy in accordance with the organization defined frequency.	DoD reviews and updates identification and authentication policy (DoDI 8520.02 and DoDI 8520.03) annually. DoD Components are automatically compliant with this CCI because they are covered at the DoD level policies, DoDI 8520.02 and DoDI 8520.03. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-1(b)(1)	CCI-000759	The organization defines a frequency for reviewing and updating the identification and authentication policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-1(b)(2)	CCI-000762	The organization reviews and updates identification and authentication procedures in accordance with the organization defined frequency.	DoD reviews and updates identification and authentication procedures (DoDI 8520.02 and DoDI 8520.03) annually. The organization being inspected/assessed is automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03. DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-1(b)(2)	CCI-000763	The organization defines a frequency for reviewing and updating the identification and authentication procedures.	DoD has defined the frequency as review annually - update as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as review annually - update as appropriate.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-8(a)	CCI-002247	The organization defines the use notification message or banner the information system displays to users before granting access to the system.	DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	LOW	X	X		X	X			3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-8(a)(1)	CCI-002243	The organization-defined information system use notification message or banner is to state that users are accessing a U.S. Government information system.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	LOW	X	X		X	X			3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-8(a)(2)	CCI-002244	The organization-defined information system use notification message or banner is to state that information system usage may be monitored, recorded, and subject to audit.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	LOW	X	X		X	X			3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-8(a)(3)	CCI-002245	The organization-defined information system use notification message or banner is to state that unauthorized use of the information system is prohibited and subject to criminal and civil penalties.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	LOW	X	X		X	X			3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-8(a)(4)	CCI-002246	The organization-defined information system use notification message or banner is to state that use of the information system indicates consent to monitoring and recording.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	LOW	X	X		X	X			3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-8(b)	CCI-000050	The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access.	The organization being inspected/assessed configures the information system to retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 50.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 50.	LOW	X	X						3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-8(c)(1)	CCI-002248	The organization defines the conditions of use which are to be displayed to users of the information system before granting further access.	DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	LOW	X	X		X	X			3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational For Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-4(a)	CCI-001970	The organization defines the personnel or roles that authorize the assignment of individual, group, role, and device identifiers.	DoD has defined the personnel or roles as the ISSM or ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSM or ISSO.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-4(a)	CCI-001971	The organization manages information system identifiers by receiving authorization from organization-defined personnel or roles to assign an individual, group, role or device identifier.	The organization being inspected/assessed implements a process to manage information system identifiers by receiving authorization from the ISSM or ISSO to assign an individual, group, role or device identifier. DoD has defined the personnel or roles as the ISSM or ISSO.	The organization conducting the inspection/assessment obtains and examines documentation and system configuration information to ensure the organization being inspected/assessed manages information system identifiers by receiving authorization from the ISSM or ISSO to assign an individual, group, role or device identifier. DoD has defined the personnel or roles as the ISSM or ISSO.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-4(b)	CCI-001972	The organization manages information system identifiers by selecting an identifier that identifies an individual, group, role, or device.	The organization being inspected/assessed implements a process to manage information system identifiers by selecting an identifier that identifies an individual, group, role, or device.	The organization conducting the inspection/assessment obtains and examines documentation or system configuration information to ensure the organization being inspected/assessed manages information system identifiers by selecting an identifier that identifies an individual, group, role, or device.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-4(c)	CCI-001973	The organization manages information system identifiers by assigning the identifier to the intended individual, group, role, or device.	The organization being inspected/assessed implements a process to manage information system identifiers by assigning the identifier to the intended individual, group, role, or device.	The organization conducting the inspection/assessment obtains and examines documentation or system configuration information to ensure the organization being inspected/assessed manages information system identifiers by assigning the identifier to the intended individual, group, role, or device.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-4(d)	CCI-001974	The organization defines the time period for which the reuse of identifiers is prohibited.	DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier).	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-4(d)	CCI-001975	The organization manages information system identifiers by preventing reuse of identifiers for an organization-defined time period.	The organization being inspected/assessed implements a process for information system identifiers to prevent reuse of identifiers for 1 year for user identifiers (DoD is not going to specify value for device identifier). DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier).	The organization conducting the inspection/assessment obtains and examines documentation or system configuration information to ensure the organization being inspected/assessed prevents the reuse of identifiers for 1 year for user identifiers (DoD is not going to specify value for device identifier). DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier).	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-4(e)	CCI-000794	The organization defines a time period of inactivity after which the identifier is disabled.	DoD has defined the time period as 35 days of inactivity.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 35 days of inactivity.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-4(e)	CCI-000795	The organization manages information system identifiers by disabling the identifier after an organization defined time period of inactivity.	The organization being inspected/assessed configures the information system to disable identifiers after 35 days of inactivity. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 795. DoD has defined the time period as 35 days of inactivity.	The organization conducting the inspection/assessment examines the information system configuration to ensure that identifiers are disabled after 35 days of inactivity. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 795. DoD has defined the time period as 35 days of inactivity.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-5	CCI-001988	The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.	The organization being inspected/assessed documents and enforces a requirement for developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.	The organization conducting the inspection/assessment obtains and examines the documented requirements placed upon developers/installers of information system components to ensure that there is a documented requirement to provide unique authenticators or change default authenticators prior to delivery/installation.	LOW								---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AC-14(a)	CCI-000061	The organization identifies and defines organization-defined user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions.	The organization being inspected/assessed identifies, defines, and documents user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions. DoD has determined the user actions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented user actions to ensure the organization being inspected/assessed identifies and defines the user actions that can be performed on the information system without identification and authentication. DoD has determined the user actions are not appropriate to define at the Enterprise level.	LOW		X						3.3.5 Permitted Actions Without Identific…		Cybersecurity requirements are met for user actions without Identification or authorization within Sub-Paragraph "Permitted Actions Without Identification or Authentication" within Part 3
N/A	AC-14(b)	CCI-000232	The organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.	The organization being inspected/assessed documents supporting rationale in the security plan for the actions defined in AC-14, CCI 61 to not require identification and authentication.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed documents the supporting rationale for the actions defined in AC-14, CCI 61 to not require identification and authentication.	LOW		X						3.3.5 Permitted Actions Without Identific…		Cybersecurity requirements are met for user actions without Identification or authorization within Sub-Paragraph "Permitted Actions Without Identification or Authentication" within Part 3

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
SC-7	SC-7(a)	CCI-001097	The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.	The organization being inspected/assessed documents and implements processes to monitor and control communications at the external boundary of the system and at key internal boundaries within the system. The organization must maintain an audit trail of monitoring activities.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring activities to ensure the organization being inspected/assessed monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.	LOW	X	X		X	X			3.7.2 Denial of Service Protection... 3.7.5 Process Isolation and Boundary Prot...		CCI requirements are addressed within subparagraph "Denial of Service Protection" of UFGS 25 05 11.
N/A	IA-2(1)	CCI-000765	The information system implements multifactor authentication for network access to privileged accounts.	The organization being inspected/assessed configures the information system to implement multifactor authentication for network access to privileged accounts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 765.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement multifactor authentication for network access to privileged accounts. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 765.	LOW	X	X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity requirements are met for user accounts (withing device capabilities) within Sub-Paragraph "USER IDENTIFICATION AND AUTHENTICATION" within Part 3
N/A	IA-2(12)	CCI-001953	The information system accepts Personal Identity Verification (PIV) credentials.	The organization being inspected/assessed configures the information system to accept PIV/CAC authentication. This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1953	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to accept PIV/CAC authentication. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1953.	LOW	X	X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-2(12)	CCI-001954	The information system electronically verifies Personal Identity Verification (PIV) credentials.	The organization being inspected/assessed configures the information system to verify PIV/CAC authentication. This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1954.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to verify PIV/CAC authentication. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1954.	LOW	X	X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(a)	CCI-000192	The information system enforces password complexity by the minimum number of upper case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of upper case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 192.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of upper case characters used. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 192.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(a)	CCI-000193	The information system enforces password complexity by the minimum number of lower case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of lower case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 193.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of lower case characters used. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 193.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(a)	CCI-000194	The information system enforces password complexity by the minimum number of numeric characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of numeric characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 194.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of numeric characters used. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 194.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "user identification and authentication"

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-5(1)(a)	CCI-000205	The information system enforces minimum password length.	The organization being inspected/assessed configures the information system to enforce minimum password length. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 205.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce minimum password length. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 205.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(a)	CCI-001611	The organization defines the minimum number of special characters for password complexity enforcement.	DoD has defined the minimum number of special characters for password complexity enforcement as one special character.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of special characters for password complexity enforcement as one special character.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(a)	CCI-001612	The organization defines the minimum number of upper case characters for password complexity enforcement.	DoD has defined the minimum number of upper case characters for password complexity enforcement as one upper-case character.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of upper case characters for password complexity enforcement as one upper-case character.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(a)	CCI-001613	The organization defines the minimum number of lower case characters for password complexity enforcement.	DoD has defined the minimum number of lower case characters for password complexity enforcement as one lower-case character.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of lower case characters for password complexity enforcement as one lower-case character.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(a)	CCI-001614	The organization defines the minimum number of numeric characters for password complexity enforcement.	DoD has defined the minimum number of numeric characters for password complexity enforcement as one numeric character.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of numeric characters for password complexity enforcement as one numeric character.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(a)	CCI-001619	The information system enforces password complexity by the minimum number of special characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of special characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1619.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of special characters used. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1619.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(b)	CCI-000195	The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.	The organization being inspected/assessed configures the information system to enforce that at least 50% of the minimum password length is changed. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 195. DoD has defined the minimum number of characters as 50% of the minimum password length.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce that at least 50% of the minimum password length is changed. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 195. DoD has defined the minimum number of characters as 50% of the minimum password length.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(b)	CCI-001615	The organization defines the minimum number of characters that are changed when new passwords are created.	DoD has defined the minimum number of characters as 50% of the minimum password length.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of characters as 50% of the minimum password length.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(c)	CCI-000196	The information system, for password-based authentication, stores only cryptographically-protected passwords.	The organization being inspected/assessed configures the information system to store only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 196.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to store only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 196.	LOW	X	X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "user identification and authentication"

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-5(1)(c)	CCI-000197	The information system, for password-based authentication, transmits only cryptographically-protected passwords.	The organization being inspected/assessed configures the information system to transmit only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 197.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to transmit only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 197.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(d)	CCI-000198	The information system enforces minimum password lifetime restrictions.	The organization being inspected/assessed configures the information system to enforce minimum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 198.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce minimum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 198.	LOW		X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(d)	CCI-000199	The information system enforces maximum password lifetime restrictions.	The organization being inspected/assessed configures the information system to enforce maximum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 199.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce maximum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 199.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(d)	CCI-001616	The organization defines minimum password lifetime restrictions.	DoD has defined the minimum password lifetime restrictions as 24 hours.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum password lifetime restrictions as 24 hours.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(a)	CCI-001980	The organization manages information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.	The organization being inspected/assessed defines and documents procedures for the secure distribution of authenticators. The process shall include verification of the identify of the individual, group, role, or device receiving the authenticator.	The organization conducting the inspection/assessment obtains and examines the documented procedures for the secure distribution of authenticators to ensure they have been defined and that they include a method to verify the identify of the individual, group, role, or device receiving the authenticator.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
IA-5	IA-5(b)	CCI-000176	The organization manages information system authenticators by establishing initial authenticator content for authenticators defined by the organization.	The organization being inspected/assessed defines and documents procedures for setting initial authenticator content.	The organization conducting the inspection/assessment obtains and examines the documented procedures for setting initial authenticator content to ensure they have been defined.	LOW		X	X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(1)(d)	CCI-001617	The organization defines maximum password lifetime restrictions.	DoD has defined the maximum password lifetime restrictions as 60 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the maximum password lifetime restrictions as 60 days.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(d)	CCI-001981	The organization manages information system authenticators by establishing administrative procedures for initial authenticator distribution.	The organization being inspected/assessed defines and documents procedures for the secure distribution of authenticators.	The organization conducting the inspection/assessment obtains and examines the documented procedures for the secure distribution of authenticators to ensure they have been defined.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(d)	CCI-001982	The organization manages information system authenticators by establishing administrative procedures for lost/compromised authenticators.	The organization being inspected/assessed defines and documents procedures for lost/compromised authenticators.	The organization conducting the inspection/assessment obtains and examines the documented procedures for lost/compromised authenticators to ensure they have been defined.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(d)	CCI-001983	The organization manages information system authenticators by establishing administrative procedures for damaged authenticators.	The organization being inspected/assessed defines and documents procedures for the secure disposal of damaged authenticators.	The organization conducting the inspection/assessment obtains and examines the documented procedures for the secure disposal of damaged authenticators to ensure they have been defined.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(d)	CCI-001984	The organization manages information system authenticators by establishing administrative procedures for revoking authenticators.	The organization being inspected/assessed defines and documents procedures for revoking authenticators.	The organization conducting the inspection/assessment obtains and examines the documented procedures for revoking authenticators to ensure the procedures are defined.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(d)	CCI-001985	The organization manages information system authenticators by implementing administrative procedures for initial authenticator distribution.	The organization being inspected/assessed implements administrative procedures for initial authenticator distribution as documented in IA-5, CCIs 1980 & 1981.	The organization conducting the inspection/assessment obtains and examines records of initial authenticator distribution and interviews individuals responsible for authenticator distribution to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCIs 1980 & 1981.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-5(d)	CCI-001986	The organization manages information system authenticators by implementing administrative procedures for lost/compromised authenticators.	The organization being inspected/assessed implements administrative procedures for the response to lost/compromised authenticators as documented in IA-5, CCI 1982.	The organization conducting the inspection/assessment obtains and examines documented procedures for the response to lost/compromised authenticators to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCI 1982.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(d)	CCI-001987	The organization manages information system authenticators by implementing administrative procedures for damaged authenticators.	The organization being inspected/assessed implements administrative procedures for the response to damaged authenticators as documented in IA-5, CCI 1983.	The organization conducting the inspection/assessment obtains and examines documented procedures for the response to damaged authenticators to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCI 1983.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(1)(e)	CCI-000200	The information system prohibits password reuse for the organization defined number of generations.	The organization being inspected/assessed configures the information system to prohibit reuse for a minimum of 5 generations. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 200. DoD has defined the number of generations as a minimum of 5.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prohibit reuse for a minimum of 5 generations. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 200. DoD has defined the number of generations as a minimum of 5.	LOW	X	X	X	X				3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(f)	CCI-000179	The organization manages information system authenticators by establishing minimum lifetime restrictions for authenticators.	The organization being inspected/assessed defines and documents minimum lifetime restrictions for authenticators.	The organization conducting the inspection/assessment obtains and examines the documented minimum lifetime restrictions for authenticators to ensure they have been defined.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(f)	CCI-000180	The organization manages information system authenticators by establishing maximum lifetime restrictions for authenticators.	Per IA-5, CCI 1610, DoD has established the maximum lifetime restrictions for authenticators as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	Per IA-5, CCI 1610, DoD has established the maximum lifetime restrictions for authenticators as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(f)	CCI-000181	The organization manages information system authenticators by establishing reuse conditions for authenticators.	The organization being inspected/assessed defines and documents the reuse conditions for authenticators.	The organization conducting the inspection/assessment obtains and examines the documented reuse conditions for authenticators to ensure they have been defined.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(1)(e)	CCI-001618	The organization defines the number of generations for which password reuse is prohibited.	DoD has defined the number of generations as a minimum of 5.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the number of generations as a minimum of 5.	LOW	X	X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(f)	CCI-002041	The information system allows the use of a temporary password for system logons with an immediate change to a permanent password.	The organization being inspected/assessed configures the information system to allow the use of a temporary password for system logons with an immediate change to a permanent password. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2041.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to allow the use of a temporary password for system logons with an immediate change to a permanent password. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2041.	LOW	X	X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(h)	CCI-000183	The organization manages information system authenticators by protecting authenticator content from unauthorized disclosure.	The organization being inspected/assessed documents and implements procedures to protect authenticator content from unauthorized disclosure.	The organization conducting the inspection/assessment obtains and examines the documented procedures to protect authenticator content from unauthorized disclosure to ensure the procedures are defined.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(h)	CCI-002042	The organization manages information system authenticators by protecting authenticator content from unauthorized modification.	The organization being inspected/assessed configures the information system to manage information system authenticators by protecting authenticator content from unauthorized modification. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2042.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to manage information system authenticators by protecting authenticator content from unauthorized modification. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2042.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(i)	CCI-002365	The organization manages information system authenticators by requiring individuals to take specific security safeguards to protect authenticators.	The organization being inspected/assessed documents within user agreements that individuals shall safeguard authenticators.	The organization conducting the inspection/assessment obtains and examines the user agreements of the organization being inspected/assessed to ensure that there are requirements for individuals to safeguard authenticators.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-5(i)	CCI-002366	The organization manages information system authenticators by having devices implement specific security safeguards to protect authenticators.	The organization being inspected/assessed configures the information system to manage information system authenticators by having devices implement, specific security safeguards to protect authenticators. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2366.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to manage information system authenticators by having devices implement, specific security safeguards to protect authenticators. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2366.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(j)	CCI-001990	The organization manages information system authenticators by changing authenticators for group/role accounts when membership to those accounts changes.	The organization being inspected/assessed documents and implements procedures for changing authenticators for group/role accounts when membership to those accounts changes.	The organization conducting the inspection/assessment obtains and examines the documented procedures for group/role authenticator change to ensure the procedures are defined and applied when membership to those accounts changes. The organization conducting the inspection/assessment obtains and examines a sampling of authenticator age data and documentation of personnel role changes to ensure that group/role authenticators are changed when membership changes.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-5(11)	CCI-002002	The organization defines the token quality requirements to be employed by the information system mechanisms for token-based authentication.	DoDI 8520.03 defines types of authentication credentials that are acceptable for authentication to different systems based on the systems' information sensitivity levels and the users' access environments. The definitions for credential strengths D, E and H found in DoDI 8520.03 Enclosure 3, Section 3 specifically deal with acceptable types of hardware PKI credentials. DoD Components are automatically compliant with this CCI because they are covered by the DoD-level policy, DoDI 8520.03.	DoDI 8520.03 defines types of authentication credentials that are acceptable for authentication to different systems based on the systems' information sensitivity levels and the users' access environments. The definitions for credential strengths D, E and H found in DoDI 8520.03 Enclosure 3, Section 3 specifically deal with acceptable types of hardware PKI credentials. DoD Components are automatically compliant with this CCI because they are covered by the DoD-level policy, DoDI 8520.03.	LOW	X	X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(11)	CCI-002003	The information system, for token-based authentication, employs mechanisms that satisfy organization-defined token quality requirements.	The information system performing hardware token-based authentication must be configured to accept only DoD-approved PKI credentials in accordance with DoDI 8520.02 and DoDI 8520.03. For unclassified systems, DoD-approved PKI credentials include DoD PKI credentials, External Certification Authority (ECA) PKI credentials, and DoD-approved external PKI credentials. For SIPRNet, DoD-approved PKI credentials include DoD PKI credentials and NSS PKI credentials. If the information system accepts DoD-approved external PKI credentials, the information system must be configured to accept only certificates at approved assurance levels, as represented by the Certificate Policy Object Identifiers (OIDs) asserted in the certificate. The current list of DoD-approved external PKIs and acceptable Object Identifiers (OIDs) for each approved external PKI is available at http://iase.disa.mil/pki-pke/interoperability.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept only DoD-approved PKI credentials in accordance with (IAW) DoDI 8520.02 and DoDI 8520.03. If the information system accepts DoD-approved external PKI credentials, the organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept only DoD-approved external PKI credentials that assert an approved Certificate Policy OID and reject credentials issued off of DoD-approved external PKIs that do not assert an approved OID.	LOW	X	X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-8	CCI-000804	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	The organization being inspected/assessed configures the information system to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 804.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 804.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-8(1)	CCI-002009	The information system accepts Personal Identity Verification (PIV) credentials from other federal agencies.	The information system performing hardware token-based authentication must be configured to accept DoD-approved external PKI PIV credentials to authenticate federal agency users in accordance with DoDI 8520.02 and DoDI 8520.03. The information system must be configured to accept only certificates at approved assurance levels, as represented by the Certificate Policy Object Identifiers (OIDs) asserted in the certificate. The current list of DoD-approved external PKIs and acceptable Object Identifiers (OIDs) for each approved external PKI is available at http://iase.disa.mil/pki-pke/interoperability. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2009.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept DoD-approved external PKI PIV credentials in accordance with DoDI 8520.02 and DoDI 8520.03. The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept only DoD-approved external PKI PIV credentials that assert an approved Certificate Policy OID and reject credentials issued off of DoD-approved external PKIs that do not assert an approved OID. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2009.	LOW	X			X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-8(1)	CCI-002010	The information system electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.	The information system performing hardware token-based authentication must be configured to validate DoD-approved external PKI PIV credentials to authenticate federal agency users in accordance with RFC 5280. The information system must be configured to perform a revocation check as part of the certificate validation process. Revocation checking may be performed using certificate revocation lists (CRLs) published by the issuing PKI or Online Certificate Status Protocol (OCSP) services. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2010.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to validate DoD-approved external PKI PIV credentials in accordance with RFC 5280. The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to perform a revocation check as part of the certificate validation process. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2010.	LOW	X			X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-8(2)	CCI-002011	The information system accepts FICAM-approved third-party credentials.	The organization being inspected/assessed configures the information system to accept Federal Identity, Credential, and Access Management (FICAM)-approved third-party credentials. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2011. FICAM Guidance is available at http://www.idmanagement.gov.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to accept FICAM-approved third-party credentials For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2011.	LOW	X			X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-8(3)	CCI-002012	The organization defines the information systems which will employ only FICAM-approved information system components.	The organization being inspected/assessed defines and documents the information systems which will employ only Federal Identity, Credential, and Access Management (FICAM)-approved information system components. DoD has determined the information systems are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information systems to ensure they have been defined. DoD has determined the information systems are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-8(3)	CCI-002013	The organization employs only FICAM-approved information system components in organization-defined information systems to accept third-party credentials.	The organization being inspected/assessed employs only Federal Identity, Credential, and Access Management (FICAM)-approved information system components to accept third-party credentials in information systems defined in IA-8 (3), CCI 2012. FICAM Guidance is available at http://www.idmanagement.gov.	The organization conducting the inspection/assessment obtains and examines the list of information system components in use to ensure the organization being inspected/assessed uses only FICAM-approved components in information systems defined in IA-8 (3), CCI 2012.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-8(4)	CCI-002014	The information system conforms to FICAM-issued profiles.	The organization being inspected/assessed configures the information system to conform to Federal Identity, Credential, and Access Management (FICAM)-issued profiles. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2014. FICAM Guidance is available at http://www.idmanagement.gov.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to conform to FICAM-issued profiles. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2014.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IR-1(a)	CCI-002776	The organization defines the personnel or roles to whom the incident response policy is disseminated.	DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-1(a)	CCI-002777	The organization defines the personnel or roles to whom the incident response procedures are disseminated.	DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-1(a)(1)	CCI-000805	The organization develops and documents an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-1(a)(1)	CCI-000806	The organization disseminates an incident response policy to organization-defined personnel or roles.	DoD disseminates via http://www.dtic.mil/cjcs_directives/, CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 to all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-1(a)(2)	CCI-000809	The organization develops and documents procedures to facilitate the implementation of the incident response policy and associated incident response controls.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meets the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-1(a)(2)	CCI-000810	The organization disseminates incident response procedures to organization-defined personnel or roles.	DoD disseminates via http://www.dtic.mil/cjcs_directives/, CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 to all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-1(b)(1)	CCI-000807	The organization reviews and updates the current incident response policy in accordance with organization-defined frequency.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IR-1(b)(1)	CCI-000808	The organization defines the frequency to review and update the current incident response policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of issuance.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-1(b)(2)	CCI-000811	The organization reviews and updates the current incident response procedures in accordance with organization-defined frequency.	DoD (in conjunction with Joint Staff for CJCSIs) reviews and updates current incident response procedures (CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2) annually. DoD Components are automatically compliant with this CCI because they are covered at the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. DoD has defined the frequency as reviewed annually - updated as appropriate.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered at the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-1(b)(2)	CCI-000812	The organization defines the frequency to review and update the current incident response procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-2(a)	CCI-000813	The organization provides incident response training to information system users consistent with assigned roles and responsibilities within an organization-defined time period of assuming an incident response role or responsibility.	The organization being inspected/assessed documents and implement a process to provide incident response training to information system users consistent with assigned roles and responsibilities within 30 working days of assuming an incident response role or responsibility. The organization must maintain a record of training. DoD has defined the time period as 30 working days.	The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of information system users to ensure the organization being inspected/assessed provides incident response training to information system users consistent with assigned roles and responsibilities within 30 working days of assuming an incident response role or responsibility. DoD has defined the time period as 30 working days.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-2(a)	CCI-002778	The organization defines the time period in which information system users whom assume an incident response role or responsibility receive incident response training.	DoD has defined the time period as 30 working days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 30 working days.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-2(b)	CCI-002779	The organization provides incident response training to information system users consistent with assigned roles and responsibilities when required by information system changes.	The organization being inspected/assessed documents and implements a process to provide incident response training to information system users, other than general users, consistent with assigned roles and responsibilities when required by information system changes. For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training. The organization must maintain a record of training.	The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of information system users to ensure the organization being inspected/assessed provides incident response training to information system users, other than general users, consistent with assigned roles and responsibilities when required by information system changes. For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-2(c)	CCI-000814	The organization provides refresher incident response training in accordance with organization-defined frequency.	The organization being inspected/assessed documents and implements a process to provide incident response training to information system users, other than general users, consistent with assigned roles and responsibilities annually. For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training. The organization must maintain a record of training. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of information system users to ensure the organization being inspected/assessed provides incident response training to information system users, other than general users, consistent with assigned roles and responsibilities annually. For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-2(c)	CCI-000815	The organization defines a frequency for refresher incident response training.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-4(a)	CCI-000822	The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	The organization being inspected/assessed must have a documented and certified CNDSP and documented procedures for information system users and site security personnel to handle incidents until they are transferred to the responsibility of the CNDSP.	The organization conducting the inspection/assessment obtains and examines the documentation identifying the CNDSP leveraged as well as the documented procedures for incident handling to ensure that there is a certified CNDSP in use and that there are procedures implemented to handle incidents until they are transferred to the responsibility of the CNDSP.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below			Enclave		Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IR-4(b)	CCI-000823	The organization coordinates incident handling activities with contingency planning activities.	The organization being inspected/assessed will coordinate the incident response plan (IR-8) and contingency plan (CP-2) to ensure they allow for an effective transfer of information system activity and maintain confidentiality and integrity of the contigency assets.	The organization conducting the inspection/assessment obtains and examines the incident response plan (IR-8) and contingency plan (CP-2) to ensure they allow for an effective transfer of information system activity and maintain confidentiality and integrity of the contigency assets.	LOW			X							---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-4(c)	CCI-000824	The organization incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises.	The organization being inspected/assessed will conduct after action reviews from incidents to identify lessons learned and will incorporate them into procedures, training, and testing/exercises. The organization must maintain records of after action reviews.	The organization conducting the inspection/assessment obtains and examines after action reports or meeting minutes to identify actionable lessons learned to verify that lessons learned are incorporated into the plan as changes are necessary.	LOW			X							---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-4(c)	CCI-001625	The organization implements the resulting incident handling activity changes to incident response procedures, training and testing/exercise accordingly.	The organization being inspected/assessed will follow the latest incident response plan (IR-8) that has been revised (based on IR-4, CCI-000824) and disseminated.	The organization conducting the inspection/assessment obtains and examines recent changes to the incident response plan (based on IR-4, CCI 000824) to verify that they have been disseminated and reviews the most recent after action report to ensure that changes have been followed.	LOW			X							---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-5	CCI-000832	The organization tracks and documents information system security incidents.	The organization being inspected/assessed will document within their incident handling plan, procedures to leverage the Joint Incident Management System (JIMS). For the DoD, JIMS is the automated mechanism.	The organization conducting the inspection/assessment obtains and examines the incident handling plan to ensure that there are procedures identified to leverage the JIMS.	LOW			X							---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-6(a)	CCI-000834	The organization defines a time period for personnel to report suspected security incidents to the organizational incident response capability.	DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance. If organizations decide to be more restrictive than the guidance in the CJCSM, then they should address the more restrictive response time requirements in their incident response plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance. The organization conducting the inspection/assessment obtains and examines the incident response plan to determine if more stringent response time requirements have been identified.	LOW			X		X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-6(a)	CCI-000835	The organization requires personnel to report suspected security incidents to the organizational incident response capability within the organization-defined time period.	The organization being inspected/assessed documents within the user agreement the requirement for all system users to report suspected security incidents to the organizational incident response capability within the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance. DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance.	The organization conducting the inspection/assessment obtains and examines the user agreement to ensure users are required to report suspected security incidents to the organizational incident response capability within the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance. DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance.	LOW			X							---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-6(b)	CCI-000836	The organization reports security incident information to organization-defined authorities.	The organization being inspected/assessed documents and implements a process to report to the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).any security incidents IAW the incident response plan (IR-8). Reporting shall be conducted IAW CJCSM 6510.01B. DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).	The organization conducting the inspection/assessment obtains and examines a sample of previous security incidents to ensure the incidents were reported to the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT). any security incidents IAW the incident response plan (IR-8). Reporting shall be conducted IAW CJCSM 6510.01B. DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).	LOW			X							---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-6(b)	CCI-002791	The organization defines authorities to whom security incident information is reported.	DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).	LOW					X					---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-7	CCI-000839	The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	The organization being inspected/assessed will establish an incident response support service, analogous to an IT help desk, to provide advice and assistance to users for handling and reporting of security incidents.	The organization conducting the inspection/assessment will interview organizational users to determine awareness of incident response support services and quality of assistance of those services when used. If interviewing organizational users is not feasible, then review users manuals/documentation to ensures it identifies an incident response support service to contact.	LOW			X							---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(a)	CCI-002794	The organization develops an incident response plan.	The organization being inspected/assessed develops and documents an incident response plan.	The organization conducting the inspection/assessment obtains and examines the documented incident response plan to ensure the organization being inspected/assessed develops an incident response plan.	LOW			X							---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(a)(1)	CCI-002795	The organization's incident response plan provides the organization with a roadmap for implementing its incident response capability.	The organization being inspected/assessed defines and documents within their incident response plan, a roadmap for implementing its incident response capability.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed provides within their plan, a roadmap for implementing its incident response capability.	LOW			X							---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IR-8(a)(2)	CCI-002796	The organization's incident response plan describes the structure and organization of the incident response capability.	The organization being inspected/assessed defines and documents within their incident response plan, the structure and organization of the incident response capability.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed describes within their plan, the structure and organization of the incident response capability.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(a)(3)	CCI-002797	The organization's incident response plan provides a high-level approach for how the incident response capability fits into the overall organization.	The organization being inspected/assessed defines and documents within their incident response plan, a high-level approach for how the incident response capability fits into the overall organization.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed provides within their plan, a high-level approach for how the incident response capability fits into the overall organization.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(a)(4)	CCI-002798	The organization's incident response plan meets the unique requirements of the organization, which relate to mission, size, structure, and functions.	The organization being inspected/assessed will ensure their incident response plan meets the unique requirements of the organization, which relate to mission, size, structure, and functions.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure it meets the unique requirements of the organization being inspected/assessed, which relate to mission, size, structure, and functions.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(a)(5)	CCI-002799	The organization's incident response plan defines reportable incidents.	The organization being inspected/assessed defines and document within their incident response plan, reportable incidents IAW CJCSM 6510.01B Table B-A-2.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed defines reportable incidents IAW CJCSM 6510.01B Table B-A-2.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(a)(6)	CCI-002800	The organization's incident response plan provides metrics for measuring the incident response capability within the organization.	The organization being inspected/assessed defines and documents within their incident response plan, metrics for measuring the incident response capability within the organization IAW CJCSM 6510.01B, Enclosure A.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed defines metrics for measuring the incident response capability within the organization IAW CJCSM 6510.01B, Enclosure A.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(a)(7)	CCI-002801	The organization's incident response plan defines the resources and management support needed to effectively maintain and mature an incident response capability.	The organization being inspected/assessed defines and documents within their incident response plan, the resources and management support needed to effectively maintain and mature an incident response capability.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed defines within their plan, the resources and management support needed to effectively maintain and mature an incident response capability.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(a)(8)	CCI-000844	The organization develops an incident response plan that is reviewed and approved by organization-defined personnel or roles.	The organization being inspected/assessed will have an incident response plan signed and approved by at a minimum, the ISSM and ISSO. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization conducting the inspection/assessment obtains and examines the incident response plan to validate it has been properly signed by at a minimum, the ISSM and ISSO. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(a)(8)	CCI-002802	The organization defines personnel or roles to review and approve the incident response plan.	DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-8(b)	CCI-000845	The organization defines incident response personnel (identified by name and/or by role) and organizational elements to whom copies of the incident response plan is distributed.	DoD has defined the list as all stakeholders identified in the incident response plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the list as all stakeholders identified in the incident response plan.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-8(b)	CCI-000846	The organization distributes copies of the incident response plan to organization-defined incident response personnel (identified by name and/or by role) and organizational elements.	The organization being inspected/assessed makes available to all stakeholders identified in the incident response plan via organizationally approved information sharing mechanism. DoD has defined the list as all stakeholders identified in the incident response plan.	The organization conducting the inspection/assessment obtains and examines organizationally approved information sharing mechanism to validate all stakeholders identified in the incident response plan have adequate access to the incident response plan. DoD has defined the list as all stakeholders identified in the incident response plan.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(c)	CCI-000847	The organization defines the frequency for reviewing the incident response plan.	DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-8(c)	CCI-000848	The organization reviews the incident response plan on an organization-defined frequency.	The organization being inspected/assessed will conduct reviews of its incident response plan at least annually. DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).	The organization conducting the inspection/assessment obtains and examines the incident response plan to validate it is current and has been reviewed within the last year. DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-8(d)	CCI-000849	The organization updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	The organization being inspected/assessed must update the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing and incorporate lessons learned from past incidents (IR-4a). The organization must document the update actions as an audit trail.	The organization conducting the inspection/assessment obtains and examines documentation of the update actions for the incident response plan to ensure the organization is updating the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing and incorporating lessons learned from past incidents (IR-4a).	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IR-8(e)	CCI-000850	The organization communicates incident response plan changes to organization-defined incident response personnel (identified by name and/or by role) and organizational elements.	The organization being inspected/assessed communicates incident response plan changes to all stakeholders identified in the incident response plan, not later than 30 days after the change is made. DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made.	The organization conducting the inspection/assessment examines the incident response plan via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been communicated to all stakeholders identified in the incident response plan, not later than 30 days after the change is made. DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(e)	CCI-002803	The organization defines incident response personnel (identified by name and/or by role) and organizational elements to whom the incident response plan changes will be communicated.	DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-8(f)	CCI-002804	The organization protects the incident response plan from unauthorized disclosure and modification.	The organization being inspected/assessed protects the incident response plan from unauthorized disclosure and modification.	The organization conducting the inspection/assessment obtains and examines artifacts which identify how the incident response plan is protected to ensure the organization being inspected/assessed protects the incident response plan from unauthorized disclosure and modification.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-1(a)	CCI-002861	The organization defines the personnel or roles to whom a system maintenance policy is disseminated.	DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	MA-1(a)	CCI-002862	The organization defines the personnel or roles to whom system maintenance procedures are to be disseminated.	DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	MA-1(a)(1)	CCI-000852	The organization develops and documents a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization being inspected/assessed develops and documents a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization conducting the inspection/assessment obtains and examines the documented maintenance policy to ensure the organization being inspected/assessed develops and documents a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-1(a)(1)	CCI-000853	The organization disseminates to organization-defined personnel or roles a system maintenance policy.	The organization being inspected/assessed ensures the maintenance policy is disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	The organization conducting the inspection/assessment obtains and examines the maintenance policy via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-1(a)(2)	CCI-000855	The organization develops and documents procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.	The organization being inspected/assessed documents the maintenance procedures within the Security Plan. The maintenance procedures shall be developed IAW maintenance policy provided in DoDI 8500.01.	The organization conducting the inspection/assessment obtains and examines the Security Plan to ensure maintenance procedures are documented and are developed IAW maintenance policy provided in DoDI 8500.01..	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-1(a)(2)	CCI-000856	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.	The organization being inspected/assessed ensures the maintenance procedures are disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system via an information sharing capability. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	The organization conducting the inspection/assessment examines the maintenance procedures via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-1(b)(1)	CCI-000851	The organization defines the frequency to review and update the current system maintenance policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	MA-1(b)(1)	CCI-000854	The organization reviews and updates the current system maintenance policy in accordance with organization-defined frequency.	The organization being inspected/assessed reviews the current system maintenance policy every 5 years and revises as necessary to comply with DoD regulations. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as every 5 years.	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the maintenance policy to ensure review is occurring every 5 years and updates are made as necessary. DoD has defined the frequency as every 5 years.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-1(b)(2)	CCI-000857	The organization reviews and updates the current system maintenance procedures in accordance with organization-defined frequency.	The organization being inspected/assessed reviews the current system maintenance procedures annually and revises as needed to comply with DoD regulations. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the maintenance procedures to ensure annual review and necessary updates are occurring. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-1(b)(2)	CCI-001628	The organization defines a frequency to review and update the current system maintenance procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(a)	CCI-002866	The organization schedules maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed schedules maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of maintenance.	The organization conducting the inspection/assessment obtains and examines the record of maintenance to ensure the organization being inspected/assessed schedules maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(a)	CCI-002867	The organization performs maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed implements a process to perform maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of maintenance procedures followed.	The organization conducting the inspection/assessment obtains and examines the record of maintenance procedures followed to ensure the organization being inspected/assessed performs maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(a)	CCI-002868	The organization documents maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed documents maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization conducting the inspection/assessment obtains and examines documentation of maintenance to ensure the organization being inspected/assessed documents maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(a)	CCI-002869	The organization reviews records of maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed documents and implements a process to review records of maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews records of maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(a)	CCI-002870	The organization schedules repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements	The organization being inspected/assessed schedules repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of repairs.	The organization conducting the inspection/assessment obtains and examines the record of repairs to ensure the organization being inspected/assessed schedules repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(a)	CCI-002871	The organization performs repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed implements a process to perform repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of repair procedures followed.	The organization conducting the inspection/assessment obtains and examines the record of repair procedures followed to ensure the organization being inspected/assessed performs repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(a)	CCI-002872	The organization documents repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed documents repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization conducting the inspection/assessment obtains and examines documentation of repairs to ensure the organization being inspected/assessed documents repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	MA-2(a)	CCI-002873	The organization reviews records of repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed documents and implements a process to review records of repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews records of repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(b)	CCI-000859	The organization approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.	The organization being inspected/assessed approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. The organization must maintain records of all approvals and monitoring activities.	The organization conducting the inspection/assessment obtains and examines records of all approvals and monitoring activities to ensure the organization being inspected/assessed approves and monitors all maintenance activities whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(c)	CCI-000860	The organization requires that organization-defined personnel or roles explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.	The organization being inspected/assessed documents within their risk management strategy personnel or roles defined in MA-2, CCI 2874 who must explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs. The organization must maintain written records of approval for the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.	The organization conducting the inspection/assessment obtains and examines: 1. the organization's risk management strategy to ensure the personnel or roles defined in MA-2, CCI 2874 have been designated to approve the removal of the information system or system components; 2. and written records of approval for the removal of the information system or system components from organizational facilities for off-site maintenance or repairs to ensure the removal is explicitly approved.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(c)	CCI-002874	The organization defines the personnel or roles who can explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.	The organization being inspected/assessed defines and documents the personnel or roles who can explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles who can explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(d)	CCI-000861	The organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.	The organization being inspected/assessed sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs IAW DoDM 5200.01-V3 for classified media and DoDM 5200.01-V4 for unclassified media. The organization must maintain written records of media sanitization.	The organization conducting the inspection/assessment obtains and examines written records of media sanitization to ensure the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(e)	CCI-000862	The organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	The organization being inspected/assessed identifies and documents the impacted security controls and takes steps to verify that the controls are still functioning properly following maintenance or repair actions.	The organization conducting the inspection/assessment obtains and examines documented evidence of the verification of security controls following maintenance and repair actions to ensure that the organization being inspected/assessed checks all potentially impacted security controls to verify that they are still functioning properly.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(f)	CCI-002875	The organization includes organization-defined maintenance-related information in organizational maintenance records.	The organization being inspected/assessed includes maintenance-related information defined in MA-2, CCI 2876 in organizational maintenance records.	The organization conducting the inspection/assessment obtains and examines maintenance records to ensure they include maintenance-related information defined in MA-2, CCI 2876.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(f)	CCI-002876	The organization defines the maintenance-related information to include in organizational maintenance records.	The organization being inspected/assessed defines and documents the maintenance-related information to include in organizational maintenance records. DoD has determined the maintenance-related information is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented maintenance-related information to ensure the organization being inspected/assessed defines the maintenance-related information to include in organizational maintenance records. DoD has determined the maintenance-related information is not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(a)	CCI-000873	The organization approves nonlocal maintenance and diagnostic activities.	The organization being inspected/assessed documents the procedures for approving non-local maintenance and diagnostic activities within the Security Plan. The organization must maintain records of approved non-local maintenance and diagnostic activities.	The organization conducting the inspection/assessment obtains and examines: 1. the Security Plan to ensure the procedures for approving non-local maintenance and diagnostic activities are documented; and 2. records approving non-local maintenance and diagnostic activities.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(a)	CCI-000874	The organization monitors nonlocal maintenance and diagnostic activities.	The organization being inspected/assessed develops and implements procedures to monitor non-local maintenance and diagnostic activities. Records of monitoring activity must be maintained.	The organization conducting the inspection/assessment obtains and examines: 1. the Security Plan to identify the authorized non-local maintenance and diagnostic activities; and 2. documented procedures to identify how the use of non-local maintenance and diagnostic activities are monitored; and 3. reviews evidence that the monitoring is conducted IAW the documented procedures.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	MA-4(b)	CCI-000876	The organization allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system.	The organization being inspected/assessed: 1. documents within the Security Plan the non local maintenance and diagnostic tools that are allowed; and 2. allows the use of non-local maintenance and diagnostic tools IAW the tools identified in the Security Plan and MA-4, CCI 873.	The organization conducting the inspection/assessment obtains and examines: 1. the Security Plan to ensure non-local maintenance and diagnostic tools have been identified; and 2. maintenance records to ensure only those tools allowed are used IAW MA-4, CCI 873.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(c)	CCI-000877	The organization employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.	The organization being inspected/assessed configures the information system to employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 877.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 877.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(d)	CCI-000878	The organization maintains records for nonlocal maintenance and diagnostic activities.	The organization being inspected/assessed maintains records of authorized non-local maintenance and diagnostic activities.	The organization conducting the inspection/assessment obtains records of authorized non-local maintenance and diagnostic activities, and examines a sampling to verify the organization is maintaining records for all non-local maintenance and diagnostic activities.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(e)	CCI-000879	The organization terminates sessions and network connections when nonlocal maintenance is completed.	The organization being inspected/assessed terminates session and network connections when non-local maintenance is completed. The organization must retain audit logs of session and network connections termination for non-local maintenance.	The organization conducting the inspection/assessment obtains and examines audit logs of session and network connections termination for non-local maintenance to ensure session and network connections are terminated when non-local maintenance is completed.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-5(a)	CCI-000890	The organization establishes a process for maintenance personnel authorization.	The organization being inspected/assessed clearly defines, documents, and establishes a process for the authorization of maintenance personnel.	The organization conducting the inspection/assessment obtains and examines procedures addressing maintenance personnel to ensure that the organization being inspected/assessed has established processes for the authorization of maintenance personnel.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-5(a)	CCI-000891	The organization maintains a list of authorized maintenance organizations or personnel.	The organization being inspected/assessed maintains a current list of authorized maintenance organizations or personnel.	The organization conducting the inspection/assessment obtains and examines the current list of authorized maintenance organizations or personnel to ensure the organization being inspected/assessed is maintaining the list.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-5(b)	CCI-002894	The organization ensures that non-escorted personnel performing maintenance on the information system have required access authorizations.	The organization being inspected/assessed documents and implements a process to ensure that non-escorted personnel performing maintenance on the information system have required access authorizations. The organization must maintain a record of personnel performing maintenance on the information system.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of personnel performing maintenance on the information system to ensure the organization being inspected/assessed ensures that non-escorted personnel performing maintenance on the information system have required access authorizations.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-5(c)	CCI-002895	The organization designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	The organization being inspected/assessed defines and documents organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	The organization conducting the inspection/assessment obtains and examines documented organizational personnel to ensure the organization being inspected/assessed designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MP-1(a)(1)	CCI-000995	The organization develops and documents a media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-1(a)(1)	CCI-000996	The organization disseminates to organization-defined personnel or roles a media protection policy.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures and is disseminated to all users via http://www.dtic.mil/whs/directives/corres/ins1.html. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-1(a)(1)	CCI-002566	The organization defines personnel or roles to whom a documented media protection policy and procedures will be disseminated.	DoD has defined the personnel or roles as all users.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all users.	LOW	X		X	X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	MP-1(a)(2)	CCI-000999	The organization develops and documents procedures to facilitate the implementation of the media protection policy and associated media protection controls.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-1(a)(2)	CCI-001000	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the media protection policy and associated media protection controls.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures and is disseminated to all users via http://www.dtic.mil/whs/directives/corres/ins1.html. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-1(b)(1)	CCI-000997	The organization reviews and updates the current media protection policy in accordance with organization-defined frequency.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-1(b)(1)	CCI-000998	The organization defines a frequency for reviewing and updating the current media protection policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-1(b)(2)	CCI-001001	The organization reviews and updates the current media protection procedures in accordance with organization-defined frequency.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-1(b)(2)	CCI-001002	The organization defines a frequency for reviewing and updating the current media protection procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-2	CCI-001003	The organization restricts access to organization-defined types of digital and/or non-digital media to organization-defined personnel or roles.	The organization being inspected/assessed restricts access to all types of digital and/or non-digital media containing information not cleared for public release to the personnel or roles defined in MP-2, CCI 1005. DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.	The organization conducting the inspection/assessment interviews organizational personnel with information system media protection responsibilities to ensure the organization being inspected/assessed restricts access to all types of digital and/or non-digital media containing information not cleared for public release to the personnel or roles defined in MP-2, CCI 1005. DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-2	CCI-001004	The organization defines types of digital and/or non-digital media for which the organization restricts access.	DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-2	CCI-001005	The organization defines personnel or roles to restrict access to organization-defined types of digital and/or non-digital media.	The organization being inspected/assessed will define and document personnel or roles to restrict access to media IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level, but personnel must be identified IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to restrict access to media to ensure the access is granted IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level, but personnel must be identified IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	MP-6(a)	CCI-001028	The organization sanitizes organization-defined information system media prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies.	The organization being inspected/assessed sanitizes all media prior to disposal, release out of organizational control, or release for reuse IAW DoDM 5200.01 Vol. 1-4 using techniques and procedures IAW NIST SP 800-88. DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88. DoD has defined the information system media as all media.	The organization conducting the inspection/assessment obtains and examines media sanitization records, audit records, any other relevant documents or records, and sanitization tools to ensure sanitization is in compliance with DoDM 5200.01 Vol. 1-4 and uses techniques and procedures IAW NIST SP 800-88. The objective of the review is to verify the organization is sanitizing its digital and non-digital information system media prior to disposal, release for reuse, or release out of the organizational control. DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88. DoD has defined the information system media as all media.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-6(a)	CCI-002578	The organization defines information system media to sanitize prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies.	DoD has defined the information system media as all media.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system media as all media.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-6(a)	CCI-002579	The organization defines the sanitization techniques and procedures in accordance with applicable federal and organization standards and policies to be used to sanitize organization-defined information system media prior to disposal, release out of organizational control, or release for reuse.	DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-6(b)	CCI-002580	The organization employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	The organization being inspected/assessed implements sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. The organization must maintain an audit trail of sanitization actions.	The organization conducting the inspection/assessment obtains and examines the audit trail of sanitization actions to ensure the organization being inspected/assessed implements sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-7	CCI-002581	The organization defines the types of information system media to restrict or prohibit on organization-defined information systems or system components using organization-defined security safeguards.	The organization being inspected/assessed defines and documents the types of information system media to restrict or prohibit on organization-defined information systems or system components using organization-defined security safeguards. DoD has determined the types of information system media are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented type of information system media to ensure the organization being inspected/assessed defines the types of information system media to restrict or prohibit on organization-defined information systems or system components using organization-defined security safeguards. DoD has determined the types of information system media are not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-7	CCI-002582	The organization defines the information systems or system components to restrict or prohibit the use of organization-defined types of information system media using organization-defined security safeguards.	The organization being inspected/assessed defines and documents the information systems or system components to restrict or prohibit the use of organization-defined types of information system media using organization-defined security safeguards. DoD has determined the information systems or system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information systems or system components to ensure the organization being inspected/assessed defines the information systems or system components to restrict or prohibit the use of organization-defined types of information system media using organization-defined security safeguards. DoD has determined the information systems or system components are not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-7	CCI-002583	The organization defines the security safeguards to use for restricting or prohibiting the use of organization-defined types of information system media on organization-defined information systems or system components.	The organization being inspected/assessed defines and documents the security safeguards to use for restricting or prohibiting the use of organization-defined types of information system media on organization-defined information systems or system components. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to use for restricting or prohibiting the use of organization-defined types of information system media on organization-defined information systems or system components. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-7	CCI-002584	The organization restricts or prohibits the use of organization-defined types of information system media on organization-defined information systems or system components using organization-defined security safeguards.	The organization being inspected/assessed documents and enforces controls for the use of media defined in MP-7, CCI 2581 on systems defined in MP-7, CCI 2582 using security safeguards defined in MP-7, CCI 2583.	The organization conducting the inspection/assessment obtains and examines the documented controls and examines information system procedures associated with the use of media to ensure the organization being inspected/assessed documents and enforces controls for the use of media defined in MP-7, CCI 2581 on systems defined in MP-7, CCI 2582 using security safeguards defined in MP-7, CCI 2583.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PE-1(a)	CCI-002908	The organization defines the personnel or roles to whom a physical and environmental protection policy is disseminated.	DoD has defined the roles as organizational personnel with physical and environmental protection responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with physical and environmental protection responsibilities.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-1(a)	CCI-002909	The organization defines the personnel or roles to whom the physical and environmental protection procedures are disseminated.	DoD has defined the roles as organizational personnel with physical and environmental protection responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with physical and environmental protection responsibilities.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-1(a)(1)	CCI-000904	The organization develops and documents a physical and environment protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-1(a)(1)	CCI-000905	The organization disseminates a physical and environmental protection policy to organization-defined personnel or roles.	DoD disseminates DoDI 5200.08 and DoD 5200.08-R organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html DoD has defined the personnel or roles as organizational personnel with physical and environmental protection responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 5200.08 and DoD 5200.08-R DoD has defined the personnel or roles as organizational personnel with physical and environmental protection responsibilities.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-1(a)(2)	CCI-000908	The organization develops and documents procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-1(a)(2)	CCI-000909	The organization disseminates physical and environmental protection procedures to organization-defined personnel or roles.	DoD disseminates DoDI 5200.08 and DoD 5200.08-R organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html DoD has defined the personnel or roles as organizational personnel with physical and environmental protection responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 5200.08 and DoD 5200.08-R DoD has defined the personnel or roles as organizational personnel with physical and environmental protection responsibilities.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-1(b)(1)	CCI-000906	The organization reviews and updates the current physical and environmental protection policy in accordance with organization-defined frequency.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-1(b)(1)	CCI-000907	The organization defines the frequency to review and update the physical and environmental protection policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PE-1(b)(2)	CCI-000910	The organization reviews and updates the current physical and environmental protection procedures in accordance with organization-defined frequency.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R. DoD has defined the frequency as reviewed annually - updated as appropriate.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-1(b)(2)	CCI-000911	The organization defines the frequency to review and update the physical and environmental protection procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
IA-5	IA-5(c)	CCI-001544	The organization manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use.	The organization being inspected/assessed documents and implements authenticator strength mechanisms sufficient for the intended use of the authenticators.	The organization conducting the inspection/assessment obtains and examines documented authenticator strength mechanisms to ensure that they are defined and that the mechanisms have sufficient strength for the intended use of the authenticators.	LOW		X	X	X				3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through the use of physical security and/or contractor requirement to change all default authentication methods within the control system's capability. This is within Sub-Paragraph "User Identification and Authentication" within Part 3

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
IA-5	IA-5(e)	CCI-001989	The organization manages information system authenticators by changing default content of authenticators prior to information system installation.	The organization being inspected/assessed documents and implements a procedures to change default authenticators prior to information system installation.	The organization conducting the inspection/assessment obtains and examines the documented procedures to change default authenticators to ensure the procedures are defined. The organization conducting the inspection/assessment obtains and examines a sampling of authenticator age data for default accounts to ensure that default authenticators are changed prior to installation.	LOW		X						3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through the use of physical security and/or contractor requirement to change all default authentication methods within the control system's capability. This is within Sub-Paragraph "User Identification and Authentication" and further enforced in "Passwords for Devices Minimally Supporting Accounts" within Part 3
N/A	PE-12	CCI-000963	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	The organization being inspected/assessed must install and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility in compliance with established OSHA requirements.	The organization conducting the inspection/assessment conducts visual inspections and interviews physical security personnel to validate the organization is in compliance with established OSHA requirements by employing and maintaining emergency lighting for the information system, the emergency lighting activates in the event of a power outage or disruption, and it covers emergency exits and evacuation routes within the facility	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS does not need lighting, it functions perfectly well in the dark."	
N/A	PE-13	CCI-000965	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	The organization being inspected/assessed must implement and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source. An independent energy source is some source other than the primary energy source for that facility. Examples include sprinkler systems, hand held fire extinguishers, fixed fire hoses, and smoke detectors.	The organization conducting the inspection/assessment will conduct visual observation and interview organizational personnel with responsibilities for fire detection and suppression devices/systems. The purpose of the reviews and interviews is to validate the fire suppression and detection devices/systems for the information system are supported by an independent energy source.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-14(a)	CCI-000971	The organization maintains temperature and humidity levels within the facility where the information system resides at organization-defined acceptable levels.	Humidity controls are not required for general office areas where information system components may be in use and are only required where there are concentrations of information systems such as server farms, mainframes, etc. The organization being inspected/assessed must maintain temperature and where applicable humidity levels of for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications. DoD has defined the acceptable levels as for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications.	The organization conducting the inspection/assessment reviews temperature and humidity controls to validate that they are set within DoD specified guidelines. DoD has defined the acceptable levels as for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-14(a)	CCI-000972	The organization defines acceptable temperature and humidity levels to be maintained within the facility where the information system resides.	DoD has defined the acceptable levels as for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the acceptable levels as for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications.	LOW	X			X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-14(b)	CCI-000973	The organization monitors temperature and humidity levels in accordance with organization-defined frequency.	The organization being inspected/assessed will maintain an independent monitor device for temperature and humidity levels not located in the immediate vicinity of the controller continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required. Records of monitoring must be maintained as an audit trail within the authorization lifecycle. DoD has defined the frequency as continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required.	The organization conducting the inspection/assessment will visually observe the inspected organization's independent monitoring device, obtain and examine audit logs, and interview physical security/safety personnel to validate the inspected organization monitors temperature and humidity levels continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required. DoD has defined the frequency as continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-14(b)	CCI-000974	The organization defines a frequency for monitoring temperature and humidity levels.	DoD has defined the frequency as continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PE-15	CCI-000977	The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible.	The organization being inspected/assessed must provide master shutoff valves that are accessible to protect the information system from damage resulting from water leakage.	The organization conducting the inspection/assessment will inspect the master shutoff valves to ensure they are installed and accessible.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-15	CCI-000978	The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are working properly.	The organization being inspected/assessed will ensure that master shutoff valves are working properly and have been inspected by the appropriate organization (e.g., fire marshal, department of public works).	The organization conducting the inspection/assessment will visually inspect master shutoff valve inspection documentation (e.g., inspection form, tag attached to valve).	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-15	CCI-000979	Key personnel have knowledge of the master water shutoff or isolation valves.	The organization being inspected/assessed will identify and document key personnel and will provide training on the location and procedures for use of master shutoff valves.	The organization conducting the inspection/assessment obtains and examines list of key personnel with knowledge of location and activation procedures for master shutoff valves and any other relevant documents or records. Interview key personnel from the list to determine if identified key personnel within the organization have knowledge of the master shutoff valves.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-16	CCI-000981	The organization authorizes organization-defined types of information system components entering and exiting the facility.	The organization being inspected/assessed authorizes and maintains authorization records of all system components entering and exiting the facility. DoD has defined the types of information system components as all system components.	The organization conducting the inspection/assessment obtains and examines records authorizing all system components entering and exiting the facility. DoD has defined the types of information system components as all system components.	LOW	X		X	X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-16	CCI-000982	The organization monitors organization-defined types of information system components entering and exiting the facility.	The organization being inspected/assessed monitors all system components entering and exiting the facility. DoD has defined the types of information system components as all system components.	The organization conducting the inspection/assessment obtains and examines records monitoring all system components entering and exiting the facility. DoD has defined the types of information system components as all system components.	LOW	X		X	X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-16	CCI-000983	The organization controls organization defined types of information system components entering and exiting the facility.	The organization being inspected/assessed: 1. Documents in their physical and environmental protection plan (PE-1) controls for all system components entering and exiting the facility. 2. Implements documented controls for system components entering and exiting the facility. DoD has defined the types of information system components as all system components.	The organization conducting the inspection/assessment obtains and examines the physical and environmental protection plan to determine if controls have been documented for all system components entering and exiting the facility and visually inspects the controls (e.g., logs, scans, etc.) to ensure implementation. DoD has defined the types of information system components as all system components.	LOW	X		X	X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-16	CCI-000984	The organization maintains records of information system components entering and exiting the facility.	The organization being inspected/assessed will maintain records of all information system components entering and exiting the facility. If the organization is following General Records Schedule (GRS) 18, Section 12 they are automatically compliant.	The organization conducting the inspection/assessment obtains and examines records of physical entry and exit events to the facility. The purpose of the reviews is to ensure the organization is maintaining detailed and accurate records of information system components that enter and exit the facility. If the organization is following GRS 18, Section 12 they are automatically compliant.	LOW	X		X	X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-16	CCI-002974	The organization defines types of information system components to authorize, monitor, and control entering and exiting the facility and to maintain records.	DoD has defined the types of information system components as all system components.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the types of information system components as all system components.	LOW	X		X	X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-2(a)	CCI-000912	The organization develops a list of individuals with authorized access to the facility where the information system resides.	The organization being inspected/assessed will develop and maintain a list of personnel with authorized access to the facilities where information systems reside. The organization will also take action to identify and officially designate its publicly accessible areas where access authorization is not required.	The organization conducting the inspection/assessment obtains and examines the list of personnel with authorized access to facilities where information systems reside to ensure it is current within every 90 days. The review process should also determine if the organization has identified and officially designated its publicly accessible areas where access authorization is not required. DoD has defined the frequency as every 90 days.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-2(a)	CCI-002910	The organization approves a list of individuals with authorized access to the facility where the information system resides.	The organization being inspected/assessed formally approves a list of individuals currently authorized to access the facility where the information system resides.	The organization conducting the inspection/assessment obtains and examines the list of individuals currently authorized to access the facility where the information system resides and ensures it is formally approved.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-2(a)	CCI-002911	The organization maintains a list of individuals with authorized access to the facility where the information system resides.	The organization being inspected/assessed maintains a list of individuals currently authorized to access the facility where the information system resides.	The organization conducting the inspection/assessment obtains and examines the list of individuals to ensure the organization being inspected/assessed maintains a list of individuals currently authorized to access the facility where the information system resides.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-2(b)	CCI-000913	The organization issues authorization credentials for facility access.	The organization being inspected/assessed utilizes the list of personnel with authorized access (IAW PE-2, CCI-000912) and issues credentials accordingly. The organization must document the credential issuing activity as an audit trail.	The organization conducting the inspection/assessment obtains and examines documentation of credential issuing activities to ensure credentials are issued to personnel with authorized access.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PE-2(c)	CCI-000914	The organization reviews the access list detailing authorized facility access by individuals in accordance with organization-defined frequency.	The organization being inspected/assessed will review the access list and authorization credentials every 90 days and document these review and approval actions as an audit trail. DoD has defined the frequency as every 90 days.	The organization conducting the inspection/assessment obtains and examines the audit records of the review actions to ensure that reviews are conducted every 90 days. DoD has defined the frequency as every 90 days.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-2(c)	CCI-000915	The organization defines the frequency to review the access list detailing authorized facility access by individuals.	DoD has defined the frequency as every 90 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 90 days.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-2(c)	CCI-001635	The organization removes individuals from the facility access list when access is no longer required.	The organization being inspected/assessed will remove personnel from the authorized access list who no longer have approved access and revoke their credentials, as identified in actions per PE-2, CCI 914. The organization must document each removal and revocation action as an audit trail.	The organization conducting the inspection/assessment obtains and examines the review and approval actions documentation to ensure that personnel no longer requiring access have been removed from the authorized access list and their credentials have been revoked.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(a)	CCI-000919	The organization enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides.	The organization being inspected/assessed will implement physical access authorizations at entry/exit points defined in PE-3, CCI 2915 and secure those physical access points (i.e. doors and/or windows) that are not intended for normal access.	The organization conducting the inspection/assessment performs a physical inspection of facility entry/exit points defined in PE-3, CCI 2915 to ensure that either physical access authorization controls are in place for those access points considered normal access points or are properly secured. Physical access points that are not documented or are not secured would be a failure of this control.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(a)	CCI-002915	The organization defines the entry/exit points to the facility where the information system resides.	The organization being inspected/assessed defines and documents the entry/exit points to the facility where the information system resides. DoD has determined the entry/exit points are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented entry/exit points and inspects the facility to ensure that all entry/exit points are documented. DoD has determined the entry/exit points are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(a)(1)	CCI-000920	The organization verifies individual access authorizations before granting access to the facility.	The organization being inspected/assessed verifies and grants access to facilities based upon individual access authorizations.	The organization conducting the inspection/assessment obtains and examines the access authorization list of personnel that have access to the facility (per access list implemented through PE-2, CCI 000912) where the information system resides. Inspect selected facilities to confirm the inspected organization is granting access at all physical access points to only authorized personnel.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(a)(2)	CCI-000921	The organization controls ingress/egress to the facility using one or more organization-defined physical access control systems/devices or guards.	The organization being inspected/assessed will control ingress/egress to the facility using the physical access control devices and/or guards defined in PE-3, CCI 2916.	The organization conducting the inspection/assessment obtains and examines the list of physical access control devices and/or guards in use defined in PE-3, CCI 2916 and conducts random inspections of entry points. The purpose is to determine whether the organization is using those physical access devices and/or guards to control entry of personnel into the facility hosting the information system.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(a)(2)	CCI-002916	The organization defines the physical access control systems/devices or guards that control ingress/egress to the facility.	The organization being inspected/assessed defines and documents the physical access control systems/devices or guards that control ingress/egress to the facility. DoD has determined the physical access control systems/devices are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented physical access control systems/devices to ensure the organization being inspected/assessed defines the physical access control systems/devices or guards that control ingress/egress to the facility. DoD has determined the physical access control systems/devices are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(b)	CCI-002917	The organization maintains physical access audit logs for organization-defined entry/exit points.	The organization being inspected/assessed maintains physical access audit logs for entry/exit points defined in PE-3, CCI 2918.	The organization conducting the inspection/assessment obtains and examines the physical access audit logs and compares the logged entry with known access to those entry points to ensure the organization being inspected/assessed maintains physical access audit logs for entry/exit points defined in PE-3, CCI 2918. Instances of access that will be compared with the audit logs include, at a minimum, access as part of the inspection/assessment. Comparison of other entry/exit events required elsewhere in system documentation that would have occurred before the inspection/assessment such as daily checks and scheduled maintenance are strongly encouraged and help to establish a history of compliance/non-compliance.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PE-3(b)	CCI-002918	The organization defines entry/exit points that require physical access audit logs be maintained.	The organization being inspected/assessed defines and documents entry/exit points that require physical access audit logs be maintained. DoD has determined the entry/exit points are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented entry/exit points to ensure the organization being inspected/assessed defines entry/exit points that require physical access audit logs be maintained. DoD has determined the entry/exit points are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(c)	CCI-002919	The organization provides organization-defined security safeguards to control access to areas within the facility officially designated as publicly accessible.	The organization being inspected/assessed provides security safeguards defined in PE-3, CCI 2920 to control access to areas within the facility officially designated as publicly accessible. The organization must document which areas are officially designated as publicly accessible.	The organization conducting the inspection/assessment obtains and examines the documentation of areas officially designated as publicly accessible to ensure the organization being inspected/assessed provides security safeguards defined in PE-3, CCI 2920 to control access to areas within the facility officially designated as publicly accessible.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(c)	CCI-002920	The organization defines security safeguards to control access to areas within the facility officially designated as publicly accessible.	The organization being inspected/assessed defines and documents security safeguards to control access to areas within the facility officially designated as publicly accessible. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines security safeguards to control access to areas within the facility officially designated as publicly accessible. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(d)	CCI-002921	The organization escorts visitors during organization-defined circumstances requiring visitor escorts.	The organization being inspected/assessed documents and implements a process to escort visitors during circumstances defined in PE-3, CCI 2922 requiring visitor escorts.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed escorts visitors during circumstances defined in PE-3, CCI 2922 requiring visitor escorts.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(d)	CCI-002922	The organization defines circumstances requiring visitor escorts.	The organization being inspected/assessed defines and documents circumstances requiring visitor escorts. DoD has determined the circumstances are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented circumstances to ensure the organization being inspected/assessed defines circumstances requiring visitor escorts. DoD has determined the circumstances are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(d)	CCI-002923	The organization monitors visitor activity during organization-defined circumstances requiring visitor monitoring.	The organization being inspected/assessed documents and implements a process to monitor visitor activity during circumstances defined in PE-3, CCI 2924 requiring visitor monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed monitors visitor activity during circumstances defined in PE-3, CCI 2924 requiring visitor monitoring.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(d)	CCI-002924	The organization defines circumstances requiring visitor monitoring.	The organization being inspected/assessed defines and documents circumstances requiring visitor monitoring. DoD has determined the circumstances are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented circumstances to ensure the organization being inspected/assessed defines circumstances requiring visitor monitoring. DoD has determined the circumstances are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(e)	CCI-000923	The organization secures keys, combinations, and other physical access devices.	The organization being inspected/assessed will secure as appropriate (in safes or secure containers) items used for physical access control such as keys, combinations, portable locks, etc. Fixed access control devices such as card readers, installed locks, key pads, etc. should be protected from tampering.	The organization conducting the inspection/assessment conducts physical inspections and interviews physical security/safety personnel to validate the organization has taken the proper precautions, and established the proper procedures to ensure it has adequately secured its keys, combinations, and other physical devices.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(f)	CCI-000924	The organization inventories organization-defined physical access devices every organization-defined frequency.	The organization being inspected/assessed conducts and documents an inventory of minimally keys or any other physical token used to gain access annually. Inventory documents must be retained for at least one year beyond the completion of the next inventory. DoD has defined the frequency as annually. DoD has defined the physical access devices as minimally keys or any other physical token used to gain access.	The organization conducting the inspection/assessment obtains and examines the records of inventory of minimally keys or any other physical token used to gain access to ensure the inventory is being conducted annually. DoD has defined the frequency as annually. DoD has defined the physical access devices as minimally keys or any other physical token used to gain access.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(f)	CCI-000925	The organization defines the frequency for conducting inventories of organization-defined physical access devices.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(f)	CCI-002925	The organization defines the physical access devices to inventory.	DoD has defined the physical access devices as minimally keys or any other physical token used to gain access.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the physical access devices as minimally keys or any other physical token used to gain access.	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PE-3(g)	CCI-000926	The organization changes combinations and keys in accordance with organization-defined frequency and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.	The organization being inspected/assessed will document each occurrence of these change actions, with the reason for the action, as an audit trail for future reference. DoD has defined the frequency as required by security relevant events.	The organization conducting the inspection/assessment obtains and examines documentation of these change actions to validate the organization is changing its keys and combinations upon occurrence of security relevant events and when keys are lost, combinations are compromised, or individuals are transferred or terminated. DoD has defined the frequency as required by security relevant events.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(g)	CCI-000927	The organization defines a frequency for changing combinations and keys.	DoD has defined the frequency as required by security relevant event.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as required by security relevant event.	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-6(a)	CCI-002939	The organization monitors physical access to the facility where the information system resides to detect and respond to physical security incidents.	The organization being inspected/assessed will implement monitoring procedures to ensure physical access intrusion alarms and surveillance equipment are actively monitored to detect and respond to all physical access security incidents.	The organization conducting the inspection/assessment obtains and examines the inspected organization's monitoring procedures addressing physical access monitoring. Organizational personnel with physical access monitoring responsibilities are to be interviewed. The objective of the reviews and interviews is to validate the organization is actively monitoring its physical access intrusion alarms and surveillance equipment to detect and respond to all physical access security incidents.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-6(b)	CCI-000939	The organization reviews physical access logs in accordance with organization-defined frequency.	The organization being inspected/assessed will review physical access logs every 30 days. The organization must document each occurrence the physical access log review, with results of any necessary incident analysis and action taken, as an audit trail for future reference. DoD has defined the frequency as every 30 days.	The organization conducting the inspection/assessment obtains and examines the inspected organization's physical access logs or records; physical access incident reports; and any other relevant documents or records. The purpose of the reviews is to determine if the organization is conducting reviews of the physical access logs every 30 days. DoD has defined the frequency as every 30 days.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-6(b)	CCI-000940	The organization defines a frequency for reviewing physical access logs.	DoD has defined the frequency as every 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 30 days.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PE-6(b)	CCI-002940	The organization reviews physical access logs upon occurrence of organization-defined events or potential indications of events	The organization being inspected/assessed documents and implements a process to review physical access logs upon occurrence of events or potential indications of events defined in PE-6, CCI 2941. The organization must maintain records of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of reviews to ensure the organization being inspected/assessed reviews physical access logs upon occurrence of events or potential indications of events defined in PE-6, CCI 2941.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-6(b)	CCI-002941	The organization defines events or potential indications of events requiring review of physical access logs.	The organization being inspected/assessed defines and documents events or potential indications of events requiring review of physical access logs. DoD has determined the events or potential indications of events are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented events or potential indications of events to ensure the organization being inspected/assessed defines events or potential indications of events requiring review of physical access logs. DoD has determined the events or potential indications of events are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-6(c)	CCI-000941	The organization coordinates results of reviews and investigations with the organizations incident response capability.	The organization being inspected/assessed will coordinate the results of reviews and investigations of physical security incidents with the organization's incident response capability (for physical security incidents).	The organization conducting the inspection/assessment obtains and examines documentation of physical security incidents to ensure coordination with the inspected organization's incident response capability occurred.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-8(a)	CCI-000947	The organization maintains visitor access records to the facility where the information system resides for organization-defined time period.	The organization being inspected/assessed must maintain visitor access records for their facilities for at least one year. DoD has defined the time period as at least one year.	The organization conducting the inspection/assessment obtains and examines visitor access records to determine if the organization is maintaining visitor access records to the facility where the information system resides for at least one year. DoD has defined the time period as at least one year.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-8(a)	CCI-002952	The organization defines the time period to maintain visitor access records to the facility where the information system resides.	DoD has defined the time period as at least one year.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as at least one year.	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-8(b)	CCI-000948	The organization reviews visitor access records in accordance with organization-defined frequency.	The organization being inspected/assessed conducts reviews of visitor access records every 30 days and must establish and maintain a documented audit trail within the authorization lifecycle. DoD has defined the frequency as every 30 days.	The organization conducting the inspection/assessment obtains and examines the audit documentation of visitor access record review to ensure the inspected organization is conducting reviews every 30 days. DoD has defined the frequency as every 30 days.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-8(b)	CCI-000949	The organization defines the frequency to review the visitor access records for the facility where the information system resides.	DoD has defined the frequency as every 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 30 days.	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PL-1(a)	CCI-003047	The organization defines the personnel or roles to whom a security planning policy is disseminated.	DoD has defined the roles as all organizational personnel with planning responsibilities or information security responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as all personnel organizational personnel with planning responsibilities or information security responsibilities.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-1(a)	CCI-003048	The organization defines the personnel or roles to whom the security planning procedures are disseminated.	DoD has defined the roles as all organizational personnel with planning responsibilities or information security responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as all organizational personnel with planning responsibilities or information security responsibilities.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-1(a)(1)	CCI-000563	The organization develops and documents a security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 8510.01 meets the requirements for a security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.	DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-1(a)(1)	CCI-000564	The organization disseminates a security planning policy to organization-defined personnel or roles .	DoD disseminates DoDI 8510.01 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) to organizational personnel with planning responsibilities or information security responsibilities. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-1(a)(2)	CCI-000566	The organization develops and documents procedures to facilitate the implementation of the security planning policy and associated security planning controls.	DoDI 8510.01 meets the requirements for developing and documenting procedures to facilitate the implementation of the security planning policy and associated security planning controls. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.	DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-1(b)(1)	CCI-001636	The organization defines the frequency to review and update the current security planning policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PL-1(b)(1)	CCI-001637	The organization reviews and updates the current security planning policy in accordance with organization-defined frequency.	DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the frequency as every 5 years.	DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the frequency as every 5 years.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-1(b)(2)	CCI-000567	The organization disseminates security planning procedures to organization-defined personnel or roles.	DoD disseminates DoDI 8510.01 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) to organizational personnel with planning responsibilities or information security responsibilities. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-1(b)(2)	CCI-000568	The organization reviews and updates the current security planning procedures in accordance with organization-defined frequency.	DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the frequency as reviewed annually - updated as appropriate.	DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PL-1(b)(2)	CCI-001638	The organization defines the frequency to review and update the current security planning procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PL-2(3)	CCI-003065	The organization plans and coordinates security-related activities affecting the information system with organization-defined individuals or groups before conducting such activities in order to reduce the impact on other organizational entities.	The organization being inspected/assessed defines and documents within the security plan, the planning and coordination of security-related activities affecting the information system with individuals or groups defined in PL-2 (3), CCI 3067 before conducting such activities in order to reduce the impact on other organizational entities.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed plans and coordinates of security-related activities affecting the information system with individuals or groups defined in PL-2 (3), CCI 3067 before conducting such activities in order to reduce the impact on other organizational entities.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(3)	CCI-003067	The organization defines the individuals or groups with whom security-related activities are planned and coordinated.	The organization being inspected/assessed defines and documents the individuals or groups with whom security-related activities are planned and coordinated. DoD has determined the individuals or groups are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented individuals or groups to ensure the organization being inspected/assessed defines the individuals or groups with whom security-related activities are planned and coordinated. DoD has determined the individuals or groups are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(a)	CCI-003049	The organization develops a security plan for the information system.	The organization being inspected/assessed develops and documents a security plan for the information system.	The organization conducting the inspection/assessment obtains and examines the documented security plan to ensure the organization being inspected/assessed develops a security plan for the information system.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(a)(1)	CCI-003050	The organization's security plan for the information system is consistent with the organization's enterprise architecture.	The organization being inspected/assessed defines a security plan for the information system which is consistent with the organization's enterprise architecture.	The organization conducting the inspection/assessment obtains and examines the security plan and the enterprise architecture to ensure the organization's security plan for the information system is consistent with the organization's enterprise architecture.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
IA-5	IA-5(g)	CCI-000182	The organization manages information system authenticators by changing/refreshing authenticators in accordance with the organization defined time period by authenticator type.	The organization being inspected/assessed documents and implements procedures for changing/refreshing authenticators in the following time periods: CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years. DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	The organization conducting the inspection/assessment obtains and examines the documented procedures for authenticator change/refresh to ensure the procedures are defined. The organization conducting the inspection/assessment obtains and examines a sampling of authenticator age data to ensure that authenticators are changed or refreshed in the following time periods: CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years. DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	LOW		X	X	X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "USER IDENTIFICATION AND AUTHENTICATION"
N/A	PL-2(a)(3)	CCI-003052	The organization's security plan for the information system describes the operational context of the information system in terms of missions and business processes.	The organization being inspected/assessed describes within the security plan the operational context of the information system in terms of missions and business processes.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed describes within the security plan the operational context of the information system in terms of missions and business processes.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
IA-5	IA-5(g)	CCI-001610	The organization defines the time period (by authenticator type) for changing/refreshing authenticators.	DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	LOW		X	X	X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	PL-2(a)(5)	CCI-003054	The organization's security plan for the information system describes the operational environment for the information system and relationships with or connections to other information systems.	The organization being inspected/assessed describes within the security plan the operational environment for the information system and relationships with or connections to other information systems.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed describes within the security plan the operational environment for the information system and relationships with or connections to other information systems.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(a)(6)	CCI-003055	The organization's security plan for the information system provides an overview of the security requirements for the system	The organization being inspected/assessed documents within the security plan, an overview of the security requirements for the system.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed their security plan for the information system provides an overview of the security requirements for the system	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(a)(7)	CCI-003056	The organization's security plan for the information system identifies any relevant overlays, if applicable.	The organization being inspected/assessed identifies within the security plan any relevant overlays, if applicable.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed identifies within the security plan any relevant overlays, if applicable.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(a)(8)	CCI-003057	The organization's security plan for the information system describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions.	The organization being inspected/assessed describes within the security plan the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed describes within the security plan the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PL-2(a)(9)	CCI-000571	The organization's security plan for the information system is reviewed and approved by the authorizing official or designated representative prior to plan implementation.	The organization being inspected/assessed obtains security plan approval by the authorizing official or designated representative prior to plan implementation.	The organization conducting the inspection/assessment obtains and examines the security plan approval to ensure the organization being inspected/assessed obtains security plan approval by the authorizing official or designated representative prior to plan implementation.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(b)	CCI-003059	The organization distributes copies of the security plan to organization-defined personnel or roles.	The organization being inspected/assessed distributes copies of the security plan to, at a minimum, the ISSO, ISSM and SCA via the organization's information sharing portal. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	The organization conducting the inspection/assessment obtains and examines the security plan via the organization's information sharing portal to ensure the organization being inspected/assessed distributes copies of the security plan to at a minimum, the ISSO, ISSM and SCA via the organization's information sharing portal. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(b)	CCI-003060	The organization defines the personnel or roles to whom copies of the security plan is distributed.	DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PL-2(b)	CCI-003061	The organization communicates subsequent changes to the security plan to organization-defined personnel or roles.	The organization being inspected/assessed distributes changes to the security plan to, at a minimum, the ISSO, ISSM and SCA via the organization's information sharing portal. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	The organization conducting the inspection/assessment examines the organization's information sharing portal to ensure at a minimum, the ISSO, ISSM and SCA have been provided changes to the security plan. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(b)	CCI-003062	The organization defines the personnel or roles to whom changes to the security plan are communicated.	DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PL-2(c)	CCI-000572	The organization defines the frequency for reviewing the security plan for the information system.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PL-2(c)	CCI-000573	The organization reviews the security plan for the information system in accordance with organization-defined frequency.	The information system owner as part of the annual security control review will also review the security plan annually. Documentation of security plan reviews is required as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit records of security plan reviews to verify the security plan has been reviewed annually. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(d)	CCI-000574	The organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.	The information system owner will update the security plan as necessary to address changes to information system/environment of operation or problems identified during plan implementation or security control assessments. Documentation of security plan updates are required as an audit trail.	The organization conducting the inspection/assessment obtains and examines the audit records of security plan updates to verify the security plan is current. The purpose of the reviews is to validate the organization is updating the Information System (IS) security plan to address changes to the IS, its environment of operation, or problems identified during plan implementation or security control assessments.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(e)	CCI-003063	The organization protects the security plan from unauthorized disclosure.	The organization being inspected/assessed documents and implements a process to protect the security plan from unauthorized disclosure.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects the security plan from unauthorized disclosure.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(e)	CCI-003064	The organization protects the security plan from unauthorized modification.	The organization being inspected/assessed documents and implements a process to protect the security plan from unauthorized modification.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects the security plan from unauthorized	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-4(a)	CCI-000592	The organization establishes the rules describing the responsibilities and expected behavior, with regard to information and information system usage, for individuals requiring access to the information system.	The organization being inspected/assessed must develop and document rules that describe information system user responsibilities and expected behavior with regard to information and information system usage, acceptable use policy (AUP). Organizations should reference Joint Ethics Regulations (DoD 5500.7-R) when developing this policy.	The organization conducting the inspection/assessment obtains and examines the organization's AUP to ensure the organization has clearly defined and established rules describing information system user responsibilities and expected behavior with regard to information and information system usage.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-4(a)	CCI-001639	The organization makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.	The organization being inspected/assessed must disseminate to all information system users, via an information sharing capability, rules that describe information system user responsibilities and expected behavior with regard to information and information system usage, acceptable use policy (AUP). Organizations should disseminate the rules by providing to users and requiring signature of acceptance.	The organization conducting the inspection/assessment obtains and examines rules that describe information system user responsibilities via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PL-4(b)	CCI-000593	The organization receives a signed acknowledgment from individuals requiring access the system, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	The organization being inspected/assessed will obtain signed acknowledgment (paper or electronic signature) from individuals indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	The organization conducting the inspection/assessment obtains a list of individuals with active accounts and validates the existence of signed acknowledgements (paper or electronic signature) of the organizational AUP associated with a sampling of individuals selected from the list.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-4(c)	CCI-003068	The organization reviews and updates the rules of behavior in accordance with organization-defined frequency.	The organization being inspected/assessed reviews and updates the rules of behavior annually. The organization must maintain an audit trail of reviews and updates. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the rules of behavior annually. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-4(c)	CCI-003069	The organization defines the frequency to review and update the rules of behavior.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PL-4(d)	CCI-003070	The organization requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.	The organization being inspected/assessed documents and implements a process to require individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated. The signed acknowledgment portion of this control may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-1(a)(1)	CCI-000073	The organization develops an organization-wide information security program plan that provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X		X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-1(a)(1)	CCI-002985	The organization disseminates an organization-wide information security program plan that provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) and the Knowledge Service is available via: https://rmfks.osd.mil. DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-1(a)(2)	CCI-001680	The organization develops an organization-wide information security program plan that includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-1(a)(2)	CCI-002986	The organization disseminates an organization-wide information security program plan that includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) and the Knowledge Service is available via: https://rmfks.osd.mil. DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-1(a)(3)	CCI-002984	The organization develops an organization-wide information security program plan that reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical).	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PM-1(a)(3)	CCI-002987	The organization disseminates an organization-wide information security program plan that reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical).	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) and the Knowledge Service is available via: https://rmfks.osd.mil. DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-1(a)(4)	CCI-000074	The organization develops an organization-wide information security program plan that is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-1(a)(4)	CCI-002988	The organization disseminates an organization-wide information security program plan that is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) and the Knowledge Service is available via: https://rmfks.osd.mil. DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-1(b)	CCI-000075	The organization reviews the organization-wide information security program plan on an organization-defined frequency.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X		X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-1(b)	CCI-000076	The organization defines the frequency to review the organization-wide information security program plan.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-1(c)	CCI-000077	The organization updates the plan to address organizational changes and problems identified during plan implementation or security control assessments.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X		X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-1(d)	CCI-002989	The organization protects the information security program plan from unauthorized disclosure.	DoD documents and implements methods to protect the information security program plan from unauthorized disclosure by marking, labeling, and handling to prevent unauthorized disclosure. DoD ensures that all changes to the information security program plan are approved.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-1(d)	CCI-002990	The organization protects the information security program plan from unauthorized modification.	DoD documents and implements methods to protect the information security program plan from unauthorized disclosure by marking, labeling, and handling to prevent unauthorized modification. DoD ensures that all changes to the information security program plan are approved.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-10(a)	CCI-000229	The organization documents the security state of organizational information systems and the environments in which those systems operate through security authorization processes.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-10(a)	CCI-000230	The organization tracks the security state of organizational information systems and the environments in which those systems operate through security authorization processes.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-10(a)	CCI-000231	The organization reports the security state of organizational information systems and the environments in which those systems operate through security authorization processes.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-10(b)	CCI-000233	The organization designates individuals to fulfill specific roles and responsibilities within the organizational risk management process.	DoDI 8510.01 meets the DoD requirement to designate roles and responsibilities for the risk management process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to designate roles and responsibilities for the risk management process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PM-10(c)	CCI-000234	The organization fully integrates the security authorization processes into an organization-wide risk management program.	DoDI 8510.01 meets the DoD requirement to fully integrate the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to fully integrate the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-11(a)	CCI-000235	The organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	DoDI 8510.01 meets the DoD requirement to define mission/business processes. DoD components are automatically complaint with this CCI as they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to define mission/business processes. DoD components are automatically complaint with this CCI as they are covered at the DoD level, DoDI 8510.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-11(b)	CCI-000236	The organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs are obtained.	The organization being inspected/asssessed determines information protection needs IAW CNSSI 1253 and as identified in RA-2.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the security categorization has been documented IAW CNSSI 1253.	LOW	X	X	X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-12	CCI-002996	The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.	The organization being inspected/assessed documents and implements an insider threat program that includes a cross-discipline insider threat incident handling team.	The organization conducting the inspection/assessment obtains and examines the documented insider threat program to ensure the organization being inspected/assessed implements an insider threat program that includes a cross-discipline insider threat incident handling team.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-13	CCI-002997	The organization establishes an information security workforce development and improvement program.	DoD 8570.01-M, "Information Assurance Workforce Improvement Program" meets the DoD requirement to establish an information security workforce development and improvement program. DoD components are automatically complaint with this CCI as they are covered at the DoD level, DoDI 8570.01-M.	DoD 8570.01-M meets the DoD requirement to establish an information security workforce development and improvement program. DoD components are automatically complaint with this CCI as they are covered at the DoD level, DoDI 8570.01-M.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-14(a)(1)	CCI-002998	The organization implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are developed.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are developed.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are developed.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-14(a)(1)	CCI-002999	The organization implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are maintained.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are maintained.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are maintained.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-14(a)(1)	CCI-003000	The organization implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are developed.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are developed.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-14(a)(1)	CCI-003001	The organization implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are maintained.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are maintained.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-14(a)(1)	CCI-003002	The organization implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are developed.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are developed.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-14(a)(1)	CCI-003003	The organization implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are maintained.	The organization being inspected/assessed documents and implements a process for conducting security monitoring activities associated with organizational information systems are maintained.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-14(a)(2)	CCI-003004	The organization implements a process for ensuring that organizational plans for conducting security testing associated with organizational information systems continue to be executed in a timely manner.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security testing associated with organizational information systems continue to be executed in a timely manner. The organization must maintain records of execution.	The organization conducting the inspection/assessment obtains and examines the documented process as well as records of execution to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security testing associated with organizational information systems continue to be executed in a timely manner.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-14(a)(2)	CCI-003005	The organization implements a process for ensuring that organizational plans for conducting security training associated with organizational information systems continue to be executed in a timely manner.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security training associated with organizational information systems continue to be executed in a timely manner. The organization must maintain records of execution.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of execution to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security training associated with organizational information systems continue to be executed in a timely manner.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PM-14(a)(2)	CCI-003006	The organization implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems continue to be executed in a timely manner.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems continue to be executed in a timely manner. The organization must maintain records of execution.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of execution to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems continue to be executed in a timely manner.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-14(b)	CCI-003007	The organization reviews testing plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	The organization being inspected/assessed documents and implements a process to review testing plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews testing plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-14(b)	CCI-003008	The organization reviews training plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	The organization being inspected/assessed reviews training plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews training plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-14(b)	CCI-003009	The organization reviews monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	The organization being inspected/assessed reviews monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-15(a)	CCI-003010	The organization establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel.	The organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel.	The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-15(b)	CCI-003011	The organization establishes and institutionalizes contact with selected groups and associations within the security community to maintain currency with recommended security practices, techniques, and technologies.	The organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to maintain currency with recommended security practices, techniques, and technologies.	The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to maintain currency with recommended security practices, techniques, and technologies.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-15(c)	CCI-003012	The organization establishes and institutionalizes contact with selected groups and associations within the security community to share current security-related information including threats, vulnerabilities, and incidents.	The organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to share current security-related information including threats, vulnerabilities, and incidents.	The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to share current security-related information including threats, vulnerabilities, and incidents.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-16	CCI-003013	The organization implements a threat awareness program that includes a cross-organization information-sharing capability.	The organization being inspected/assessed documents and implements a threat awareness program that includes a cross-organization information-sharing capability.	The organization conducting the inspection/assessment obtains and examines the documented threat awareness program to ensure the organization being inspected/assessed implements a threat awareness program that includes a cross-organization information-sharing capability.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-2	CCI-000078	The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	The Deputy DoD CIO for Cyber Security is the DoD Senior Information Security Officer (SISO), appointed in writing with the mission and resources to coordinate, develop, implement and maintain a DoD-wide information security program.	DoD organizations are automatically compliant with this CCI as they are covered by the appointment of the DoD SISO.	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PM-3(a)	CCI-000080	The organization ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement.	The organization being inspected/assessed documents and implements a process to ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-3(b)	CCI-000081	The organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required.	The organization being inspected/assessed documents and implements a process to employ a business case/Exhibit 300/Exhibit 53 to record the resources required.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs a business case/Exhibit 300/Exhibit 53 to record the resources required.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-3(c)	CCI-000141	The organization ensures that information security resources are available for expenditure as planned.	The organization being inspected/assessed documents and implements a process to ensure that information security resources are available for expenditure as planned.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensure that information security resources are available for expenditure as planned.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PM-4(a)(1)	CCI-000142	The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process for plans of action and milestones for the security program. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process for plans of action and milestones for the security program. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-4(a)(1)	CCI-002991	The organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems are developed.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to develop a process for plans of action and milestones for the security program. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to develop a process for plans of action and milestones for the security program. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-4(a)(2)	CCI-000170	The organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-4(a)(3)	CCI-002992	The organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems are reported in accordance with OMB FISMA reporting requirements.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to implement a process ensuring that the plans of action and milestones for the security program are reported in accordance with OMB FISMA reporting requirements. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to implement a process ensuring that the plans of action and milestones for the security program are reported in accordance with OMB FISMA reporting requirements. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-4(b)	CCI-002993	The organization reviews plans of action and milestones for the security program and associated organization information systems for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	The organization being inspected/assessed documents and implements a process to review plans of action and milestones for the security program and associated organization information systems for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews plans of action and milestones for the security program and associated organization information systems for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
PM-5	PM-5	CCI-000207	The organization develops and maintains an inventory of its information systems.	DITPR is the inventory for all DoD information systems. The organization being inspected/assessed must register and maintain their information systems in DITPR.	DITPR is the inventory for all DoD information systems. The organization conducting the inspection/assessment obtains and examines the inventory of information systems via DITPR to ensure the organization being inspected/assessed registers their information systems in DITPR.	LOW		X	X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-6	CCI-000209	The organization develops the results of information security measures of performance.	The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance.	The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance. DoD organizations are automatically compliant with this CCI as they are covered at the DoD level by FISMA.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-6	CCI-000210	The organization monitors the results of information security measures of performance.	The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance.	The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance. DoD organizations are automatically compliant with this CCI as they are covered at the DoD level by FISMA.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-6	CCI-000211	The organization reports on the results of information security measures of performance.	The organization being inspected/assessed reports the results of information security measures of performance IAW FISMA reporting guidance.	The organization conducting the inspection/assessment obtains and examines FISMA reporting documentation.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-7	CCI-000212	The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	The GIG IA Architecture meets the DoD requirements for enterprise architecture. DoD components are automatically compliant with this CCI as they covered at the DoD level.	The GIG IA Architecture meets the DoD requirements for enterprise architecture. DoD components are automatically compliant with this CCI as they covered at the DoD level.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-8	CCI-000216	The organization develops and documents a critical infrastructure and key resource protection plan that addresses information security issues.	DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan. DoD components are automatically compliant with this CCI as they are covered by the DoD level, DoDD 3020.40.	DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan. DoD components are automatically compliant with this CCI as they are covered by the DoD level, DoDD 3020.40.	LOW							A LOW Control System doesn't deal with critical infrastructure.	---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PM-8	CCI-001640	The organization updates the critical infrastructure and key resources protection plan that addresses information security issues.	DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan. DoD components are automatically compliant with this CCI as they are covered by the DoD level, DoDD 3020.40.	DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan. DoD components are automatically compliant with this CCI as they are covered by the DoD level, DoDD 3020.40.	LOW							A LOW Control System doesn't deal with critical infrastructure.	---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-9(a)	CCI-000227	The organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems.	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by the DoD Risk Management Framework (DoDI 8510.01).	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by DoD Risk Management Framework (DoDI 8510.01).	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-9(b)	CCI-000228	The organization implements a comprehensive strategy to manage risk to organization operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems consistently across the organization.	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by the DoD Risk Management Framework (DoDI 8510.01).	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by DoD Risk Management Framework (DoDI 8510.01).	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-9(c)	CCI-002994	The organization reviews and updates the risk management strategy in accordance with organization-defined frequency or as required, to address organizational changes.	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by the DoD Risk Management Framework (DoDI 8510.01).	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by DoD Risk Management Framework (DoDI 8510.01).	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-9(c)	CCI-002995	The organization defines the frequency to review and update the risk management strategy to address organizational changes.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(a)	CCI-003017	The organization defines the personnel or roles to whom a personnel security policy is disseminated.	DoD has defined the roles as organizational personnel with access control responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with access control responsibilities.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-1(a)	CCI-003018	The organization defines the personnel or roles to whom the personnel security procedures are disseminated.	DoD has defined the roles as organizational personnel with access control responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with access control responsibilities.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-1(a)(1)	CCI-001504	The organization develops and documents a personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(a)(1)	CCI-001505	The organization disseminates a personnel security policy to organization-defined personnel or roles.	DoD disseminates DoD 5200.2-R via the DoD Issuance site: http://www.dtic.mil/whs/directives/corres/pub1.html to meet the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(a)(2)	CCI-001509	The organization develops and documents procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(a)(2)	CCI-001510	The organization disseminates personnel security procedures to organization-defined personnel or roles.	DoD disseminates DoD 5200.2-R via the DoD Issuance site: http://www.dtic.mil/whs/directives/corres/pub1.html to meet the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PS-1(b)(1)	CCI-001506	The organization reviews and updates the current personnel security policy in accordance with organization-defined frequency.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(b)(1)	CCI-001507	The organization defines the frequency to review and update the current personnel security policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(b)(2)	CCI-001508	The organization defines the frequency to review and update the current personnel security procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(b)(2)	CCI-001511	The organization reviews and updates the current personnel security procedures in accordance with organization-defined frequency.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-2(a)	CCI-001512	The organization assigns a risk designation to all organizational positions.	The organization being inspected/assessed will designate and document all organizational positions, to include government and contract positions, with the appropriate ADP/IT level designation, IAW DoD 5200.2-R.	The organization conducting the inspection/assessment obtains and examines documentation of the ADP/IT level designations.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-2(b)	CCI-001513	The organization establishes screening criteria for individuals filling organizational positions.	DoD 5200.2-R meets the DoD requirements for establishing screening criteria for individuals filling organizational positions. DoD organizations are automatically compliant with this CCI as they are covered at the DoD level by DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for establishing screening criteria for individuals filling organizational positions. DoD organizations are automatically compliant with this CCI as they are covered at the DoD level by DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-2(c)	CCI-001514	The organization reviews and updates position risk designations in accordance with organization-defined frequency.	The organization being inspected/assessed reviews position risk designations annually and revises designations as required based on the reviews. Records of these reviews must be maintained as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment reviews the audit records of the position designation reviews to ensure reviews are done annually. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-2(c)	CCI-001515	The organization defines the frequency to review and update position risk designations.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-3(a)	CCI-001516	The organization screens individuals prior to authorizing access to the information system.	The organization being inspected/assessed will screen all government and contract personnel to ensure they meet the appropriate ADP/IT level designation requirements IAW DoD 5200.2-R prior to authorizing access to the information system.	The organization conducting the inspection/assessment obtains and examines the information system access list (AC-2) and compares a sampling of authorized users to manning documents (PS-2) to ensure access was granted appropriately IAW ADP/IT level designation requirements within DoD 5200.2-R.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-3(b)	CCI-001517	The organization rescreens individuals with authorized access to the information system according to organization-defined conditions requiring rescreening, and where rescreening is so indicated, the organization-defined frequency of such rescreening.	The information system owner will rescreen individuals according to system owner defined list of conditions requiring rescreening (CCI-001518) individuals for access to the information system and frequency (CCI - 001519) of such rescreening. Rescreening actions will be maintained as an audit trail (AU-2).	The organization conducting the inspection/assessment obtains and examines audit records of rescreening actions to ensure the system owner is rescreening individuals according to a system owner-defined list of conditions requiring rescreening and, where re-screening is so indicated, based on the system owner-defined frequency of such rescreening.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-3(b)	CCI-001518	The organization defines the conditions requiring rescreening of individuals with authorized access to the information system.	The information system owner will develop and document the list of conditions requiring rescreening individuals for access to the information system. DoD has determined the list of conditions is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documentation of conditions requiring rescreening of individuals for access to the information system. DoD has determined the list of conditions is not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-3(b)	CCI-001519	The organization defines the frequency for rescreening individuals with authorized access to the information system when organization defined conditions requiring rescreening are met.	The information system owner will define and document the required frequency of rescreening for access to the information system. DoD has determined the frequency is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documentation defining the required frequency for rescreening individuals for access to the system. DoD has determined the frequency is not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PS-4(a)	CCI-001522	The organization, upon termination of individual employment, disables information system access within organization-defined time period.	The organization being inspected/assessed upon termination of individual employment, terminates information system access immediately and IAW organization security policy and procedures. The organization must retain an audit trail of account termination actions (AU-2). DoD has defined the time period as immediately.	The organization conducting the inspection/assessment obtains and examines organizational security policy and procedures documentation and audit records of account termination actions to ensure account termination actions are conducted immediately and IAW organizational security policy and procedures. DoD has defined the time period as immediately.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(a)	CCI-003022	The organization defines the time period to disable information system access upon termination of individual employment.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-4(b)	CCI-003023	The organization, upon termination of individual employment, terminates/revokes any authenticators/credentials associated with the individual.	The organization being inspected/assessed documents and implements a process to terminate/revoke any authenticators/credentials associated with the individual upon termination of individual employment. The organization must maintain records of termination/revocation of any authenticators/credentials.	The organization conducting the inspection/assessment obtains and examines the documented process as well as a sampling of records of termination/revocation of any authenticators/credentials to ensure the organization being inspected/assessed terminates/revokes any authenticators/credentials associated with the individual upon termination of individual employment.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(c)	CCI-001523	The organization, upon termination of individual employment, conducts exit interviews that include a discussion of organization-defined information security topics.	The organization being inspected/assessed, conducts exit interviews that include a discussion of information security topics defined in PS-4, CCI 3024 upon termination of individual employment IAW organization security policy and procedures. The organization must retain an audit trail of conducted exit interviews (AU-2)	The organization conducting the inspection/assessment obtains and examines documentation of departed personnel and the audit trail of conducted exit interviews to ensure all departed personnel had exit interviews conducted that include a discussion of information security topics defined in PS-4, CCI 3024.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(c)	CCI-003024	The organization defines information security topics to be discussed while conducting exit interviews.	The organization being inspected/assessed defines and documents information security topics to be discussed while conducting exit interviews. DoD has determined the information security topics are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information security topics to ensure the organization being inspected/assessed defines information security topics to be discussed while conducting exit interviews. DoD has determined the information security topics are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(d)	CCI-001524	The organization, upon termination of individual employment, retrieves all security-related organizational information systems-related property.	The organization being inspected/assessed upon termination of individual employment retrieves all security-related organizational information systems-related property IAW organization security policy and procedures. The organization must retain an audit trail of all retrieved security-related organizational information systems-related property (AU-2).	The organization conducting the inspection/assessment obtains and examines appropriate organization security-related organizational information systems-related property documentation/logs and compares to audit trail of all retrieved security-related organizational information systems-related property (AU-2) to ensure all property has been retrieved.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(e)	CCI-001525	The organization, upon termination of individual employment, retains access to organizational information formerly controlled by terminated individual.	The organization being inspected/assessed upon termination of individual employment retains access to organizational information formerly controlled by terminated individual IAW organization security policy and procedures. Organizational information formerly controlled by terminated individuals generally refers to online work-product including email files.	The organization conducting the inspection/assessment interviews appropriate IT and security personnel to validate the organization has procedures in place which, upon termination of individual's employment, will ensure it retains access to organizational information formerly controlled by the terminated individual.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(e)	CCI-001526	The organization, upon termination of individual employment, retains access to organizational information systems formerly controlled by terminated individual.	The organization being inspected/assessed upon termination of individual employment retains access to organizational information systems formerly controlled by terminated individual IAW organization security policy and procedures. Organizational information systems formerly controlled by terminated individuals generally refers to issued hardware (e.g. laptops, BlackBerrys, PEDs, removable media, etc.)	The organization conducting the inspection/assessment interviews appropriate IT and security personnel to validate the organization has procedures in place which, upon termination of individual's employment, will ensure it retains access to organizational information systems formerly controlled by the terminated individual.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(f)	CCI-003016	The organization, upon termination of individual employment, notifies organization-defined personnel or roles within an organization-defined time period.	The organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for revoking credentials immediately or within 24 hours upon termination of individual employment. The organization must maintain records of termination notification. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials. DoD has defined the time period as immediately or within 24 hours.	The organization conducting the inspection/assessment obtains and examines records of termination notification to ensure the organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for revoking credentials immediately or within 24 hours upon termination of individual employment. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials. DoD has defined the time period as immediately or within 24 hours.	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PS-4(f)	CCI-003025	The organization defines personnel or roles to notify upon termination of individual employment.	DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials.	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(f)	CCI-003026	The organization defines the time period in which to notify organization-defined personnel or roles upon termination of individual employment.	DoD has defined the time period as immediately or within 24 hours.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately or within 24 hours.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-5(a)	CCI-001527	The organization reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization.	The organization being inspected/assessed reviews and confirms ongoing operational need for logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization. The organization must maintain an audit trail of reviews.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure that the organization has confirmed the ongoing operational need for logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-5(b)	CCI-001528	The organization initiates organization-defined transfer or reassignment actions within an organization-defined time period following the formal personnel transfer action.	The organization being inspected/assessed initiates transfer or reassignment actions to ensure all system accesses no longer required are removed and actions to ensure all system accesses required due to the individual's new position are granted immediately when personnel are reassigned or transferred to other positions. DoD defines transfer or reassignment actions as actions to ensure all system accesses no longer required are removed. DoD defines the time period as immediately.	The organization conducting the inspection/assessment obtains and examines appropriate organization security-related organizational physical and logical access documentation/logs and compares to transferred personnel documentation to ensure appropriate logical and physical access have been revoked for previous positions and granted for new positions immediately. DoD defines the time period as immediately.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-5(b)	CCI-001529	The organization defines transfer or reassignment actions to initiate within an organization-defined time period following the formal personnel transfer action.	DoD defines transfer or reassignment actions as actions to ensure all system accesses no longer required are removed.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD defines transfer or reassignment actions as actions to ensure all system accesses no longer required are removed.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-5(b)	CCI-001530	The organization defines the time period within which the organization initiates organization-defined transfer or reassignment actions, following the formal personnel transfer action.	DoD defines the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD defines the time period as immediately.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-5(c)	CCI-003031	The organization modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.	The organization being inspected/assessed documents and implements a process to modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.	The organization conducting the inspection/assessment obtains and examines the documented process and a sampling of accounts of users recently transferred or reassigned to ensure the organization being inspected/assessed modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-5(d)	CCI-003032	The organization notifies organization-defined personnel or roles within an organization-defined time period when individuals are transferred or reassigned to other positions within the organization.	The organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for transferring credentials within 24 hours when individuals are transferred or reassigned to other positions within the organization. The organization must maintain records of transfer/reassignment notifications. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. DoD has defined the time period as within 24 hours.	The organization conducting the inspection/assessment obtains and examines records of transfer/reassignment notifications to ensure the organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for transferring credentials within 24 hours when individuals are transferred or reassigned to other positions within the organization. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. DoD has defined the time period as within 24 hours.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-5(d)	CCI-003033	The organization defines personnel or roles to be notified when individuals are transferred or reassigned to other positions within the organization.	DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-5(d)	CCI-003034	The organization defines the time period within which organization-defined personnel or roles are to be notified when individuals are transferred or reassigned to other positions within the organization.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PS-6(a)	CCI-003035	The organization develops and documents access agreements for organizational information systems.	The organization being inspected/assessed develops and documents access agreements for organizational information systems.	The organization conducting the inspection/assessment obtains and examines the documented access agreements to ensure the organization being inspected/assessed develops and documents access agreements for organizational information systems.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PS-6(b)	CCI-001532	The organization reviews and updates the access agreements in accordance with organization-defined frequency.	The organization being inspected/assessed reviews/updates the access agreements annually of employees who have signed access agreements. The purpose of this review/update is to ensure access agreements are current and departed employees no longer have access agreements. The organization must maintain an audit trail of the review and update activity for review.	The organization conducting the inspection/assessment obtains and examines the audit trail to ensure review/update occurred annually and departed employees no longer have valid access agreements.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-6(b)	CCI-001533	The organization defines the frequency to review and update the access agreements.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-6(c)(1)	CCI-001531	The organization ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access.	The organization being inspected/assessed will ensure all individuals have appropriate access agreements in place prior to being granted access to information and information systems. DD Form 2875 is the accepted DoD methodology of requesting and granting of access to information and information systems.	The organization conducting the inspection/assessment obtains a list of organizational individuals with active accounts and validates the existence of signed DD Form 2875 (paper or electronic) associated with a sampling of individuals selected from the list.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-6(c)(2)	CCI-003036	The organization ensures that individuals requiring access to organizational information and information systems re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or in accordance with organization-defined frequency.	The organization being inspected/assessed requires that individuals re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or when there is a change to the user's level of access. DoD has defined the frequency as when there is a change to the user's level of access.	The organization conducting the inspection/assessment obtains and examines a sampling of re-signed access agreements to ensure the organization being inspected/assessed requires that individuals re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or when there is a change to the user's level of access. DoD has defined the frequency as when there is a change to the user's level of access.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-6(c)(2)	CCI-003037	The organization defines the frequency for individuals requiring access to organization information and information systems to re-sign access agreements.	DoD has defined the frequency as when there is a change to the user's level of access.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as when there is a change to the user's level of access.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-7(a)	CCI-001539	The organization establishes personnel security requirements including security roles and responsibilities for third-party providers.	DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41 meet the DoD personnel security requirements including security roles and responsibilities for third-party providers. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41.	DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41 meet the DoD personnel security requirements including security roles and responsibilities for third-party providers. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-7(b)	CCI-003040	The organization requires third-party providers to comply with personnel security policies and procedures established by the organization.	The organization being inspected/assessed documents and implements a process to require third-party providers to comply with personnel security policies and procedures established by the organization.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires third-party providers to comply with personnel security policies and procedures established by the	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-7(c)	CCI-001540	The organization documents personnel security requirements for third-party providers.	The organization being inspected/assessed documents personnel security requirements for third-party providers.	The organization conducting the inspection/assessment obtains and examines the personnel security requirements to ensure the organization being inspected/assessed documents personnel security requirements for third-party providers.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-7(d)	CCI-003041	The organization requires third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within an organization-defined time period.	The organization being inspected/assessed documents and implements a process to require third-party providers to notify at a minimum, the ISSO and personnel responsible for transferring credentials of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges immediately. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. DoD has defined the time period as immediately.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires third-party providers to notify at a minimum, the ISSO and personnel responsible for transferring credentials of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges immediately. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. DoD has defined the time period as immediately.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-7(d)	CCI-003042	The organization defines personnel or roles whom third-party providers are to notify when third-party personnel who possess organizational credentials and /or badges or who have information system privileges are transferred or terminated.	DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PS-7(d)	CCI-003043	The organization defines the time period for third-party providers to notify organization-defined personnel or roles when third-party personnel who possess organizational credentials and /or badges or who have information system privileges are transferred or terminated.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-7(e)	CCI-001541	The organization monitors third-party provider compliance with personnel security requirements.	The organization being inspected/assessed monitors third-party provider compliance with personnel security requirements. The organization must maintain an audit trail of monitoring activity.	The organization conducting the inspection/assessment obtains and examines the audit trail of monitoring activity to ensure the organization being inspected/assessed monitors third-party provider compliance with personnel security requirements.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-8(a)	CCI-001542	The organization employs a formal sanctions process for individuals failing to comply with established information security policies and procedures.	The organization being inspected/assessed will develop formal procedures within the organizational security policy to employ formal sanctions for personnel failing to comply with established information security policies and procedures.	The organization conducting the inspection/assessment obtains and examines the organizational security policy to ensure it addresses formal procedures for sanctions and interviews security personnel to validate the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-8(b)	CCI-003044	The organization notifies organization-defined personnel or roles within an organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	The organization being inspected/assessed notifies at a minimum, the ISSO immediately when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. The organization must maintain records of notifications of employee sanctions. DoD has defined the personnel or roles as at a minimum, the ISSO. DoD has defined the time period as immediately.	The organization conducting the inspection/assessment obtains and examines the records of notifications of employee sanctions to ensure the organization being inspected/assessed notifies at a minimum, the ISSO immediately when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. DoD has defined the personnel or roles as at a minimum, the ISSO. DoD has defined the time period as immediately.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-8(b)	CCI-003045	The organization defines personnel or roles whom are to be notified when a formal employee sanctions process is initiated.	DoD has defined the personnel or roles as at a minimum, the ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-8(b)	CCI-003046	The organization defines the time period to notify organization-defined personnel or roles when a formal employee sanctions process is initiated.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(a)	CCI-002368	The organization defines the personnel or roles to whom the risk assessment policy is disseminated.	DoD has defined the roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(a)	CCI-002369	The organization defines the personnel or roles to whom the risk assessment procedures are disseminated.	DoD has defined the roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(a)(1)	CCI-001037	The organization develops and documents a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(a)(1)	CCI-001038	The organization disseminates a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to organization-defined personnel or roles.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures and is disseminated via the NIST publications site: http://csrc.nist.gov/publications/PubsSPs.html DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(a)(2)	CCI-001041	The organization develops and documents procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	RA-1(a)(2)	CCI-001042	The organization disseminates risk assessment procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls to organization-defined personnel or roles.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures and is disseminated via the NIST publications site: http://csrc.nist.gov/publications/PubsSPs.html DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(b)(1)	CCI-001039	The organization reviews and updates the current risk assessment policy in accordance with organization-defined frequency.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(b)(1)	CCI-001040	The organization defines the frequency to review and update the current risk assessment policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(b)(2)	CCI-001043	The organization reviews and updates the current risk assessment procedures in accordance with organization-defined frequency.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(b)(2)	CCI-001044	The organization defines the frequency to review and update the current risk assessment procedures.	DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy. DoD has defined the frequency as annually - updated as appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-2(a)	CCI-001045	The organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The organization being inspected/assessed documents and implements a process to categorize information and the information system in accordance with CNSSI 1253 and applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed categorizes information and the information system in accordance with CNSSI 1253 and applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-2(b)	CCI-001046	The organization documents the security categorization results (including supporting rationale) in the security plan for the information system.	The organization being inspected/assessed documents the security categorization results (including supporting rationale) in the security plan for the information system IAW CNSSI 1253.	The organization conducting the inspection/assessment obtains and examines the documented security categorization results to ensure the organization being inspected/assessed documents the security categorization results (including supporting rationale) in the security plan for the information system IAW CNSSI 1253.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-2(c)	CCI-001047	The organization ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	The organization being inspected/assessed documents and implements a process IAW CNSSI 1253 to ensure the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-3(a)	CCI-001048	The organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction.	The organization being inspected/assessed conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction. The organization must maintain an audit trail of assessments.	The organization conducting the inspection/assessment obtains and examines the audit trail of assessments to ensure the organization being inspected/assessed conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction.	LOW		X	X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-3(b)	CCI-001049	The organization documents risk assessment results in the organization-defined document.	The organization being inspected/assessed documents risk assessment results in the risk assessment report. DoD has defined the document as a risk assessment report.	The organization conducting the inspection/assessment obtains and examines the risk assessment report to ensure the organization being inspected/assessed documents risk assessment results in the risk assessment report. DoD has defined the document as a risk assessment report.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-3(b)	CCI-001642	The organization defines the organizational document in which risk assessment results are documented (e.g., security plan, risk assessment report).	DoD has defined the document as a risk assessment report.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the document as a risk assessment report.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	RA-3(c)	CCI-001050	The organization reviews risk assessment results on an organization-defined frequency.	The organization being inspected/assessed reviews risk assessment results upon re-accreditation. The organization must maintain a record of reviews. DoD has defined the frequency as upon re-accreditation.	The organization conducting the inspection/assessment obtains and examines the record of reviews to ensure the organization being inspected/assessed reviews risk assessment results upon re-accreditation. DoD has defined the frequency as upon re-accreditation.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-3(c)	CCI-001051	The organization defines a frequency for reviewing risk assessment results.	DoD has defined the frequency as upon re-accreditation.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as upon re-accreditation.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-3(d)	CCI-002370	The organization disseminates risk assessment results to organization-defined personnel or roles.	The organization being inspected/assessed documents and implements a process to disseminates risk assessment results to the ISSM, ISSO, AO, and PM. DoD has defined the personnel or roles as the ISSM, ISSO, AO, and PM.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed disseminates the risk assessment results to the ISSM, ISSO, AO, and PM. DoD has defined the personnel or roles as the ISSM, ISSO, AO, and PM.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-3(d)	CCI-002371	The organization defines the personnel or roles whom the risk assessment results will be disseminated.	DoD has defined the personnel or roles as the ISSM, ISSO, AO, and PM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSM, ISSO, AO, and PM.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-3(e)	CCI-001052	The organization updates the risk assessment on an organization-defined frequency or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	The organization being inspected/asssessed updates the risk assessment upon re-accreditation or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. DoD has defined the frequency as upon re-accreditation.	The organization conducting the inspection/assessment obtains and examines historical versions of the risk assessment as well as records of changes to the system to ensure the organization being inspected/assessed updates the risk assessment upon re-accreditation or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. DoD has defined the frequency as upon re-accreditation.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-3(e)	CCI-001053	The organization defines a frequency for updating the risk assessment.	DoD has defined the frequency as upon re-accreditation.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as upon re-accreditation.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IA-6	CCI-000206	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	The organization being inspected/assessed configures the information system to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 206.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 206.	LOW	X	X		X				3.4.6 Authenticator Feedback		CCI requirements are met within subparagraph "Authenticator Feedback" of UFGS 25 05 11.
N/A	AU-12(a)	CCI-000169	The information system provides audit record generation capability for the auditable events defined in AU-2 a at organization defined information system components.	The organization being inspected/assessed acquires or designs all information system and network components that provide audit record generation capability for the auditable events defined in AU-2 a. DoD has defined the information system components as all information system and network components.	The organization conducting the inspection/assessment examines the information system to ensure that all information system and network components provide audit record generation capability for the auditable events defined in AU-2 a. DoD has defined the information system components as all information system and network components.	LOW		X						3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
RA-5	RA-5(a)	CCI-001056	The organization scans for vulnerabilities in the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported.	The organization being inspected/assessed will conduct vulnerability scans of the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported via authoritative sources (e.g., IAVM, CTO, DTM, STIG, product vendor).	The organization conducting the inspection/assessment obtains and examines the organization's vulnerability scanning procedures and results in order to validate the organization conducts vulnerability scans of its Information System (IS) and hosted applications when new vulnerabilities potentially affecting the IS and/or applications are identified and reported.	LOW	X	X	X					3.11 VULNERABILITY SCANNING	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-12(a)	CCI-001459	The organization defines information system components that provide audit record generation capability.	DoD has defined the information system components as all information system and network components.	DoD has defined the information system components as all information system and network components.	LOW		X		X	X			3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-12(b)	CCI-000171	The information system allows organization-defined personnel or roles to select which auditable events are to be audited by specific components of the information system.	The organization being inspected/assessed configures the information system to ensure that only the ISSM or individuals appointed by the ISSM select which auditable events are to be audited by specific components of the information system. DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	The organization conducting the inspection/assessment examines a sampling of information system components and confirms that the individuals capable of selecting auditable events are the ISSM or individuals appointed by the ISSM. DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	LOW		X		X				3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-12(b)	CCI-001910	The organization defines the personnel or roles allowed select which auditable events are to be audited by specific components of the information system.	DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	LOW		X		X	X			3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-12(c)	CCI-000172	The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.	The organization being inspected/assessed configures the information system to generate audit records for the events defined in AU-2 d with the content defined in AU-3. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 172.	The organization conducting the inspection/assessment examines the information system to ensure that the system generates audit records for the events defined in AU-2 d with the content defined in AU-3. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 172.	LOW		X						3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-2(a)	CCI-000123	The organization determines the information system must be capable of auditing an organization-defined list of auditable events.	The organization being inspected/assessed determines whether the information system is capable of auditing: - successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. Classification levels), - Successful and unsuccessful logon attempts, - Privileged activities or other system level access, - Starting and ending time for user access to the system, - Concurrent logons from different workstations, - Successful and unsuccessful accesses to objects, - All program initiations, - All direct access to the information system, - All account creations, modifications, disabling, and terminations, - All kernel module load, unload, and restart. The organization must document those auditable events that are not captured. DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g.	The organization conducting the inspection/assessment obtains and examines the documentation of the auditable events to ensure the information system is capable of auditing the: - successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. Classification levels), - Successful and unsuccessful logon attempts, - Privileged activities or other system level access, - Starting and ending time for user access to the system, - Concurrent logons from different workstations, - Successful and unsuccessful accesses to objects, - All program initiations, - All direct access to the information system, - All account creations, modifications, disabling, and terminations, - All kernel module load, unload, and restart. DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information	LOW		X	X					3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	RA-5(d)	CCI-001060	The organization defines response times for remediating legitimate vulnerabilities in accordance with an organization assessment of risk.	DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs).	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	RA-5(e)	CCI-001061	The organization shares information obtained from the vulnerability scanning process and security control assessments with organization-defined personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	The organization being inspected/assessed documents and implements a process to share information obtained from the vulnerability scanning process and security control assessments with at a minimum, the ISSM and ISSO to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed shares information obtained from the vulnerability scanning process and security control assessments with at a minimum, the ISSM and ISSO to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-5(e)	CCI-002376	The organization defines the personnel or roles whom the information obtained from the vulnerability scanning process and security control assessments will be shared.	DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(a)	CCI-003089	The organization defines the personnel or roles to whom the system and services acquisition policy is disseminated.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-1(a)	CCI-003090	The organization defines the personnel or roles to whom procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls are disseminated.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.	LOW			X	X	X			---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-1(a)(1)	CCI-000602	The organization develops and documents a system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(a)(1)	CCI-000603	The organization disseminates to organization-defined personnel or roles a system and services acquisition policy.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(a)(2)	CCI-000605	The organization develops and documents procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(a)(2)	CCI-000606	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(b)(1)	CCI-000601	The organization defines the frequency to review and update the current system and services acquisition policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(b)(1)	CCI-000604	The organization reviews and updates the current system and services acquisition policy in accordance with organization-defined frequency.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(b)(2)	CCI-000607	The organization reviews and updates the current system and services acquisition procedures in accordance with organization-defined frequency.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(b)(2)	CCI-001646	The organization defines the frequency to review and update the current system and services acquisition procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-2(a)	CCI-003091	The organization determines information security requirements for the information system or information system service in mission/business process planning.	The organization being inspected/assessed determines and documents information security requirements for the information system or information system service in mission/business process planning.	The organization conducting the inspection/assessment obtains and examines the documented information security requirements to ensure the organization being inspected/assessed determines information security requirements for the information system or information system service in mission/business process planning.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-2(b)	CCI-000610	The organization determines the resources required to protect the information system or information system service as part of its capital planning and investment control process.	The organization being inspected/assessed determines the resources (funding, staffing, etc.) required for the cybersecurity requirements to protect the information system or information system service as part of its planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has determined the resources required for cybersecurity requirements to protect the information system or information system service.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-2(b)	CCI-000611	The organization documents the resources required to protect the information system or information system service as part of its capital planning and investment control process.	The organization being inspected/assessed documents the resources (funding, staffing, etc.) required for the cybersecurity requirements to protect the information system or information system service as part of its planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has documented the resources required for cybersecurity requirements to protect the information system or information system service.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-2(b)	CCI-000612	The organization allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process.	The organization being inspected/assessed allocates the resources (funding, staffing, etc.) required for the cybersecurity requirements to protect the information system or information system service as part of its planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has allocated the resources required for cybersecurity requirements to protect the information system or information system service.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-2(c)	CCI-000613	The organization establishes a discrete line item for information security in organizational programming documentation.	The organization being inspected/assessed identifies and establishes an individual line item for cybersecurity requirements to protect the information system as part of the planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has identified and established an individual line item for cybersecurity requirements to protect the information system.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-2(c)	CCI-000614	The organization establishes a discrete line item for information security in organizational budgeting documentation.	The organization being inspected/assessed identifies and establishes an individual line item for cybersecurity requirements to protect the information system as part of the planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has identified and established an individual line item for cybersecurity requirements to protect the information system.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-3(a)	CCI-000615	The organization manages the information system using organization-defined system development life cycle that incorporates information security considerations.	The organization being inspected/assessed documents and implements a process to manage the information system using the system development life cycle defined in SA-3, CCI 3092 that incorporates information security considerations IAW DoDI 8580.1.	The organization conducting the inspection/assessment obtains and examines the documented process and artifacts of the system development life cycle process to ensure the organization being inspected/assessed manages the information system using the system development life cycle defined in SA-3, CCI 3092 that incorporates information security considerations IAW DoDI 8580.1.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-3(a)	CCI-003092	The organization defines a system development life cycle that is used to manage the information system.	The organization being inspected/assessed defines and documents a system development life cycle that is used to manage the information system. DoD has determined the system development life cycle is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented system development life cycle to ensure the organization being inspected/assessed defines a system development life cycle that is used to manage the information system. DoD has determined the system development life cycle is not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-3(b)	CCI-000616	The organization defines and documents information system security roles and responsibilities throughout the system development life cycle.	The organization being inspected/assessed defines and documents information system security roles and responsibilities throughout the system development life cycle IAW DoDI 8580.1 .	The organization conducting the inspection/assessment obtains and examines the information system security roles and responsibilities to ensure the organization being inspected/assessed defines and documents information system security roles and responsibilities throughout the system development life cycle IAW DoDI 8580.1.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-3(c)	CCI-000618	The organization identifies individuals having information system security roles and responsibilities.	The organization being inspected/assessed identifies and documents individuals having information system security roles and responsibilities.	The organization conducting the inspection/assessment obtains and examines the documented individuals having information system security roles and responsibilities to ensure the organization being inspected/assessed identifies individuals having information system security roles and responsibilities.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-3(d)	CCI-003093	The organization integrates the organizational information security risk management process into system development life cycle activities.	The organization being inspected/assessed documents and implements a process to integrate the organizational information security risk management process into system development life cycle activities.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed integrates the organizational information security risk management process into system development life cycle	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-2(a)	CCI-001571	The organization defines the information system auditable events.	DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module load, unload, and restart.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module load, unload, and restart.	LOW		X		X	X			3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	SA-4(a)	CCI-003094	The organization includes the security functional requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, the security functional requirements, explicitly or by reference, IAW DoDI 8580.1.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes the security functional requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs including DoDI 8580.1.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-4(b)	CCI-003095	The organization includes the security strength requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, the security strength requirements, explicitly or by reference, IAW DoDI 8580.1.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes the security strength requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs including DoDI 8580.1.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(c)	CCI-003096	The organization includes the security assurance requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, the security assurance requirements, explicitly or by reference, IAW DoDI 8580.1.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes the security assurance requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs including DoDI 8580.1.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(d)	CCI-003097	The organization includes the security-related documentation requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, the security-related documentation requirements, explicitly or by reference.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes the security-related documentation requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(e)	CCI-003098	The organization includes requirements for protecting security-related documentation, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, requirements for protecting security-related documentation, explicitly or by reference.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes requirements for protecting security-related documentation, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(f)	CCI-003099	The organization includes description of the information system development environment and environment in which the system is intended to operate, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, a description of the information system development environment and environment in which the system is intended to operate, explicitly or by reference.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes a description of the information system development environment and environment in which the system is intended to operate, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(g)	CCI-003100	The organization includes acceptance criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, acceptance criteria, explicitly or by reference.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes acceptance criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	LOW			X	X				---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-2(c)	CCI-000125	The organization provides a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents.	The organization being inspected/assessed documents in the audit and accountability policy the list of auditable system events, the organization provides clearly stated rationale for the selection of each system event. The rationale will support any after-action investigations of security event.	The organization conducting the inspection/assessment obtains and examines the audit and accountability policy and procedures to ensure the organization being inspected/assess has defined the auditable system events, rationale for the selection, and that the organization has defined how the auditable events will support after-action investigations of security events.	LOW		X	X					3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-2(d)	CCI-001485	The organization defines the events which are to be audited on the information system on an organization defined frequency of (or situation requiring) auditing for each identified event.	The organization being inspected/assessed defines and documents events which are to be audited on the information system. Events should be selected from the events the information system is capable of auditing as defined in AU-2 (a) and should be based on ongoing risk assessments of current threat information and environment. DoD has determined that the events are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented list of events which are to be audited on the information system to ensure those events have been defined. DoD has determined that the events are not appropriate to define at the Enterprise level.	LOW		X	X					3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-3	CCI-000130	The information system generates audit records containing information that establishes what type of event occurred.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes what type of event occurred For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 130.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes what type of event occurred. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes what type of event occurred. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 130.	LOW		X						3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-3	CCI-000131	The information system generates audit records containing information that establishes when an event occurred.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes when an event occurred For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 131.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes when an event occurred. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes when an event occurred. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 131.	LOW		X						3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-3	CCI-000132	The information system generates audit records containing information that establishes where the event occurred.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes where the event occurred For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 132.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes where the event occurred. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes where the event occurred. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 132.	LOW		X						3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-3	CCI-000133	The information system generates audit records containing information that establishes the source of the event.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes the source of the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 133.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes the source of the event. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes the source of the event. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 133.	LOW		X						3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-3	CCI-000134	The information system generates audit records containing information that establishes the outcome of the event.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes the outcome of the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 134.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes the outcome of the event. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes the outcome of the event. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 134.	LOW		X						3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-3	CCI-001487	The information system generates audit records containing information that establishes the identity of any individuals or subjects associated with the event.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes the identity of any individuals or subjects associated with the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1487.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes the identity of any individuals or subjects associated with the event. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes the identity of any individuals or subjects associated with the event. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1487.	LOW		X		X				3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	SA-5(c)	CCI-000642	The organization documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.	The organization being inspected/assessed documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.	The organization conducting the inspection/assessment obtains and examines the documented attempts to ensure the organization being inspected/assessed documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-5(c)	CCI-003132	The organization takes organization-defined actions in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service.	The organization being inspected/assessed takes actions defined in SA-5, CCI 3133 in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service. The organization must maintain a record of actions taken. DoD has determined the actions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the record of actions taken to ensure the organization being inspected/assessed takes actions defined in SA-5, CCI 3133 in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service. DoD has determined the actions are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-5(c)	CCI-003133	The organization defines actions to be taken in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service.	The organization being inspected/assessed defines and documents actions to be taken in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service. DoD has determined the actions are not appropriate to define at the Enterprise level.	The organization conducting inspection/assessment obtains and examines the documented actions to ensure the organization being inspected/assessed defines action to be taken in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service. DoD has determined the actions are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-5(d)	CCI-003134	The organization protects information system, system component, or information system service documentation as required, in accordance with the risk management strategy.	The organization being inspected/assessed documents and implements processes to store and handle information system, system component, or information system service documentation as required, in accordance with the risk management strategy.	The organization conducting the inspection/assessment obtains and examines the documented processes to ensure the organization being inspected/assessed stores and handles information system, system component, or information system service documentation as required, in accordance with the risk management strategy.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-5(e)	CCI-003135	The organization distributes information system, system component, or information system service documentation to organization defined personnel or roles.	The organization being inspected/assessed distributes information system, system component, or information system service documentation to at a minimum, the ISSO, ISSM, and SCA, via an information sharing capability. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA.	The organization conducting the inspection/assessment obtains and examines the information system, system component, or information system service documentation via the organization's information sharing capability to ensure the organization being inspected/assessed distributes information system, system component, or information system service documentation to at a minimum, the ISSO, ISSM, and SCA. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-5(e)	CCI-003136	The organization defines the personnel or roles the information system, system component, or information system service documentation is to be distributed.	DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-9(a)	CCI-000669	The organization requires that providers of external information system services comply with organizational information security requirements.	The organization being inspected/assessed documents within contracts/agreements, requirements that providers of external information system services comply with any organization-specific information security requirements.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that providers of external information system services comply with any organization-specific information security requirements.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-9(a)	CCI-000670	The organization requires that providers of external information system services employ organization-defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The organization being inspected/assessed documents within contracts/agreements, the requirement that providers of external information system services employ security controls defined in CNSSI 1253. DoD has defined the security controls as security controls defined by CNSSI 1253.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that providers of external information system services employ security controls defined in CNSSI 1253. DoD has defined the security controls as security controls defined by CNSSI 1253.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-9(a)	CCI-003137	The organization defines security controls that providers of external information system services employ in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	DoD has defined the security controls as security controls defined by CNSSI 1253.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security controls as security controls defined by CNSSI 1253.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-9(b)	CCI-000671	The organization defines government oversight with regard to external information system services.	The organization being inspected/assessed must define in the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) the government oversight to be conducted on external information system services and service provider.	The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly defined the government oversight to be conducted on external information system services and service providers.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-9(b)	CCI-000672	The organization documents government oversight with regard to external information system services.	The organization being inspected/assessed must establish in the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) the government oversight to be conducted on external information system services and service provider.	The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly established the government oversight to be conducted on external information system services and service providers.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-9(b)	CCI-000673	The organization defines user roles and responsibilities with regard to external information system services.	The organization being inspected/assessed must define in the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) the roles and responsibilities of all types of users of the external information system services.	The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly defined the roles and responsibilities of all types of users of the external information system services.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-9(b)	CCI-000674	The organization documents user roles and responsibilities with regard to external information system services.	The organization being inspected/assessed must establish in the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) the roles and responsibilities of all types of users of the external information system services.	The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly established the roles and responsibilities of all types of users of the external information system services.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-9(c)	CCI-003138	The organization employs organization defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.	The organization being inspected/assessed implements the processes, methods, and techniques defined in SA-9, CCI 3139 to monitor security control compliance by external service providers on an ongoing basis. The organization must maintain records of monitoring.	The organization conducting the inspection/assessment obtains and examines the records of monitoring to ensure the organization being inspected/assessed implements the processes, methods, and techniques defined in SA-9, CCI 3139 to monitor security control compliance by external service providers on an ongoing basis.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-9(c)	CCI-003139	The organization defines processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis.	The organization being inspected/assessed defines and documents processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis. DoD has determined the processes, methods, and techniques are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented processes, methods, and techniques to ensure the organization being inspected/assessed defines processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-1(a)	CCI-002378	The organization defines the personnel or roles to be recipients of the system and communications protection policy.	The organization being inspected/assessed defines and documents personnel or roles to be recipients of the system and communications protection policy. The personnel or roles must include at a minimum, the ISSM/ISSO. DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles to be recipients of the system and communications protection policy. The personnel or roles must include at a minimum, the ISSM/ISSO. DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-1(a)	CCI-002380	The organization defines the personnel or roles to be recipients of the procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	The organization being inspected/assessed defines and documents personnel or roles to be recipients of the procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. The personnel or roles must include at a minimum, the ISSM/ISSO. DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles to be recipients of the procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. The personnel or roles must include at a minimum, the ISSM/ISSO. DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-1(a)(1)	CCI-001074	The organization develops and documents a system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for developing a system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for developing a system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(a)(1)	CCI-001075	The organization disseminates to organization-defined personnel or roles the system and communications protection policy.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(a)(2)	CCI-001078	The organization develops and documents system and communications protection procedures to facilitate the implementation of the system and communications protection policy and communications protection controls and associated system and communications protection controls.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for developing system and communications protection procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for developing system and communications protection procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(a)(2)	CCI-001079	The organization disseminates to organization-defined personnel or roles the procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the procedures to facilitate the implementation of the system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the procedures to facilitate the implementation of the system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(b)(1)	CCI-001076	The organization reviews and updates the system and communications protection policy in accordance with organization-defined frequency.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(b)(1)	CCI-001077	The organization defines the frequency for reviewing and updating the system and communications protection policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(b)(2)	CCI-001080	The organization reviews and updates the system and communications protection procedures in accordance with organization-defined frequency.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(b)(2)	CCI-001081	The organization defines the frequency of system and communications protection procedure reviews and updates.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-12	CCI-002428	The organization defines the requirements for cryptographic key generation to be employed within the information system.	DoD has defined the requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW	X			X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-12	CCI-002429	The organization defines the requirements for cryptographic key distribution to be employed within the information system.	DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW	X			X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-2(d)	CCI-001230	The organization incorporates flaw remediation into the organizational configuration management process.	The organization being inspected/assessed documents within their configuration management plan, flaw remediation processes.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure that it incorporates flaw remediation.	LOW			X					---		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	SC-12	CCI-002431	The organization defines the requirements for cryptographic key access to be employed within the information system.	DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW	X			X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-12	CCI-002432	The organization defines the requirements for cryptographic key destruction to be employed within the information system.	DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW	X			X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-12	CCI-002433	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key generation.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002434	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key distribution.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002435	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key storage.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-12	CCI-002436	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key access.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002437	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key destruction.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002438	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key generation.	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key generation as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key generation as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002439	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key distribution.	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002440	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key storage.	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-12	CCI-002441	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key access.	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002442	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key destruction.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-8(a)	CCI-000159	The information system uses internal system clocks to generate time stamps for audit records.	The organization being inspected/assessed configures the information system to use internal system clocks to generate time stamps for audit records. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 159.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to use internal system clocks to generate time stamps for audit records. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 159.	LOW		X						3.5.2 Audit Time Stamps		CCI requirements are met within subparagraph "Audit Time Stamps" of UFGS 25 05 11.
N/A	AU-8(b)	CCI-001889	The information system records time stamps for audit records that meets organization-defined granularity of time measurement.	The organization being inspected/assessed configures the information system to generate time in the time stamps for audit records that meets one second granularity of time measurement. DoD has defined the granularity of time measurement as one second. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1889.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate time in the time stamps for audit records that meets one second granularity of time measurement. DoD has defined the granularity of time measurement as one second. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1889.	LOW		X						3.5.2 Audit Time Stamps		CCI requirements are met within subparagraph "Audit Time Stamps" of UFGS 25 05 11.
N/A	AU-8(b)	CCI-001890	The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	The organization being inspected/assessed configures the information system to generate time stamps for audit records that contain time zones or time offsets that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1890.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate time stamps for audit records that contain time zones or time offsets that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1890.	LOW		X						3.5.2 Audit Time Stamps		CCI requirements are met within subparagraph "Audit Time Stamps" of UFGS 25 05 11.
N/A	SC-15(a)	CCI-001151	The organization defines exceptions to the prohibiting of collaborative computing devices where remote activation is to be allowed.	DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed.	LOW	X			X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs Incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-4	CCI-001848	The organization defines the audit record storage requirements.	The organization being inspected/assessed defines and documents the required audit record storage capacity. DoD has determined the audit record storage requirements are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented audit record storage requirements to ensure the organization being inspected/assessed has defined those requirements. DoD has determined the audit record storage requirements are not appropriate to define at the Enterprise level.	LOW		X	X					3.5.4 Audit Storage Capacity and Audit Up...		CCI requirements are met within subparagraph "Audit Storage Capacity and Audit Upload" of UFGS 25 05 11.
N/A	SC-20(a)	CCI-001178	The information system provides additional data origin authentication artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.	The organization being inspected/assessed configures the authoritative name server software for external queries to enable DNSSEC and creates resource records with digital signatures (RRSig) for each A record. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 1178.	The organization conducting the inspection/assessment: 1. inspects the configuration files for the presence of DNSSEC records for each A record hosted in a zone; 2. utilizes DNSSEC diagnostic tools, such as dig; and 3. performs queries which will exercise the data flow path for authoritative name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 1178.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS does not act as external DNS server."	
N/A	SC-20(a)	CCI-002462	The information system provides additional integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.	The organization being inspected/assessed configures the authoritative name server software for external queries to enable DNSSEC and creates resource records with digital signatures (RRSig) for each A record. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2462.	The organization conducting the inspection/assessment: 1. inspects the configuration files for the presence of DNSSEC records for each A record hosted in a zone; 2. utilizes DNSSEC diagnostic tools, such as dig; and 3. performs queries which will exercise the data flow path for authoritative name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2462.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS does not act as external DNS server."	
N/A	SC-20(b)	CCI-001179	The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child zones.	The organization being inspected/assessed configures the authoritative name server software to enable DNSSEC and creates delegation signer (DS) resource records for each child zone and place those records in the parent zone. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 1179.	The organization conducting the inspection/assessment inspect the configuration files for the presence of Delegation Signer (DS) Records for any child domains. Note: This is only applicable for zones with child domains. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 1179.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS does not act as external DNS server."	
N/A	SC-20(b)	CCI-001663	The information system, when operating as part of a distributed, hierarchical namespace, provides the means to enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services).	The organization being inspected/assessed installs and utilizes software capable of validating the chain of trust (Examples of software include dig, dnsviz, dnssec-debugger, dnssec validator for Mozilla, etc.). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1663.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for authoritative name resolution services where parent and child domains exist. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that pertains to CCI 1663.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS does not act as external DNS server."	
N/A	SC-21	CCI-002465	The information system requests data origin authentication verification on the name/address resolution responses the system receives from authoritative sources.	The organization being inspected/assessed configures the: 1. recursive/caching name server software to enable DNSSEC; 2. software to enable DNSSEC validation; and 3. software to establish a secure entry point trust anchor by installing key signing keys in the software configuration of trusted keys. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2465.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2465.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-21	CCI-002466	The information system requests data integrity verification on the name/address resolution responses the system receives from authoritative sources.	The organization being inspected/assessed configures the: 1. recursive/caching name server software to enable DNSSEC; 2. software to enable DNSSEC validation; and 3. software to establish a secure entry point trust anchor by installing key signing keys in the software configuration of trusted keys. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2466.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2466.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-21	CCI-002467	The information system performs data integrity verification on the name/address resolution responses the system receives from authoritative sources.	The organization being inspected/assessed configures the: 1. recursive/caching name server software to enable DNSSEC; 2. software to enable DNSSEC validation; and 3. software to establish a secure entry point trust anchor by installing key signing keys in the software configuration of trusted keys. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2467.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2467.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-21	CCI-002468	The information system performs data origin verification authentication on the name/address resolution responses the system receives from authoritative sources.	The organization being inspected/assessed configures the: 1. recursive/caching name server software to enable DNSSEC; 2. software to enable DNSSEC validation; and 3. software to establish a secure entry point trust anchor by installing key signing keys in the software configuration of trusted keys. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2468.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2468.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-22	CCI-001182	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant.	The organization being inspected/assessed implements a name service resolution architecture consisting of primary and secondary servers. The organization must document the architecture in the site security plan. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1182.	The organization conducting the inspection/assessment reviews the sites implementation documentation of the name resolution servers and verifies primary and alternate services are available. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1182.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS does not act as external DNS server."	
N/A	SC-22	CCI-001183	The information systems that collectively provide name/address resolution service for an organization implement internal/external role separation.	The organization being inspected/assessed implements a name service resolution architecture where recursive and authoritative server software is not installed on the same information system. The organization must document the architecture in the site security plan. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1183.	The organization conducting the inspection/assessment reviews the sites implementation documentation of the name resolution servers and verifies authoritative and recursive services are not hosted on the same information system. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1183.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS does not act as external DNS server."	
N/A	SC-39	CCI-002530	The information system maintains a separate execution domain for each executing process.	The organization being inspected/assessed configures the information system to maintain a separate execution domain for each executing process. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2530.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to maintain a separate execution domain for each executing process. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2530.	LOW		X						---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-4	CCI-001849	The organization allocates audit record storage capacity in accordance with organization-defined audit record storage requirements.	The organization being inspected/assessed allocates, and configures the information system to allocate audit record storage capacity as defined in AU-4, CCI 1848. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1849.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to allocate audit record storage capacity as defined in AU-4, CCI 1848. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1849.	LOW		X	X					3.5.4 Audit Storage Capacity and Audit Up...		CCI requirements are met within subparagraph "Audit Storage Capacity and Audit Upload" of UFGS 25 05 11.
N/A	AU-5(a)	CCI-000139	The information system alerts designated organization-defined personnel or roles in the event of an audit processing failure.	The organization being inspected/assessed configures the information system to alert at a minimum, the SCA and ISSO in the event of an audit processing failure. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 139. DoD has defined the personnel or roles as at a minimum, the SCA and ISSO.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to alert at a minimum, the SCA and ISSO in the event of an audit processing failure. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 139. DoD has defined the personnel or roles as at a minimum, the SCA and ISSO.	LOW	X	X		X				3.5.5 Response to Audit Processing Failur...	FRCS has no computers	
N/A	AU-5(b)	CCI-000140	The information system takes organization defined actions upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).	The organization being inspected/assessed configures the information system to take actions as defined in AU-5, CCI 1490 upon audit failure. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 140.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to take actions as defined in AU-5, CCI 1490 upon audit failure. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 140.	LOW	X	X		X				3.5.5 Response to Audit Processing Failur...	FRCS has no computers	
N/A	AU-5(b)	CCI-001490	The organization defines actions to be taken by the information system upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).	The organization being inspected/assessed will define and document actions to be taken by the information system upon audit failure. The organization shall consider trade-offs between the needs for system availability and audit integrity when defining the actions. Unless availability is an overriding concern, the default action should be to shut down the information system. DoD has determined that the actions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented actions to ensure the organization being inspected/assessed has defined the actions to be taken by the information system upon audit failure. DoD has determined that the actions are not appropriate to define at the Enterprise level.	LOW	X	X	X	X				3.5.5 Response to Audit Processing Failur...	FRCS has no computers	
CM-6	CM-6(a)	CCI-000363	The organization defines security configuration checklists to be used to establish and document configuration settings for the information system technology products employed.	DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.). The organization being inspected/assessed documents in the security plan, the configuration guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) which apply to their information system components.	DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.). The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed has documented the configuration guidance which apply to their information system components. The organization conducting the inspection/assessment reviews the list of documented guidance to ensure that all applicable guidance is identified given the information system components within the authorization boundary.	LOW		X						3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity requires the contractor to submit the Software and Configuration Backups and ensuring all STIGs/SRGs area applied where applicable. The contractor is responsible to for the configuration and software that are only strictly necessary for operation an maintenance of system. This design requirement is captured in Sub-Paragraph "Requirements for Lease Functionality" within Part 3.
CM-6	CM-6(a)	CCI-000364	The organization establishes configuration settings for information technology products employed within the information system using organization-defined security configuration checklists.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for establishing configuration settings. DoD Components are automatically compliant with this CCI because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for establishing configuration settings. DoD Components are automatically compliant with this CCI because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	LOW		X						3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity requires the contractor to submit the Software and Configuration Backups and ensuring all STIGs/SRGs area applied where applicable. The contractor is responsible to for the configuration and software that are only strictly necessary for operation an maintenance of system. This design requirement is captured in Sub-Paragraph "Requirements for Lease Functionality" within Part 3.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
CM-6	CM-6(a)	CCI-000365	The organization documents configuration settings for information technology products employed within the information system using organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for documenting configuration settings. DoD Components are automatically compliant with this CCI because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for documenting configuration settings. DoD Components are automatically compliant with this CCI because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	LOW		X	X	X	X			3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity design requires the contractor to configure and document that the control system follow any applicable STIG/SRG and/or only provide essential capabilities. This design requirement is captured in Sub-Paragraph "Requirements for Lease Functionality" within Part 3.
N/A	SC-7(b)	CCI-002395	The information system implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks.	The organization being inspected/assessed designs the information system to leverage subnetworks so that publicly accessible system components are physically and/or logically separated from internal organizational networks.	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component partitioning to ensure the organization being inspected/assessed implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks.	LOW						X		---	Per UFC 4-010-06 Appendix G, Table G-2; the "CS is not publically accessible."	
CM-6	CM-6(c)	CCI-001755	The organization defines the information system components for which any deviation from the established configuration settings are to be identified, documented and approved.	DoD has defined the information system components as all configurable information system components.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system components as all configurable information system components.	LOW		X	X	X	X			3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity design requires the contractor to configure and document that the control system follow any applicable STIG/SRG and/or only provide essential capabilities. This design requirement is captured in Sub-Paragraph "Requirements for Lease Functionality" within Part 3.
N/A	SI-1(a)	CCI-002601	The organization defines the personnel or roles to whom the system and information integrity policy and procedures are to be disseminated.	DoD has defined the personnel or roles as all appointed information assurance personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all appointed information assurance personnel.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-1(a)(1)	CCI-001217	The organization develops and documents a system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-1(a)(1)	CCI-001218	The organization disseminates the system and information integrity policy to organization-defined personnel or roles.	DoD disseminates DoDI 8510.01 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) that meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-1(a)(2)	CCI-001220	The organization develops and documents procedures to facilitate the implementation of the system and information integrity policy and associated system integrity controls.	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) .	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-1(a)(2)	CCI-001221	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the system and information integrity policy and associated system integrity controls.	DoD disseminates DoDI 8510.01 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) that meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-1(b)(1)	CCI-001219	The organization reviews and updates system and information integrity policy in accordance with organization-defined frequency.	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-1(b)(1)	CCI-001223	The organization defines the frequency of system and information integrity policy reviews and updates.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-1(b)(2)	CCI-001222	The organization reviews and updates system and information integrity procedures in accordance with organization-defined frequency.	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-1(b)(2)	CCI-001224	The organization defines the frequency of system and information integrity procedure reviews and updates	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-12	CCI-001315	The organization handles information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization being inspected/assessed identifies and documents federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system. The organization documents and implements a process to handle information IAW those documented federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization conducting the inspection/assessment obtains and examines the documented list of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system, as well as the documented process for information handling to ensure the organization being inspected/assessed handles information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-12	CCI-001678	The organization retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization being inspected/assessed identifies and documents federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system. The organization documents and implements a process to retain information IAW those documented federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization conducting the inspection/assessment obtains and examines the documented list of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system, as well as the documented process for information retention to ensure the organization being inspected/assessed retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-15(a)	CCI-001150	The information system prohibits remote activation of collaborative computing devices excluding the organization-defined exceptions where remote activation is to be allowed.	The organization being inspected/assessed configures the information system to prohibit remote activation of collaborative computing devices excluding dedicated VTC suites located in approved VTC locations that are centrally managed. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1150. DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prohibit remote activation of collaborative computing devices excluding dedicated VTC suites located in approved VTC locations that are centrally managed. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1150. DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed.	LOW	X			X				3.7.1 Collaborative Computing	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-15(b)	CCI-001152	The information system provides an explicit indication of use to users physically present at collaborative computing devices.	The organization being inspected/assessed configures the information system to provide an explicit indication of use to users physically present at collaborative computing devices. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1152.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide an explicit indication of use to users physically present at collaborative computing devices. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1152.	LOW	X			X				3.7.1 Collaborative Computing	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-12	CCI-002430	The organization defines the requirements for cryptographic key storage to be employed within the information system.	DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW	X			X	X			3.7.2 Denial of Service Protection...		CCI requirements are addressed within subparagraph "Denial of Service Protection" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-2(a)	CCI-001225	The organization identifies information system flaws.	The organization being inspected/assessed documents and implements a process to identify information system flaws. The process shall include review of the system through automated scans and manual checks to determine the existence of flaws such as IAVM, CVE, or other resources.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed identifies information system flaws.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-2(a)	CCI-001226	The organization reports information system flaws.	The organization being inspected/assessed reports information system flaws according to DoD Cybersecurity policy and organizational roles and responsibilities. The organization must report information system flaws in their POA&M.	The organization conducting the inspection/assessment obtains and examines the authorization package, verifies the POA&M is up to date and includes recently identified information system flaws, and verifies that the organization has notified appropriate personnel as defined by DoD Cybersecurity policy and organizational roles and responsibilities.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-5	CCI-001093	The organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system.	The organization being inspected/assessed defines and documents the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system. DoD has determined the types of denial of service attacks are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented types of denial of service attacks to ensure the organization being inspected/assessed defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system. DoD has determined the types of denial of service attacks are not appropriate to define at the Enterprise level.	LOW	X	X						3.7.2 Denial of Service Protection...		CCI requirements are addressed within subparagraph "Denial of Service Protection" of UFGS 25 05 11.
N/A	SI-2(b)	CCI-001228	The organization tests software updates related to flaw remediation for effectiveness before installation.	The organization being inspected/assessed documents and implements a process to test software updates related to flaw remediation for effectiveness before installation. If the software update is being provided by a vendor who has documented the effectiveness of the update in fixing the affected IAVM/CVE, further testing by the organization may not be required.	The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests software updates related to flaw remediation for effectiveness before installation.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-2(b)	CCI-001229	The organization tests software updates related to flaw remediation for potential side effects before installation.	The organization being inspected/assessed documents and implements a process for regression testing IAW CM-4 to identify any potential side effects before installation of software updates.	The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests software updates related to flaw remediation for potential side effects before installation.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-2(b)	CCI-002602	The organization tests firmware updates related to flaw remediation for effectiveness before installation.	The organization being inspected/assessed documents and implements a process to test firmware updates related to flaw remediation for effectiveness before installation. If the firmware update is being provided by a vendor who has documented the effectiveness of the update in fixing the affected IAVM/CVE, further testing by the organization may not be required.	The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests firmware updates related to flaw remediation for effectiveness before installation.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-2(b)	CCI-002603	The organization tests firmware updates related to flaw remediation for potential side effects before installation.	The organization being inspected/assessed documents and implements a process for regression testing IAW CM-4 to identify any potential side effects before installation of software updates.	The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests firmware updates related to flaw remediation for potential side effects before installation.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-2(c)	CCI-002604	The organization defines the time period within the release of updates that security-related software updates are to be installed.	DoD has defined the time period as 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 30 days	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-5	CCI-002385	The information system protects against or limits the effects of organization-defined types of denial of service attacks by employing organization-defined security safeguards.	The organization being inspected/assessed configures the information system to protect against or limits the effects of types of denial of service attacks defined in SC-5, CCI 1093 by employing security safeguards defined in SC-5, CCI 2386. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2385.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect against or limits the effects of types of denial of service attacks defined in SC-5, CCI 1093 by employing security safeguards defined in SC-5, CCI 2386. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2385.	LOW	X	X						3.7.2 Denial of Service Protection...		CCI requirements are addressed within subparagraph "Denial of Service Protection" of UFGS 25 05 11.
N/A	SI-2(c)	CCI-002606	The organization defines the time period within the release of updates that security-related firmware updates are to be installed.	DoD has defined the time period as 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 30 days	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-2(c)	CCI-002607	The organization installs security-relevant firmware updates within organization-defined time period of the release of the updates	The organization being inspected/assessed configures the information system to install security-relevant firmware updates within 30 days of the release of the updates. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2607. DoD has defined the time period as 30 days.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to install security-relevant firmware updates within 30 days of the release of the updates. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2607. DoD has defined the time period as 30 days.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-5	CCI-002386	The organization defines the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks.	The organization being inspected/assessed defines and documents the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	LOW	X	X	X					3.7.2 Denial of Service Protection...		CCI requirements are addressed within subparagraph "Denial of Service Protection" of UFGS 25 05 11.
N/A	SI-3(a)	CCI-002619	The organization employs malicious code protection mechanisms at information system entry points to detect malicious code.	The organization being inspected/assessed identifies and documents the information system entry points and implements malicious code protection mechanisms at those entry points to detect malicious code. Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies.	The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system entry points and verifies that malicious code protection mechanisms are implemented.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-3(a)	CCI-002620	The organization employs malicious code protection mechanisms at information system exit points to detect malicious code.	The organization being inspected/assessed identifies and documents the information system exit points and implements malicious code protection mechanisms at those exit points to detect malicious code. Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies.	The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system exit points and verifies that malicious code protection mechanisms are implemented.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-3(a)	CCI-002621	The organization employs malicious code protection mechanisms at information system entry points to eradicate malicious code.	The organization being inspected/assessed configures the malicious code protection mechanisms identified in SI-3, CCI 2619 to eradicate malicious code.	The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system entry points and verifies that malicious code protection mechanisms are implemented to eradicate malicious code.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-3(a)	CCI-002622	The organization employs malicious code protection mechanisms at information system exit points to eradicate malicious code.	The organization being inspected/assessed configures the malicious code protection mechanisms identified in SI-3, CCI 2620 to eradicate malicious code.	The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system exit points and verifies that malicious code protection mechanisms are implemented to eradicate malicious code.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-3(b)	CCI-001240	The organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures.	The organization being inspected/assessed configures the information system to update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1240.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1240.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-7(c)	CCI-001098	The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	The organization being inspected/assessed designs the information system to enforce requirements that components connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component connectivity to ensure the organization being inspected/assessed connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	LOW	X							3.7.5 Process Isolation and Boundary Prot...	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-3(c)(1)	CCI-001242	The organization configures malicious code protection mechanisms to perform real-time scans of files from external sources at endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy.	The organization being inspected/assessed configures malicious code protection mechanisms to perform real-time scans of files from external sources at endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1242.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform real-time scans of files from external sources at endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1242.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-12	CCI-002855	The information system, when organization-defined conditions are detected, enters a safe mode of operation with organization-defined restrictions of safe mode of operation.	The organization being inspected/assessed configures the information system to enter a safe mode of operation with restrictions of safe mode of operation defined in CP-12, CCI 2857 when conditions defined in CP-12, CCI 2856 are detected. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2855.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enter a safe mode of operation with restrictions of safe mode of operation defined in CP-12, CCI 2857 when conditions defined in CP-12, CCI 2856 are detected. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2855.	LOW		X						3.8 SAFE MODE AND FAIL SAFE OPERATION		CCI requirements are addressed within subparagraph "Safe Mod and Fail Safe Operation" of UFGS 25 05 11.
N/A	SI-3(c)(1)	CCI-002624	The organization configures malicious code protection mechanisms to perform real-time scans of files from external sources at network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy.	The organization being inspected/assessed configures the malicious code protection mechanisms to perform real-time scans of files from external sources at network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2624.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform real-time scans of files from external sources at network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2624.	LOW	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-3(c)(2)	CCI-001243	The organization configures malicious code protection mechanisms to perform organization-defined action(s) in response to malicious code detection.	The organization being inspected/assessed configures malicious code protection mechanisms to perform block and quarantine malicious code and then send an alert to the administrator immediately in near real-time in response to malicious code detection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1243. DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform block and quarantine malicious code and then send an alert to the administrator immediately in near real-time in response to malicious code detection. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1243. DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-3(c)(2)	CCI-001244	The organization defines one or more actions to perform in response to malicious code detection, such as blocking malicious code, quarantining malicious code, or sending alert to administrator.	DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-3(d)	CCI-001245	The organization addresses the receipt of false positives during malicious code detection and eradication, and the resulting potential impact on the availability of the information system.	The organization being inspected/assessed configures the information system to address the receipt of false positives during malicious code detection and eradication, and the resulting potential impact on the availability of the information system. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1245.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to address the receipt of false positives during malicious code detection and eradication, and the resulting potential impact on the availability of the information system. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1245.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CP-12	CCI-002856	The organization defines the conditions, that when detected, the information system enters a safe mode of operation with organization-defined restrictions of safe mode of operation.	The organization being inspected/assessed defines and documents the conditions, that when detected, the information system enters a safe mode of operation with organization-defined restrictions of safe mode of operation. DoD has determined the conditions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure the organization being inspected/assessed defines the conditions, that when detected, the information system enters a safe mode of operation with organization-defined restrictions of safe mode of operation. DoD has determined the conditions are not appropriate to define at the Enterprise level.	LOW		X						3.8 SAFE MODE AND FAIL SAFE OPERATION		CCI requirements are addressed within subparagraph "Safe Mod and Fail Safe Operation" of UFGS 25 05 11.
N/A	SI-4(a)(1)	CCI-002641	The organization monitors the information system to detect attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives.	The organization being inspected/assessed documents and implements a process to monitor the information system to detect attacks and indicators of potential attacks in accordance with sensor placement and monitoring requirements within CJCSI 6510.01F. The organization must maintain an audit trail of monitoring. DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect attacks and indicators of potential attacks in accordance with sensor placement and monitoring requirements within CJCSI 6510.01F.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(a)(2)	CCI-002642	The organization monitors the information system to detect unauthorized local connections.	The organization being inspected/assessed documents and implements a process to monitor the information system to detect unauthorized local connections. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized local connections.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(a)(2)	CCI-002643	The organization monitors the information system to detect unauthorized network connections.	The organization being inspected/assessed documents and implements a process to monitor the information system to detect unauthorized network connections. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized network connections.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(a)(2)	CCI-002644	The organization monitors the information system to detect unauthorized remote connections.	The organization being inspected/assessed documents and implements a process to monitor information system to detect unauthorized remote connections. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized remote connections.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-12	CCI-002857	The organization defines the restrictions of safe mode of operation that the information system will enter when organization-defined conditions are detected.	The organization being inspected/assessed defines and documents the restrictions of safe mode of operation that the information system will enter when organization-defined conditions are detected. DoD has determined the restrictions on safe mode of operation are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented restrictions to ensure the organization being inspected/assessed defines the restrictions of safe mode of operation that the information system will enter when organization-defined conditions are detected. DoD has determined the restrictions on safe mode of operation are not appropriate to define at the Enterprise level.	LOW		X						3.8 SAFE MODE AND FAIL SAFE OPERATION		CCI requirements are addressed within subparagraph "Safe Mod and Fail Safe Operation" of UFGS 25 05 11.
N/A	SI-4(b)	CCI-002646	The organization identifies unauthorized use of the information system through organization-defined techniques and methods.	The organization being inspected/assessed identifies unauthorized use of the information system through techniques and methods defined in SI-4, CCI 2645. The organization must maintain an audit trail of identified instances of unauthorized use.	The organization conducting the inspection/assessment obtains and examines the audit trail of identified instances of unauthorized use to ensure the organization being inspected/assessed identifies unauthorized use of the information system through techniques and methods defined in SI-4, CCI 2645.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(c)	CCI-001255	The organization deploys monitoring devices strategically within the information system to collect organization determined essential information.	The organization being inspected/assessed documents and implements a process to deploy monitoring devices strategically within the information system to collect organization determined essential information.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed deploys monitoring devices strategically within the information system to collect organization determined essential information.	LOW			X					---	Per UFC 4-10-060 Table G-1 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(c)	CCI-001256	The organization deploys monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization.	The organization being inspected/assessed documents and implements a process to deploy monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed deploys monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(d)	CCI-002647	The organization protects information obtained from intrusion-monitoring tools from unauthorized access.	The organization being inspected/assessed documents and implements a process to protect information obtained from intrusion-monitoring tools from unauthorized access.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects information obtained from intrusion-monitoring tools from unauthorized access.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(d)	CCI-002648	The organization protects information obtained from intrusion-monitoring tools from unauthorized modification.	The organization being inspected/assessed documents and implements a process to protect information obtained from intrusion-monitoring tools from unauthorized modification.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects information obtained from intrusion-monitoring tools from unauthorized modification.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(d)	CCI-002649	The organization protects information obtained from intrusion-monitoring tools from unauthorized deletion.	The organization being inspected/assessed documents and implements a process to protect information obtained from intrusion-monitoring tools from unauthorized deletion.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects information obtained from intrusion-monitoring tools from unauthorized deletion.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-4(e)	CCI-001257	The organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	The organization being inspected/assessed documents and implements a process to heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(f)	CCI-001258	The organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	The organization being inspected/assessed obtains and documents legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	The organization conducting the inspection/assessment obtains and examines the documented legal opinion to ensure the organization being inspected/assessed obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(g)	CCI-002650	The organization defines the information system monitoring information that is to be provided the organization-defined personnel or roles.	The organization being inspected/assessed defines and documents the information system monitoring information that is to be provided the organization-defined personnel or roles. DoD has determined the information system monitoring information is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system monitoring information to ensure the organization being inspected/assessed defines the information system monitoring information that is to be provided the organization-defined personnel or roles. DoD has determined the information system monitoring information is not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(g)	CCI-002651	The organization defines the personnel or roles that are to be provided organization-defined information system monitoring information.	The organization being inspected/assessed defines and documents the personnel or roles that are to be provided organization-defined information system monitoring information. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles that are to be provided organization-defined information system monitoring information. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(g)	CCI-002652	The organization defines the frequency at which the organization will provide the organization-defined information system monitoring information to organization-defined personnel or roles	The organization being inspected/assessed defines and documents the frequency at which the organization will provide the organization-defined information system monitoring information to organization-defined personnel or roles DoD has determined the frequency is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented frequency to ensure the organization being inspected/assessed defines the frequency at which the organization will provide the organization-defined information system monitoring information to organization-defined personnel or roles. DoD has determined the frequency is not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(g)	CCI-002654	The organization provides organization-defined information system monitoring information to organization-defined personnel or roles as needed or per organization-defined frequency.	The organization being inspected/assessed provides information system monitoring information defined in SI-4, CCI 2650 to personnel or roles defined in SI-4, CCI 2651 as needed or per the frequency defined in SI-4, CCI 2652. The organization must maintain an audit trail of when information is provided.	The organization conducting the inspection/assessment obtains and examines the audit trail of when information is provided to ensure the organization being inspected/assessed provides information system monitoring information defined in SI-4, CCI 2650 to personnel or roles defined in SI-4, CCI 2651 as needed or per the frequency defined in SI-4, CCI 2652.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-5(a)	CCI-001285	The organization receives information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis.	The organization being inspected/assessed receives information system security alerts, advisories, and directives from at a minimum, USCYBERCOM on an ongoing basis. DoD has defined the external organizations as at a minimum, USCYBERCOM.	The organization conducting the inspection/assessment obtains and examines alerts, advisories, and directives received by the organization being inspected/assessed to ensure they receive information system security alerts, advisories, and directives from at a minimum, USCYBERCOM on an ongoing basis. DoD has defined the external organizations as at a minimum, USCYBERCOM.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-5(a)	CCI-002692	The organization defines the external organizations from which it receives information system security alerts, advisories and directives.	DoD has defined the external organizations as at a minimum, USCYBERCOM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the external organizations as at a minimum, USCYBERCOM.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-5(b)	CCI-001286	The organization generates internal security alerts, advisories, and directives as deemed necessary.	The organization being inspected/assessed documents and implements a process to generate internal security alerts, advisories, and directives as deemed necessary.	The organization conducting the inspection/assessment obtains and examines documented process as well as the generated internal security alerts, advisories, and directives to ensure the organization being inspected/assessed generates internal security alerts, advisories, and directives as deemed necessary.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-5(c)	CCI-001287	The organization disseminates security alerts, advisories, and directives to organization-defined personnel or roles, organization-defined elements within the organization, and/or organization-defined external organizations.	The organization being inspected/assessed disseminates security alerts, advisories, and directives to the ISSO and ISSM and/or external organizations defined in SI-5, CCI 2694. DoD has defined the personnel or roles as the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines any applicable artifacts showing dissemination of security alerts, advisories, and directives to ensure the organization being inspected/assessed disseminates security alerts, advisories, and directives to the ISSO and ISSM and/or external organizations defined in SI-5, CCI 2694. DoD has defined the personnel or roles as the ISSO and ISSM.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-5(c)	CCI-001288	The organization defines the personnel or roles to whom the organization will disseminate security alerts, advisories and directives.	DoD has defined the personnel or roles as the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSO and ISSM.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-5(c)	CCI-002693	The organization defines the elements within the organization to whom the organization will disseminate security alerts, advisories and directives.	DoD has determined the elements are not applicable as elements are not selected as recipients of security alerts, advisories and directives.	DoD has determined the elements are not applicable as elements are not selected as recipients of security alerts, advisories and directives.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-5(c)	CCI-002694	The organization defines the external organizations to whom the organization will disseminate security alerts, advisories and directives.	DoD has defined the external organizations as CNDSP Tier 1 for vetting. The CNDSP Tier 1 will pass the information to the accredited Tier 2 CNDSPs. Tier 2 CNDSPs are responsible for ensuring all Tier 3 entities receive the information. Tier 3 organizations will ensure all local Op Centers/LAN shops receive information (i.e. Component IT System and Security Personnel) (e.g. ISSM, ISSOs, and system administrators).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the external organizations as CNDSP Tier 1 for vetting. The CNDSP Tier 1 will pass the information to the accredited Tier 2 CNDSPs. Tier 2 CNDSPs are responsible for ensuring all Tier 3 entities receive the information. Tier 3 organizations will ensure all local Op Centers/LAN shops receive information (i.e. Component IT System and Security Personnel) (e.g. ISSM, ISSOs, and system administrators).	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-5(d)	CCI-001289	The organization implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	The organization being inspected/assessed implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	The organization conducting the inspection/assessment examines the information system and obtains and examines records of compliance and/or non-compliance reporting to ensure that security directives have been implemented in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-7 (a)	CCI-003071	The organization develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security.	The organization being inspected/assessed develops and documents a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security.	The organization conducting the inspection/assessment obtains and examines the security CONOPS to ensure the organization being inspected/assessed develops a security CONOPS for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security.	LOW		X						1.9 Cybersecurity Documentation		Default requirement in UFGS 25 05 11 for "Cybersecurity Documentation"
N/A	PL-8(a)	CCI-003072	The organization develops an information security architecture for the information system.	The organization being inspected/assessed develops and documents an information security architecture for the information system.	The organization conducting the inspection/assessment obtains and examines the documented information security architecture to ensure the organization being inspected/assessed develops an information security architecture for the information system.	MOD		X	X					1.9.2 Cybersecurity Interconnection Schedule; 1.9.3 Network Communication Report; 1.9.6 Cybersecurity Riser Diagram		Requirement is met by requiring the contractor to submit the "Cybersecurity Interconnection Schedule", "Network Communications Report", and "Cybersecurity Riser Diagram"
N/A	PL-8(a)(1)	CCI-003073	The organization's information security architecture for the information system describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.	The organization being inspected/assessed describes within the information security architecture for the information system, the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.	The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization being inspected/assessed describes within the information security architecture for the information system, the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.	MOD		X	X					1.9.2 Cybersecurity Interconnection Schedule; 1.9.3 Network Communication Report; 1.9.6 Cybersecurity Riser Diagram		Requirement is met by requiring the contractor to submit the "Cybersecurity Interconnection Schedule", "Network Communications Report", and "Cybersecurity Riser Diagram"
N/A	PL-8(a)(3)	CCI-003075	The organization's information security architecture for the information system describes any information security assumptions about, and dependencies on, external services.	The organization being inspected/assessed describes within the information security architecture for the information system, any information security assumptions about, and dependencies on, external services.	The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization being inspected/assessed describes within the information security architecture for the information system, any information security assumptions about, and dependencies on, external services.	MOD		X	X					1.9.2 Cybersecurity Interconnection Schedule; 1.9.3 Network Communication Report; 1.9.6 Cybersecurity Riser Diagram		Requirement is met by requiring the contractor to submit the "Cybersecurity Interconnection Schedule", "Network Communications Report", and "Cybersecurity Riser Diagram"
N/A	SC-7(9)(a)	CCI-002398	The information system detects outgoing communications traffic posing a threat to external information systems.	The organization being inspected/assessed configures the information system to detect outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2398.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to detect outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2398.	MOD	X	X	X					1.9.2 Cybersecurity Interconnection Schedule; 3.7.3 Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems		CCI requirements are addressed within subparagraph "Cybersecurity Interconnection Schedule" of UFGS 25 05 11.
N/A	SC-7(9)(a)	CCI-002399	The information system denies outgoing communications traffic posing a threat to external information systems.	The organization being inspected/assessed configures the information system to deny outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2399.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to deny outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2399.	MOD	X	X	X					1.9.2 Cybersecurity Interconnection Schedule; 3.7.3 Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems		CCI requirements are addressed within subparagraph "Cybersecurity Interconnection Schedule" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-7(11)	CCI-002401	The organization defines the authorized sources from which the information system will allow incoming communications.	The organization being inspected/assessed defines and documents the authorized sources from which the information system will allow incoming communications. DoD has determined the authorized sources are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented authorized sources to ensure the organization being inspected/assessed defines the authorized sources from which the information system will allow incoming communications. DoD has determined the authorized sources are not appropriate to define at the Enterprise level.	MOD	X	X	X					1.9.2 Cybersecurity Interconnection Schedule		Default Requirement in UFGS 25 05 11 listed in "Cybersecurity Interconnection Schedule"
N/A	SC-7(11)	CCI-002402	The organization defines the authorized destinations for routing inbound communications.	The organization being inspected/assessed defines and documents the authorized destinations for routing inbound communications. DoD has determined the authorized destinations are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented authorized destinations to ensure the organization being inspected/assessed defines the authorized destinations for routing inbound communications. DoD has determined the authorized destinations are not appropriate to define at the Enterprise level.	MOD	X	X	X					1.9.2 Cybersecurity Interconnection Schedule		Default Requirement in UFGS 25 05 11 listed in "Cybersecurity Interconnection Schedule"
N/A	SC-7(11)	CCI-002403	The information system only allows incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.	The organization being inspected/assessed configures the information system to allow incoming communications from authorized sources defined in SC-7 (11), CCI 2401 routed to authorized destinations defined in SC-7 (11), CCI 2402. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2403.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to allow incoming communications from authorized sources defined in SC-7 (11), CCI 2401 routed to authorized destinations defined in SC-7 (11), CCI 2402. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2403.	MOD	X	X	X					1.9.2 Cybersecurity Interconnection Schedule; 3.7.3 Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems		CCI requirements are addressed within subparagraph "Cybersecurity Interconnection Schedule" of UFGS 25 05 11.
N/A	SA-22 (b)	CCI-003374	The organization documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	The organization being inspected/assessed documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	The organization conducting the inspection/assessment obtains and examines the hardware and software lists as well as the documented approvals to ensure the organization being inspected/assessed documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	LOW		X						1.9.8 Control System Cybersecurity Documentation		Requirement is met in "Control System Cybersecurity Documentation"
N/A	SI-7(14)(a)	CCI-002737	The organization prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code.	The organization being inspected/assessed prohibits the use of binary or machine-executable code obtained from sources without vendor support or with no warranty and without the provision of source code.	The organization conducting the inspection/assessment obtains and examines the software list and examines the information system to ensure the organization being inspected/assessed prohibits the use of binary or machine-executable code obtained from sources without vendor support or with no warranty and without the provision of source code.	MOD		X	X	X				1.10 SOFTWARE LICENSING		CCI requirements are addressed within subparagraph "Software Licensing" of UFGS 25 05 11.
N/A	AC-18(3)	CCI-001449	The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.	The organization being inspected/assessed documents and implements a process to disable wireless networking capabilities internally embedded within information system components prior to issuance and deployment when not intended for use.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment. The organization conducting the inspection/assessment obtains and examines a sampling of information systems to ensure that any internally embedded wireless networking capabilities are disabled unless a documented need exists.	MOD		X						3.2.3 Wireless and Wired Broadcast Communication		CCI requirements are addressed in "Wireless and Wired Broadcast Communication" subparagraph
N/A	IA-2(9)	CCI-001942	The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.	The organization being inspected/assessed configures the information system to implement replay-resistant authentication mechanisms for network access to non-privileged accounts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1942.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement replay-resistant authentication mechanisms for network access to non-privileged accounts. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1942.	MOD		X		X						Control System does not contain classified information	
N/A	IA-3(1)	CCI-001959	The organization defines the specific devices and/or type of devices the information system is to authenticate before establishing a connection.	DoD has defined the value as all network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the value as all network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	MOD		X		X	X				Control System does not contain classified information	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-3 (1)	CCI-001967	The information system authenticates organization-defined devices and/or types of devices before establishing a local, remote and/or network connection using bidirectional authentication that is cryptographically based.	The organization being inspected/assessed configures the information system to use cryptographically based bidirectional authentication. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1967.	The organization conducting the inspection/assessment examine a sampling of the network infrastructure device configurations to ensure devices connecting to the infrastructure use cryptographically based bidirectional authentication. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1967.	MOD		X		X					Control System does not contain classified information	
SC-8	SC-8	CCI-002418	The information system protects the confidentiality and/or integrity of transmitted information.	The organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of transmitted information. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2418.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of transmitted information. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2418.	MOD		X							Control System does not contain classified information	
N/A	SC-23(1)	CCI-001185	The information system invalidates session identifiers upon user logout or other session termination.	The organization being inspected/assessed configures the information system to invalidate session identifiers upon user logout or other session termination. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1185.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to invalidate session identifiers upon user logout or other session termination. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1185.	MOD		X							Control System does not contain classified information	
N/A	SC-23(3)	CCI-001188	The information system generates unique session identifiers for each session with organization-defined randomness requirements.	The organization being inspected/assessed configures the information system to generate unique session identifiers for each session with randomness requirements defined in SC-23 (3), CCI 1189. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1188.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to generate unique session identifiers for each session with randomness requirements defined in SC-23 (3), CCI 1189. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1188.	MOD		X							Control System does not contain classified information	
N/A	SC-23(3)	CCI-001664	The information system recognizes only session identifiers that are system-generated.	The organization being inspected/assessed configures the information system to recognize only session identifiers that are system-generated. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1664.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to recognize only session identifiers that are system-generated. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1664.	MOD		X							Control System does not contain classified information	
N/A	AC-6(1)	CCI-001558	The organization defines the security functions (deployed in hardware, software, and firmware) for which access must be explicitly authorized.	DoD has defined the security functions as all functions not publicly accessible.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security functions as all functions not publicly accessible.	MOD		X		X	X			3.3.1 User Accounts; 3.4 USER IDENTIFICATION AND AUTHENTICATION; 3.2.3 IP Controls Networks		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts", "USER IDENTIFICATION AND AUTHENTICATION", and "IP Controls Networks" within Part 3
N/A	AC-6(1)	CCI-002221	The organization defines the security-relevant information for which access must be explicitly authorized.	DoD has defined the security-relevant information as all security-relevant information not publicly available.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security-relevant information as all security-relevant information not publicly available.	MOD		X		X	X			3.3.1 User Accounts		CCI requirements are addressed within subparagraph "User Accounts" of UFGS 25 05 11.
N/A	AC-6(1)	CCI-002222	The organization explicitly authorizes access to organization-defined security functions.	The organization being inspected/assessed documents and implements a process to explicitly authorize access to all functions not publicly accessible. Explicit authorization can be in the form of an acceptable use policy signed by the user at the time of access being granted. DoD has defined the security functions as all functions not publicly accessible.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed explicitly authorizes access to all functions not publicly accessible. DoD has defined the security functions as all functions not publicly accessible.	MOD		X		X	X			3.3.1 User Accounts; 3.4 USER IDENTIFICATION AND AUTHENTICATION		CCI requirements are addressed within subparagraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-6(1)	CCI-002223	The organization explicitly authorizes access to organization-defined security-relevant information.	The organization being inspected/assessed documents and implements a process to explicitly authorize access to all security-relevant information not publicly available. Explicit authorization can be in the form of an acceptable use policy signed by the user at the time of access being granted. DoD has defined the security-relevant information as all security-relevant information not publicly available.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed explicitly authorizes access to all security-relevant information not publicly available. DoD has defined the security-relevant information as all security-relevant information not publicly available.	MOD		X		X	X			3.3.1 User Accounts; 3.4 USER IDENTIFICATION AND AUTHENTICATION		CCI requirements are addressed within subparagraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION" of UFGS 25 05 11.
N/A	AC-6(10)	CCI-002235	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	The organization being inspected/assessed configures the information system to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2235.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2235.	MOD		X		X				3.3.1 User Accounts; 3.4 USER IDENTIFICATION AND AUTHENTICATION		CCI requirements are addressed within subparagraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION" of UFGS 25 05 11.
N/A	AC-6(2)	CCI-000039	The organization requires that users of information system accounts or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing nonsecurity functions.	The organization being inspected/assessed documents and implements a process to require that users of information system accounts or roles, with access to any privileged security functions or security-relevant information, use non-privileged accounts, or roles, when accessing nonsecurity functions. DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires that users of information system accounts or roles, with access to any privileged security functions or security-relevant information, use non-privileged accounts, or roles, when accessing nonsecurity functions. DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.	MOD		X		X	X			3.3.1 User Accounts; 3.4 USER IDENTIFICATION AND AUTHENTICATION		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION" within Part 3
N/A	AC-6(2)	CCI-001419	The organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access.	DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.	MOD		X		X	X			3.3.1 User Accounts; 3.4 USER IDENTIFICATION AND AUTHENTICATION		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION"within Part 3
N/A	AC-6(9)	CCI-002234	The information system audits the execution of privileged functions.	The organization being inspected/assessed configures the information system to audit the execution of privileged functions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2234.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to audit the execution of privileged functions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2234.	MOD		X		X				3.3.1 User Accounts; 3.4 USER IDENTIFICATION AND AUTHENTICATION		CCI requirements are addressed within subparagraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION" of UFGS 25 05 11.
N/A	CM-11(2)	CCI-001812	The information system prohibits user installation of software without explicit privileged status.	The organization being inspected/assessed must configure the information system to prevent the installation of software by non-privileged users. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1812.	The organization conducting the inspection/assessment obtains and examines the configuration of the information system components to ensure that installation of software without explicit privileged status is prohibited. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1812.	MOD		X	X					3.3.1 User Accounts		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts" within Part 3

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-10	CCI-000166	The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.	The organization being inspected/assessed configures the information system to protect against an individual falsely denying having performed actions to be covered by non-repudiation defined in DoDI 8520.02 and DoDI 8520.03. DoDI 8520.02 and DoDI 8520.03 meet the DoD requirement to define the actions to be covered by non-repudiation. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 166.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed protects against an individual falsely denying having performed actions to be covered by non-repudiation defined in DoDI 8520.02 and DoDI 8520.03. DoDI 8520.02 and DoDI 8520.03 meet the DoD requirement to define the actions to be covered by non-repudiation. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 166.	MOD		X						3.5.1 Audit Events, Content of Audit Records, and Audit Generation		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-10	CCI-001899	The organization defines the action to be covered by non-repudiation.	DoD has defined the actions to be covered by non-repudiation as actions defined by DoDI 8520.02 and DoDI 8520.03.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the actions to be covered by non-repudiation as actions defined by DoDI 8520.02 and DoDI 8520.03.	MOD		X	X		X			3.5.1 Audit Events, Content of Audit Records, and Audit Generation		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-12(3)	CCI-001914	The information system provides the capability for organization-defined individuals or roles to change the auditing to be performed on organization-defined information system components based on organization-defined selectable event criteria within organization-defined time thresholds.	The organization being inspected/assessed configures the information system to provide the capability for individuals or roles defined in AU-12 (3), CCI 1913 to change the auditing to be performed on information system components defined in AU-12 (3), CCI 2047 based on selectable event criteria defined in AU-12 (3), CCI 1911 within time thresholds defined in AU-12 (3), CCI 1912. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1914.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for individuals or roles defined in AU-12 (3), CCI 1913 to change the auditing to be performed on information system components defined in AU-12 (3), CCI 2047 based on selectable event criteria defined in AU-12 (3), CCI 1911 within time thresholds defined in AU-12 (3), CCI 1912. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1914.	MOD		X						3.5.1 Audit Events, Content of Audit Records, and Audit Generation		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-14(b)	CCI-001919	The information system provides the capability for authorized users to select a user session to capture/record or view/hear.	The organization being inspected/assessed configures the information system to provide the capability for authorized users to select a user session to capture/record or view/hear. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1919.	The organization conducting the inspection/assessments examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for authorized users to select a user session to capture/record or view/hear. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1919.	MOD		X	X					3.5.1 Audit Events, Content of Audit Records, and Audit Generation		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-14(1)	CCI-001464	The information system initiates session audits at system start-up.	The organization being inspected/assessed configures the information system to initiate session audits at system start-up. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1464.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to initiate session audits at system start-up. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1464.	MOD		X	X					3.5.1 Audit Events, Content of Audit Records, and Audit Generation		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-14(2)	CCI-001462	The information system provides the capability for authorized users to capture/record and log content related to a user session.	The organization being inspected/assessed configures the information system to provide the capability for authorized users to capture/record and log content related to a user session. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1462.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for authorized users to capture/record and log content related to a user session. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1462.	MOD		X	X					3.5.1 Audit Events, Content of Audit Records, and Audit Generation		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to FRCS	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11- Reference	Rational for Non-inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-14 (3)	CCI-001920	The information system provides the capability for authorized users to remotely view/hear all content related to an established user session in real time.	The organization being inspected/assessed configures the information system to provide the capability for authorized users to remotely view/hear all content related to an established user session in real time. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1920.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for authorized users to remotely view/hear all content related to an established user session in real time. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1920.	LOW		X						3.5.1 Audit Events, Content of Audit Records, and Audit Generation		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	CM-5(1)	CCI-001814	The Information system supports auditing of the enforcement actions.	The organization being inspected/assessed leverages only information systems which support auditing of enforcement actions.	The organization conducting the inspection/assessment reviews vendor documentation to ensure the information system supports auditing of the enforcement actions. If vendor documentation is not available, the organization conducting the inspection/assessment tests the information system for the capability.	MOD		X	X					3.5.1 Audit Events, Content of Audit Records, and Audit Generation		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	SC-7(9)(b)	CCI-002400	The information system audits the identity of internal users associated with denied outgoing communications traffic posing a threat to external information systems.	The organization being inspected/assessed configures the information system to audit the identity of internal users associated with denied outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2400.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to audit the identity of internal users associated with denied outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2400.	MOD		X		X				3.5.1 Audit Events, Content of Audit Records, and Audit Generation		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	SI-10(3)	CCI-002754	The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.	The organization being inspected/assessed documents proper behavior that reflects organizational and system objectives for when invalid inputs are received. The organization being inspected/assessed configures the information system to behave in the documented manner when invalid inputs are received. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2754.	The organization conducting the inspection/assessment obtains and examines the documented behavior to ensure the organization being inspected/assessed documents proper behavior that reflects organizational and system objectives for when invalid inputs are received. The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to behave in the documented manner when invalid inputs are received. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2754.	MOD		X		X				3.8 SAFE MODE AND FAIL SAFE OPERATION		CCI requirements are addressed within subparagraph "Safe Mod and Fail Safe Operation" of UFGS 25 05 11.
N/A	MA-3	CCI-000865	The organization approves information system maintenance tools.	The organization being inspected/assessed documents the approved maintenance tools within the Security Plan.	The organization conducting the inspection/assessment: 1. obtains and examines the Security Plan to ensure the list of approved maintenance tools is documented; 2. ensures only the approved maintenance tools are used within the system.	MOD		X	X					3.9 SYSTEM MAINTENANCE TOOL SOFTWARE		CCI requirements are addressed within subparagraph "System Maintenance Tool Software" of UFGS 25 05 11.
N/A	CM-7(3)	CCI-000388	The organization ensures compliance with organization-defined registration requirements for functions, ports, protocols, and services.	The organization being inspected/assessed implements DoDI 8551.01. DoD has defined the registration requirements as IAW DoDI 8551.01.	The organization conducting the inspection/assessment obtains and examines a documented listing of ports, protocols, and services in use, and reviews a sampling of those ports, protocols, and services to ensure the organization being inspected/assessed is compliant with DoDI 8551.01. DoD has defined the registration requirements as IAW DoDI 8551.01.	MOD		X	X					1.9.3 Network Communication Report		Requirements met in UFGS 25 05 11 within "Network Communications Requirement" submission

CCI List and Tailoring Information

Fire & Life Safety (FLS)

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-1(a)(1)	CCI-000001	The organization develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization being inspected/assessed develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization conducting the inspection/assessment obtains and examines the access control policy to ensure the organization being inspected/assessed develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-1(a)(1)	CCI-000002	The organization disseminates the access control policy to organization-defined personnel or roles.	The organization being inspected/assessed disseminates via an information sharing capability to all personnel. DoD has defined the personnel or roles as all personnel.	The organization conducting the inspection/assessment examines the access control policy via the organization's information sharing capability to ensure the organization being inspected/assessed disseminates the policy to all personnel. DoD has defined the personnel or roles as all personnel.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-1(b)(1)	CCI-000003	The organization reviews and updates the access control policy in accordance with organization-defined frequency.	The organization being inspected/assessed annually reviews and updates the access control policy. The organization must maintain review and update activity as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed annually reviews and updates the access control policy. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-1(a)(2)	CCI-000004	The organization develops and documents procedures to facilitate the implementation of the access control policy and associated access controls.	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of the access control policy and associated access controls.	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the access control policy and associated access controls to ensure the organization being inspected/assessed develops and documents procedures to facilitate the implementation of the access control policy and associated access controls.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-1(a)(2)	CCI-000005	The organization disseminates the procedures to facilitate access control policy and associated access controls to the organization-defined personnel or roles .	The organization being inspected/assessed disseminates via an information sharing capability to all personnel the procedures to facilitate access control policy and associated access controls. DoD has defined the personnel or roles as all personnel.	The organization conducting the inspection/assessment examines the procedures to facilitate access control policy and associated access controls via the organization's information sharing capability to ensure the organization being inspected/assessed disseminates the procedures to all personnel. DoD has defined the personnel or roles as all personnel.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-1(b)(2)	CCI-000006	The organization reviews and updates the access control procedures in accordance with organization-defined frequency.	The organization being inspected/assessed annually reviews and updates the access control procedures. The organization must maintain review and update activity as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed annually reviews and updates the access control procedures. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(c)	CCI-000008	The organization establishes conditions for group membership.	The organization being inspected/assessed documents conditions for adding accounts as members of groups.	The organization conducting the inspection/assessment obtains and examines the documented conditions for adding accounts as members of groups to ensure that the conditions are established.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(e)	CCI-000010	The organization requires approvals by organization-defined personnel or roles for requests to create information system accounts.	The organization being inspected/assessed implements a process for the ISSM or ISSO to approve information system account requests. The organization being inspected/assessed maintains an audit trail of approvals. DoD has defined the personnel or roles as the ISSM or ISSO.	The organization conducting the inspection/assessment obtains and examines the audit trail of approvals to ensure that the organization being inspected/assessed implements a process for the ISSM or ISSO to approve information system account requests. DoD has defined the personnel or roles as the ISSM or ISSO.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(f)	CCI-000011	The organization creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions.	The organization being inspected/assessed implements account maintenance processes to create, enable, modify, disable, and remove information system accounts in accordance with procedures or conditions defined in AC-2, 2121. The organization being inspected/assessed maintains an audit trail of account maintenance activities.	The organization conducting the inspection/assessment obtains and examines the audit trail of account maintenance activities to ensure the organization being inspected/assessed implements account maintenance processes to create, enable, modify, disable, remove, and track information system accounts in accordance with procedures or conditions defined in AC-2, 2121.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(j)	CCI-000012	The organization reviews information system accounts for compliance with account management requirements per organization-defined frequency.	The organization being inspected/assessed implements a process to review information system accounts for compliance with account management requirements at a minimum, annually. The organization being inspected/assessed maintains an audit trail of reviews. DoD has defined the frequency as at a minimum, annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organization being inspected/assessed implements a process to review information system accounts for compliance with account management requirements at a minimum, annually. DoD has defined the frequency as at a minimum, annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(1)	CCI-000015	The organization employs automated mechanisms to support the information system account management functions.	The organization being inspected/assessed configures the information system to employ automated mechanisms to support the information system account management functions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 000015.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to employ automated mechanisms to support the information system account management functions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 000015.	MOD	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-2(2)	CCI-000016	The information system automatically removes or disables temporary accounts after an organization-defined time period for each type of account.	The organization being inspected/assessed configures the information system to automatically remove or disable temporary accounts after 72 hours. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 000016. DoD has defined the time period as 72 hours.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically remove or disable temporary accounts after 72 hours. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 000016. DoD has defined the time period as 72 hours.	MOD	X			X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(3)	CCI-000017	The information system automatically disables inactive accounts after an organization-defined time period.	The organization being inspected/assessed configures the information system to disable inactive accounts after 35 days. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 000017. DoD has defined the time period as 35 days.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to disable inactive accounts after 35 days. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 000017. DoD has defined the time period as 35 days.	MOD	X	X	X	X	X			3.3.1 User Accounts		CCI requirements are met within subparagraph "User Accounts" of UFGS 25 05 11.
N/A	AC-2(4)	CCI-000018	The information system automatically audits account creation actions.	The organization being inspected/assessed configures the information system to automatically audit account creation actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 18.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically audit account creation actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 18.	MOD	X	X		X				3.3.1 User Accounts		CCI requirements are met within subparagraph "User Accounts" of UFGS 25 05 11.
N/A	AC-2(5)(a)	CCI-000019	The organization requires that users log out in accordance with the organization-defined time period of inactivity and/or description of when to log out.	The organization being inspected/assessed documents in the user policies that users are required to log out at the end of the users standard work period unless otherwise defined in formal organizational policy and IAW conditions defined in AC-2 (5) CCI 2133. DoD has defined the time period as at the end of the users standard work period unless otherwise defined in formal organizational policy.	The organization conducting the inspection/assessment obtains and examines the user policies to ensure that users are required to log out at the end of the users standard work period unless otherwise defined in formal organizational policy and IAW conditions defined in AC-2 (5) CCI 2133. DoD has defined the time period as at the end of the users standard work period unless otherwise defined in formal organizational policy.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AC-5(a)	CCI-000036	The organization separates organization-defined duties of individuals.	The organization being inspected/assessed documents and implements processes to maintain separation of the duties defined in AC-5, CCI 2219 across different individuals within the organization.	The organization conducting the inspection/assessment obtains and examines the documented processes to ensure the organization being inspected/assessed maintains separation of the duties defined in AC-5, CCI 2219 across different individuals within the organization.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-6(2)	CCI-000039	The organization requires that users of information system accounts or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing nonsecurity functions.	The organization being inspected/assessed documents and implements a process to require that users of information system accounts or roles, with access to any privileged security functions or security-relevant information, use non-privileged accounts, or roles, when accessing nonsecurity functions. DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires that users of information system accounts or roles, with access to any privileged security functions or security-relevant information, use non-privileged accounts, or roles, when accessing nonsecurity functions. DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.	MOD		X		X	X			3.3.1 User Accounts 3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION" within Part 3
N/A	AC-7(a)	CCI-000043	The organization defines the maximum number of consecutive invalid logon attempts to the information system by a user during an organization-defined time period.	DoD has defined the maximum number as three.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the maximum number as three.	LOW		X		X	X			3.3.2 Unsuccessful Logon Attempts		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "Unsuccessful Logon Attempts" within Part 3
N/A	AC-7(a)	CCI-000044	The information system enforces the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.	The organization being inspected/assessed configures the information system to limit invalid logon attempts by a user to three attempts during a 15 minute time period. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 44. DoD has defined the maximum number as three. DoD has defined the time period as 15 minutes.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to limit invalid logon attempts by a user to three attempts during a 15 minute time period. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 44. DoD has defined the maximum number as three. DoD has defined the time period as 15 minutes.	LOW		X						3.3.2 Unsuccessful Logon Attempts		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "Unsuccessful Logon Attempts" within Part 3

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-8(a)	CCI-000048	The information system displays an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The organization being inspected/assessed configures the information system to display the DoD Information Systems – Standard Consent Banner and User Agreement before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 48. DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display the DoD Information Systems – Standard Consent Banner and User Agreement before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 48. DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	LOW	X	X		X				3.3.3 System Use Notification		Cybersecurity requirements are met within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-8(b)	CCI-000050	The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access.	The organization being inspected/assessed configures the information system to retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 50.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 50.	LOW	X	X						3.3.3 System Use Notification		Cybersecurity requirements are met within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-10	CCI-000054	The information system limits the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number of sessions.	The organization being inspected/assessed configures the information system to limit the number of concurrent sessions for all accounts and/or account types to a number of sessions defined in AC-10, CCI 55. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 54. DoD has defined the account types and/or accounts as all account types and/or accounts.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to limit the number of concurrent sessions for all accounts and/or account types to a number of sessions defined in AC-10, CCI 55. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 54. DoD has defined the account types and/or accounts as all account types and/or accounts.	MOD		X			X			3.3.4 Session Lock and Session Terminatio...		CCI requirements are addressed within subparagraph "Session Lock and Session Termination Requirements In MODERATE Impact Systems:" of UFGS 25 05 11.
N/A	AC-10	CCI-000055	The organization defines the maximum number of concurrent sessions to be allowed for each organization-defined account and/or account type.	The organization being inspected/assessed defines and documents the maximum number of concurrent sessions to be allowed for each organization-defined account and/or account type. The maximum number of concurrent sessions should be defined based upon the systems operational environment and mission needs. DoD has determined the maximum number is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented maximum number to ensure the organization being inspected/assessed defines the maximum number of concurrent sessions to be allowed for each organization-defined account and/or account type. DoD has determined the maximum number is not appropriate to define at the Enterprise level.	MOD		X	X					3.3.4 Session Lock and Session Terminatio...		CCI requirements are addressed within subparagraph "Session Lock and Session Termination Requirements In MODERATE Impact Systems:" of UFGS 25 05 11.
N/A	AC-11(b)	CCI-000056	The information system retains the session lock until the user reestablishes access using established identification and authentication procedures.	The organization being inspected/assessed configures the information system to retain the session lock until the user reestablishes access using established identification and authentication procedures. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 56.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to retain the session lock until the user reestablishes access using established identification and authentication procedures. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 56.	MOD	X	X		X				3.3.4 Session Lock and Session Terminatio...		CCI requirements are addressed within subparagraph "Session Lock and Session Termination Requirements In MODERATE Impact Systems:" of UFGS 25 05 11.
N/A	AC-11(a)	CCI-000057	The information system initiates a session lock after the organization-defined time period of inactivity.	The organization being inspected/assessed configures the information system to initiate a session lock after the organization-defined time period defined in CCI 59.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to initiate a session lock after the organization-defined time period defined in CCI 59.	MOD								3.3.4 Session Lock and Session Terminatio...		CCI requirements are addressed within subparagraph "Session Lock and Session Termination Requirements In MODERATE Impact Systems:" of UFGS 25 05 11.
N/A	AC-11(a)	CCI-000058	The information system provides the capability for users to directly initiate session lock mechanisms.	The organization being inspected/assessed configures the information system to provide the capability for users to directly initiate session lock mechanisms. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 58.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for users to directly initiate session lock mechanisms. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 58.	MOD	X	X		X				3.3.4 Session Lock and Session Terminatio...		CCI requirements are addressed within subparagraph "Session Lock and Session Termination Requirements In MODERATE Impact Systems:" of UFGS 25 05 11.
N/A	AC-11(a)	CCI-000059	The organization defines the time period of inactivity after which the information system initiates a session lock.	DoD has defined the time period as 15 minutes.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 15 minutes.	MOD	X	X		X	X			3.3.4 Session Lock and Session Terminatio...		CCI requirements are addressed within subparagraph "Session Lock and Session Termination Requirements In MODERATE Impact Systems:" of UFGS 25 05 11.
N/A	AC-14(a)	CCI-000061	The organization identifies and defines organization-defined user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions.	The organization being inspected/assessed identifies, defines, and documents user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions. DoD has determined the user actions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented user actions to ensure the organization being inspected/assessed identifies and defines the user actions that can be performed on the information system without identification and authentication. DoD has determined the user actions are not appropriate to define at the Enterprise level.	LOW		X						3.3.5 Permitted Actions Without Identific...		CCI requirements are addressed within subparagraph "Permitted Actions Without Identification or Authentication" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-17(a)	CCI-000063	The organization defines allowed methods of remote access to the information system.	The organization being inspected/assessed defines and documents the allowed methods of remote access to the information system. The methods should be defined IAW ports, protocols, and service requirements, as well as access control requirements for any STIGs applicable to the technology in use. DoD has determined the allowed methods of remote access are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented methods to ensure the organization being inspected/assessed defines allowed methods of remote access to the information system. DoD has determined the allowed methods of remote access are not appropriate to define at the Enterprise level.	LOW	X		X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-17(b)	CCI-000065	The organization authorizes remote access to the information system prior to allowing such connections	The organization being inspected/assessed authorizes remote access to the information system prior to allowing such connections. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes remote access to the information system prior to allowing such connections.	LOW	X		X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-17(1)	CCI-000067	The information system monitors remote access methods.	The organization being inspected/assessed configures the information system to monitor remote access methods. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 67.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to monitor remote access methods. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 67.	MOD	X								---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(2)	CCI-000068	The information system implements cryptographic mechanisms to protect the confidentiality of remote access sessions.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the confidentiality of remote access sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 68.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the confidentiality of remote access sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 68.	MOD	X								---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(3)	CCI-000069	The information system routes all remote accesses through organization-defined number managed network access control points.	The organization being inspected/assessed configures the information system to route all remote accesses through the number of managed network access control points defined in AC-17 (3), CCI 2315. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 69.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to route all remote accesses through the number of managed network access control points defined in AC-17 (3), CCI 2315. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 69.	MOD	X		X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-17(4)(a)	CCI-000070	The organization authorizes the execution of privileged commands via remote access only for organization-defined needs.	The organization being inspected/assessed authorizes the execution of privileged commands via remote access only for needs defined in AC-17 (4), CCI 2317. The organization being inspected/assessed maintains an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes the execution of privileged commands via remote access only for needs defined in AC-17 (4), CCI 2317.	MOD	X		X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-1(a)(1)	CCI-000073	The organization develops an organization-wide information security program plan that provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X		X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-1(a)(4)	CCI-000074	The organization develops an organization-wide information security program plan that is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW					X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-1(b)	CCI-000075	The organization reviews the organization-wide information security program plan on an organization-defined frequency.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X		X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-1(b)	CCI-000076	The organization defines the frequency to review the organization-wide information security program plan.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW					X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-1(c)	CCI-000077	The organization updates the plan to address organizational changes and problems identified during plan implementation or security control assessments.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X		X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-2	CCI-000078	The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	The Deputy DoD CIO for Cyber Security is the DoD Senior Information Security Officer (SISO), appointed in writing with the mission and resources to coordinate, develop, implement and maintain a DoD-wide information security program.	DoD organizations are automatically compliant with this CCI as they are covered by the appointment of the DoD SISO.	LOW				X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures		Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PM-3(a)	CCI-000080	The organization ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement.	The organization being inspected/assessed documents and implements a process to ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement.	LOW	X		X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-3(b)	CCI-000081	The organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required.	The organization being inspected/assessed documents and implements a process to employ a business case/Exhibit 300/Exhibit 53 to record the resources required.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs a business case/Exhibit 300/Exhibit 53 to record the resources required.	LOW	X		X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-19(a)	CCI-000082	The organization establishes usage restrictions for organization controlled mobile devices.	The organization being inspected/assessed establishes and documents usage restrictions for organization controlled mobile devices.	The organization conducting the inspection/assessment obtains and examines the documented usage restrictions to ensure the organization being inspected/assessed establishes usage restrictions for organization controlled mobile devices.	LOW	X		X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-19(a)	CCI-000083	The organization establishes implementation guidance for organization controlled mobile devices.	The organization being inspected/assessed establishes and documents implementation guidance for organization controlled mobile devices.	The organization conducting the inspection/assessment obtains and examines the documented implementation guidance to ensure the organization being inspected/assessed establishes implementation guidance for organization controlled mobile devices.	LOW	X		X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-19(b)	CCI-000084	The organization authorizes connection of mobile devices to organizational information systems.	The organization being inspected/assessed authorizes connection of mobile devices to organizational information systems. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes connection of mobile devices to organizational information systems.	LOW	X		X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-20(a)	CCI-000093	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems.	The organization being inspected/assessed establishes and documents terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems.	The organization conducting the inspection/assessment obtains and examines the documented terms and conditions to ensure the organization being inspected/assessed establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems.	LOW	X		X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-21(a)	CCI-000098	The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information circumstances where user discretion is required.	The organization being inspected/assessed documents and implements a process to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for information circumstances defined in AC-21, CCI 1470 where user discretion is required.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed determines whether access authorizations assigned to the sharing partner match the access restrictions on the information for information circumstances defined in AC-21, CCI 1470 where user discretion is required.	LOW	X		X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AT-1(a)(1)	CCI-000100	The organization develops and documents a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. Comment: DoDD 8570.01 will be updated with DoDD 8140 once signed. The organization's use of their higher command policy/procedures meets this requirement if more stringent.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. Comment: The organization's use of their higher command policy/procedures meets this requirement if more stringent.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-1(a)(1)	CCI-000101	The organization disseminates a security awareness and training policy to organization-defined personnel or roles.	DoD disseminates DoDD 8570.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-1(b)(1)	CCI-000102	The organization reviews and updates the current security awareness and training policy in accordance with organization-defined frequency.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW					X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-1(a)(2)	CCI-000103	The organization develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	DoD develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls within DoDD 8570.01. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-1(a)(2)	CCI-000104	The organization disseminates security awareness and training procedures to organization-defined personnel or roles.	DoD disseminates DoDD 8570.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. DoD has defined the roles as organizational personnel with security awareness and training responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. DoD has defined the roles as organizational personnel with security awareness and training responsibilities.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-1(b)(2)	CCI-000105	The organization reviews and updates the current security awareness and training procedures in accordance with organization-defined frequency.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. DoD has defined the frequency as annually.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01. DoD has defined the frequency as annually.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AT-2(a)	CCI-000106	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-3(a)	CCI-000108	The organization provides role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the information system or performing assigned duties	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT for privileged users is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT for privileged users is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-3(b)	CCI-000109	The organization provides role-based security training to personnel with assigned security roles and responsibilities when required by information system changes.	Privileged user type Security-related education/training available through DISA IASE (e.g. VTE, Skill Soft, other professional sources) meets the provision of this control. The organization being inspected/assessed may define specific requirements within the above listed sources for their personnel.	The organization conducting the inspection/assessment obtains and examines documented records (IAW AT-4) of their privileged users training.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-3(c)	CCI-000110	The organization provides refresher role-based security training to personnel with assigned security roles and responsibilities in accordance with organization-defined frequency.	Privileged user type Security-related education/training available through DISA IASE (e.g. VTE, Skill Soft, other professional sources) meets the provision of this control. The organization being inspected/assessed may define specific requirements within the above listed sources for their personnel.	The organization conducting the inspection/assessment obtains and examines documented records (IAW AT-4) of their privileged users training.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-3(c)	CCI-000111	The organization defines a frequency for providing refresher role-based security training.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-2(b)	CCI-000112	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) when required by information system changes.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-4(a)	CCI-000113	The organization documents individual information system security training activities, including basic security awareness training and specific information system security training.	The organization being inspected/assessed identifies and documents training activities to include basic security awareness training (per AT-2) and role-based security related training (per AT-3) IAW DoD 8570.01M.	The organization conducting the inspection/assessment obtains and examines the security awareness training activities to ensure the organization being inspected/assessed documents training activities to include basic security awareness training (per AT-2) and role-based security related training (per AT-3) IAW DoD 8570.01M.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-4(a)	CCI-000114	The organization monitors individual information system security training activities, including basic security awareness training and specific information system security training.	The organization being inspected/assessed maintains and monitors records identifying personnel who have received training and the date the training was received	The organization conducting the inspection/assessment obtains and examines records identifying personnel who have received training and the date the training was received	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-1(a)(1)	CCI-000117	The organization develops and documents an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization being inspected/assessed develops and documents an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization conducting the inspection/assessment obtains and examines the audit and accountability policy to ensure that the audit and accountability policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-1(b)(1)	CCI-000119	The organization reviews and updates the audit and accountability policy on an organization-defined frequency.	The organization being inspected/assessed reviews and updates the audit and accountability policy annually. The organization must maintain an audit trail of reviews and updates. Any changes or acceptance of the document without change must be captured in the audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the audit and accountability policy annually. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-1(a)(2)	CCI-000120	The organization develops and documents procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The organization conducting the inspection/assessment obtains and examines the audit and accountability procedures to ensure that the procedures facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-1(b)(2)	CCI-000122	The organization reviews and updates the audit and accountability procedures on an organization-defined frequency.	The organization being inspected/assessed reviews and updates the audit and accountability procedures annually. The organization must maintain an audit trail of reviews and updates. Any changes or acceptance of the document without change must be captured in the audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the audit and accountability procedures annually. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-2(a)	CCI-000123	The organization determines the information system must be capable of auditing an organization-defined list of auditable events.	The organization being inspected/assessed determines whether the information system is capable of auditing: - successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. Classification levels), - Successful and unsuccessful logon attempts, - Privileged activities or other system level access, - Starting and ending time for user access to the system, - Concurrent logons from different workstations, - Successful and unsuccessful accesses to objects, - All program initiations, - All direct access to the information system, - All account creations, modifications, disabling, and terminations, - All kernel module load, unload, and restart. The organization must document those auditable events that are not captured. DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time	The organization conducting the inspection/assessment obtains and examines the documentation of the auditable events to ensure the information system is capable of auditing the: - successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. Classification levels), - Successful and unsuccessful logon attempts, - Privileged activities or other system level access, - Starting and ending time for user access to the system, - Concurrent logons from different workstations, - Successful and unsuccessful accesses to objects, - All program initiations, - All direct access to the information system, - All account creations, modifications, disabling, and terminations, - All kernel module load, unload, and restart. DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module load, unload, and restart.	LOW		X	X					3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within Sub-Paragraph "Audit Events, Content of Audit Records, and Audit Generation" within Part 3
N/A	AU-2(b)	CCI-000124	The organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.	The organization being inspected/assessed documents and implements within the audit and accountability policy and procedures, a process to coordinate the additional auditable events. The objective is to enhance mutual support and to help guide the selection of auditable events. The organization must maintain artifacts of the coordination.	The organization conducting the inspection/assessment obtains and examines the audit and accountability policy and procedures as well as artifacts of the coordination to determine if coordination is necessary and if necessary, whether it has been performed.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-2(c)	CCI-000125	The organization provides a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents.	The organization being inspected/assessed documents in the audit and accountability policy the list of auditable system events, the organization provides clearly stated rationale for the selection of each system event. The rationale will support any after-action investigations of security event.	The organization conducting the inspection/assessment obtains and examines the audit and accountability policy and procedures to ensure the organization being inspected/assess has defined the auditable system events, rationale for the selection, and that the organization has defined how the auditable events will support after action investigations of security events.	LOW		X	X					3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-2(d)	CCI-000126	The organization determines that the organization-defined subset of the auditable events defined in AU-2 are to be audited within the information system.	The organization conducting the inspection/assessment reviews the documented audit process as well as audit logs to ensure that the organization being inspected/assessed audits all auditable events defined in AU-2 (a) per occurrence. DoD has defined the actions as all auditable events defined in AU-2 (a) per occurrence.	The organization conducting the inspection/assessment reviews the documented audit process as well as audit logs to ensure that the organization being inspected/assessed audits all auditable events defined in AU-2 (a) per occurrence. DoD has defined the actions as all auditable events defined in AU-2 (a) per occurrence.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-2(3)	CCI-000127	The organization reviews and updates the list of organization-defined audited events on an organization-defined frequency.	The organization being inspected/assessed will conduct reviews of the list of auditable events as defined in AU-2 (d), CCI 1485 annually or more frequently upon changes to situational awareness of threats or vulnerabilities. The organization will generate and maintain an audit trail to document the completion of the review and update actions. DoD has defined the frequency as annually or more frequently upon changes to situational awareness of threats or vulnerabilities.	The organization conducting the inspection/assessment reviews the audit trail showing reviews and updates to the list of audited events to ensure that the list is reviewed and updated annually or more frequently upon changes to situational awareness of threats or vulnerabilities. DoD has defined the frequency as annually or more frequently upon changes to situational awareness of threats or vulnerabilities.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-3	CCI-000130	The information system generates audit records containing information that establishes what type of event occurred.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes what type of event occurred For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 130.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes what type of event occurred. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes what type of event occurred. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 130.	LOW		X						3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-3	CCI-000131	The information system generates audit records containing information that establishes when an event occurred.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes when an event occurred For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 131.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes when an event occurred. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes when an event occurred. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 131.	LOW		X						3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-3	CCI-000132	The information system generates audit records containing information that establishes where the event occurred.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes where the event occurred For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 132.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes where the event occurred. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes where the event occurred. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 132.	LOW		X						3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-3	CCI-000133	The information system generates audit records containing information that establishes the source of the event.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes the source of the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 133.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes the source of the event. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes the source of the event. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 133.	LOW		X						3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-3	CCI-000134	The information system generates audit records containing information that establishes the outcome of the event.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes the outcome of the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 134.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes the outcome of the event. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes the outcome of the event. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 134.	LOW		X						3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-3(1)	CCI-000135	The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.	The organization being inspected/assessed configures the information system to generate audit records containing the organization defined additional, more detailed information as defined in AU-3 (1), CCI 1488 that is to be included in the audit records. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 135.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing the organization defined additional, more detailed information as defined in AU-3 (1), CCI 1488 that is to be included in the audit records. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain organization defined additional, more detailed information that is to be included in the audit records. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 135.	MOD		X		X				3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-5(a)	CCI-000139	The information system alerts designated organization-defined personnel or roles in the event of an audit processing failure.	The organization being inspected/assessed configures the information system to alert at a minimum, the SCA and ISSO in the event of an audit processing failure. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 139. DoD has defined the personnel or roles as at a minimum, the SCA and ISSO.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to alert at a minimum, the SCA and ISSO in the event of an audit processing failure. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 139. DoD has defined the personnel or roles as at a minimum, the SCA and ISSO.	LOW	X	X		X				3.5.5 Response to Audit Processing Failur...	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-5(b)	CCI-000140	The information system takes organization defined actions upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).	The organization being inspected/assessed configures the information system to take actions as defined in AU-5, CCI 1490 upon audit failure. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 140.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to take actions as defined in AU-5, CCI 1490 upon audit failure. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 140.	LOW	X	X		X				3.5.5 Response to Audit Processing Failur...	FRCS has no computers in scope	
N/A	PM-3(c)	CCI-000141	The organization ensures that information security resources are available for expenditure as planned.	The organization being inspected/assessed documents and implements a process to ensure that information security resources are available for expenditure as planned.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensure that information security resources are available for expenditure as planned.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PM-4(a)(1)	CCI-000142	The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process for plans of action and milestones for the security program. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process for plans of action and milestones for the security program. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	LOW	X		X					---	CS is not publically accessible	
N/A	AU-6(a)	CCI-000148	The organization reviews and analyzes information system audit records on an organization defined frequency for indications of organization-defined inappropriate or unusual activity.	The organization being inspected/assessed documents and implements a process to review and analyze information system audit records every seven days or more frequently if required by an alarm event or anomaly for indications of activity defined in AU-6, CCI 1862. The organization must maintain an audit trail of the reviews. DoD has defined the frequency as every seven days or more frequently if required by an alarm event or anomaly.	The organization conducting the inspection/assessment obtains and examines the documented process for audit trail reviews as well as the audit trail showing the reviews to ensure the organization being inspected/assessed reviews and analyzes information system audit records every seven days or more frequently if required by an alarm event or anomaly for indications of activity defined in AU-6, CCI 1862. DoD has defined the frequency as every seven days or more frequently if required by an alarm event or anomaly.	LOW			X					---	CS is not publically accessible	
N/A	AU-6(b)	CCI-000149	The organization reports any findings to organization-defined personnel or roles for indications of organization-defined inappropriate or unusual activity.	The organization being inspected/assessed documents and implements a process for reporting any findings of inappropriate or unusual activity as defined in AU-6, CCI 1862 to at a minimum, the ISSO and ISSM. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines the documented process for reporting findings as well as a sampling of historical reports to ensure the organization being inspected/assessed reports any findings of inappropriate or unusual activity as defined in AU-6, CCI 1862 to at a minimum, the ISSO and ISSM. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	LOW			X					---	CS is not publically accessible	
N/A	AU-6(a)	CCI-000151	The organization defines the frequency for the review and analysis of information system audit records for organization-defined inappropriate or unusual activity.	DoD has defined the frequency as every seven days or more frequently if required by an alarm event or anomaly.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every seven days or more frequently if required by an alarm event or anomaly.	LOW				X				---	CS is not publically accessible	
N/A	AU-6(3)	CCI-000153	The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	The organization being inspected/assessed documents and implements a process to analyze and correlate audit records across different repositories to gain organization-wide situational awareness. The organization must maintain a record of the analysis.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of analysis to ensure the organization being inspected/assessed analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	MOD			X					---	CS is not publically accessible	
N/A	AU-6(4)	CCI-000154	The information system provides the capability to centrally review and analyze audit records from multiple components within the system.	The organization being inspected/assessed configures the information system to provide a capability to centrally review and analyze audit records from multiple components within the system. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 154.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to provide a capability to centrally review and analyze audit records from multiple components within the system. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 154.	MOD		X						3.5.3.4 Audit Reduction and Report Generati...	FRCS does not have Auditing Front End Software in scope	
N/A	AU-7(1)	CCI-000158	The information system provides the capability to process audit records for events of interest based on organization-defined audit fields within audit records.	The organization being inspected/assessed must employ information systems that provide the capability to process audit records for events of interest based on audit fields within audit records defined in AU-7 (1), CCI 1883. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 158.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed employs information systems that provides the capability to process audit records for events of interest based on audit fields within audit records as defined in AU-7 (1), CCI 1883. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 158.	MOD	X	X		X					3.5.3.4 Audit Reduction and Report Generati...	FRCS does not have Auditing Front End Software in scope	
N/A	AU-8(a)	CCI-000159	The information system uses internal system clocks to generate time stamps for audit records.	The organization being inspected/assessed configures the information system to use internal system clocks to generate time stamps for audit records. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 159.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to use internal system clocks to generate time stamps for audit records. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 159.	LOW		X						3.5.2 Audit Time Stamps		CCI requirements are met within subparagraph "Audit Time Stamps" of UFGS 25 05 11.
N/A	AU-8(1)	CCI-000161	The organization defines the frequency for the synchronization of internal information system clocks.	DoD has defined the frequency as every 24 hours for networked systems.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 24 hours for networked systems.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-9	CCI-000162	The information system protects audit information from unauthorized access.	The organization being inspected/assessed configures the information system to disallow unauthorized access to audit information. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 162.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized access to audit information. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 162.	LOW	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-9	CCI-000163	The information system protects audit information from unauthorized modification.	The organization being inspected/assessed configures the information system to disallow unauthorized modification of audit information. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 163.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized modification of audit information. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 163.	LOW	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-9	CCI-000164	The information system protects audit information from unauthorized deletion.	The organization being inspected/assessed configures the information system to disallow unauthorized deletion of audit information. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 164.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized deletion of audit information. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 164.	LOW	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-10	CCI-000166	The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.	The organization being inspected/assessed configures the information system to protect against an individual falsely denying having performed actions to be covered by non-repudiation defined in DoDI 8520.02 and DoDI 8520.03. DoDI 8520.02 and DoDI 8520.03 meet the DoD requirement to define the actions to be covered by non-repudiation. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 166.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed protects against an individual falsely denying having performed actions to be covered by non-repudiation defined in DoDI 8520.02 and DoDI 8520.03. DoDI 8520.02 and DoDI 8520.03 meet the DoD requirement to define the actions to be covered by non-repudiation. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 166.	MOD		X						3.5.1 Audit Events, Content of Audit Reco…		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-11	CCI-000167	The organization retains audit records for an organization defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	The organization being inspected/assessed will take action to ensure it retains audit records for 5 years for SAMI; otherwise for at least 1 year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. DoD has defined the time period as 5 years for SAMI; otherwise for at least 1 year.	The organization conducting the inspection/assessment reviews the information system audit records and any other relevant documents or records to ensure the organization being inspected/assessed retains its audit records for 5 years for SAMI; otherwise for at least 1 year. DoD has defined the time period as 5 years for SAMI; otherwise for at least 1 year.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-11	CCI-000168	The organization defines the time period for retention of audit records which is consistent with its records retention policy, to provide support for after-the-fact investigations of security incidents, and meet regulatory and organizational information retention requirements.	DoD has defined the time period as 5 years for SAMI; otherwise for at least 1 year.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 5 years for SAMI; otherwise for at least 1 year.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-12(a)	CCI-000169	The information system provides audit record generation capability for the auditable events defined in AU-2 a at organization defined information system components.	The organization being inspected/assessed acquires or designs all information system and network components that provide audit record generation capability for the auditable events defined in AU-2 a. DoD has defined the information system components as all information system and network components.	The organization conducting the inspection/assessment examines the information system to ensure that all information system and network components provide audit record generation capability for the auditable events defined in AU-2 a. DoD has defined the information system components as all information system and network components.	LOW		X						3.5.1 Audit Events, Content of Audit Reco…		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	PM-4(a)(2)	CCI-000170	The organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to maintain a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-12(b)	CCI-000171	The information system allows organization-defined personnel or roles to select which auditable events are to be audited by specific components of the information system.	The organization being inspected/assessed configures the information system to ensure that only the ISSM or individuals appointed by the ISSM select which auditable events are to be audited by specific components of the information system. DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	The organization conducting the inspection/assessment examines a sampling of information system components and confirms that the individuals capable of selecting auditable events are the ISSM or individuals appointed by the ISSM. DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	LOW		X		X				3.5.1 Audit Events, Content of Audit Reco…		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-12(c)	CCI-000172	The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.	The organization being inspected/assessed configures the information system to generate audit records for the events defined in AU-2 d with the content defined in AU-3. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 172.	The organization conducting the inspection/assessment examines the information system to ensure that the system generates audit records for the events defined in AU-2 d with the content defined in AU-3. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 172.	LOW		X						3.5.1 Audit Events, Content of Audit Reco…		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-12(1)	CCI-000173	The organization defines the level of tolerance for relationship between time stamps of individual records in the audit trail that will be used for correlation.	The organization being inspected/assessed will define and document their level of tolerance for variation in the time stamps applied to the audit data generated by the organization's information systems. DoD has determined that the level of tolerance is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment reviews the organization's audit and accountability policy and procedures addressing audit record generation and retention; information system audit configuration settings and associated documentation; information system audit records; and any other relevant documents or records. The objective is to validate the organization has defined and documented its level of tolerance for variation in the time stamps applied to the audit data generated by the organization's information systems. DoD has determined that the level of tolerance is not appropriate to define at the Enterprise level.	MOD		X	X					3.5.3.4 Audit Reduction and Report Generati...	FRCS does not have Auditing Front End Software in scope	
N/A	AU-12(1)	CCI-000174	The information system compiles audit records from organization-defined information system components into a system-wide (logical or physical) audit trail that is time-correlated to within organization defined level of tolerance for relationship between time stamps of individual records in the audit trail.	The organization being inspected/assessed configures the information system to compile audit records from information system components defined in AU-12 (1), CCI 1577 into a system-wide (logical or physical) audit trail that is time-correlated to within the level of tolerance defined in AU-12 (1), CCI-000173 for relationship between time stamps of individual records in the audit trail. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 174.	The organization conducting the inspection/assessment examines the information system to ensure the information system is configured to compile audit records from information system components defined in AU-12 (1), CCI 1577 into a system-wide (logical or physical) audit trail that is time-correlated to within the level of tolerance defined in AU-12 (1), CCI-000173 for relationship between time stamps of individual records in the audit trail. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 174.	MOD		X						3.5.3.4 Audit Reduction and Report Generati...	FRCS does not have Auditing Front End Software in scope	
N/A	IA-5(b)	CCI-000176	The organization manages information system authenticators by establishing initial authenticator content for authenticators defined by the organization.	The organization being inspected/assessed defines and documents procedures for setting initial authenticator content.	The organization conducting the inspection/assessment obtains and examines the documented procedures for setting initial authenticator content to ensure they have been defined.	LOW		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(f)	CCI-000179	The organization manages information system authenticators by establishing minimum lifetime restrictions for authenticators.	The organization being inspected/assessed defines and documents minimum lifetime restrictions for authenticators.	The organization conducting the inspection/assessment obtains and examines the documented minimum lifetime restrictions for authenticators to ensure they have been defined.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(f)	CCI-000180	The organization manages information system authenticators by establishing maximum lifetime restrictions for authenticators.	Per IA-5, CCI 1610, DoD has established the maximum lifetime restrictions for authenticators as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	Per IA-5, CCI 1610, DoD has established the maximum lifetime restrictions for authenticators as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(f)	CCI-000181	The organization manages information system authenticators by establishing reuse conditions for authenticators.	The organization being inspected/assessed defines and documents the reuse conditions for authenticators.	The organization conducting the inspection/assessment obtains and examines the documented reuse conditions for authenticators to ensure they have been defined.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(g)	CCI-000182	The organization manages information system authenticators by changing/refreshing authenticators in accordance with the organization defined time period by authenticator type.	The organization being inspected/assessed documents and implements procedures for changing/refreshing authenticators in the following time periods: CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years. DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	The organization conducting the inspection/assessment obtains and examines the documented procedures for authenticator change/refresh to ensure the procedures are defined. The organization conducting the inspection/assessment obtains and examines a sampling of authenticator age data to ensure that authenticators are changed or refreshed in the following time periods: CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years. DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	LOW		X	X	X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "USER IDENTIFICATION AND AUTHENTICATION"
N/A	IA-5(h)	CCI-000183	The organization manages information system authenticators by protecting authenticator content from unauthorized disclosure.	The organization being inspected/assessed documents and implements procedures to protect authenticator content from unauthorized disclosure.	The organization conducting the inspection/assessment obtains and examines the documented procedures to protect authenticator content from unauthorized disclosure to ensure the procedures are defined.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(2)(a)	CCI-000185	The information system, for PKI-based authentication validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.	The information system performing hardware token-based authentication must be configured to validate DoD-approved PKI credentials in accordance with RFC 5280. The information system must be configured to perform a revocation check as part of the certificate validation process. Revocation checking may be performed using certificate revocation lists (CRLs) published by the issuing PKI or Online Certificate Status Protocol (OCSP) services. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 185.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to validate DoD-approved PKI credentials in accordance with RFC 5280. The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to perform a revocation check as part of the certificate validation process. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 185.	MOD	X	X		X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(2)(b)	CCI-000186	The information system, for PKI-based authentication enforces authorized access to the corresponding private key.	Information systems must not have access to users' private keys. The cryptographic container in which the private keys are stored (e.g. smart card or software module) implements access controls and protections to ensure that only the authorized user can activate the private key. DoD users agree to protect their PKI credentials in accordance with the DD-2842 agreement that is executed for each credential. They are reminded of these responsibilities in annual IA training. The private key identifying the information system must be stored in a cryptographic container that is FIPS 140-2 validated. Only authorized information system operators should have access to activation data (e.g. password or PIN) for the private key.	The organization conducting the inspection/assessment examines the information system to ensure the information system does not contain any users' private keys. The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to store its own private key in a FIPS 140-2 validated cryptographic module.	MOD	X	X						---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-5(2)(c)	CCI-000187	The information system, for PKI-based authentication, maps the authenticated identity to the account of the individual or group.	The information system performing PKI-based authentication must be configured to map the authenticated PKI credential to a corresponding network or information system account or role in accordance with DoDI 8520.03. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 187.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to map authenticated PKI credentials to corresponding network or information system accounts or roles in accordance with DoDI 8520.03. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 187.	MOD	X	X						---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-5(1)(a)	CCI-000192	The information system enforces password complexity by the minimum number of upper case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of upper case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 192.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of upper case characters used. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 192.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT…		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(a)	CCI-000193	The information system enforces password complexity by the minimum number of lower case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of lower case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 193.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of lower case characters used. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 193.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT…		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(a)	CCI-000194	The information system enforces password complexity by the minimum number of numeric characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of numeric characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 194.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of numeric characters used. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 194.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT…		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(b)	CCI-000195	The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.	The organization being inspected/assessed configures the information system to enforce that at least 50% of the minimum password length is changed. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 195. DoD has defined the minimum number of characters as 50% of the minimum password length.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce that at least 50% of the minimum password length is changed. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 195. DoD has defined the minimum number of characters as 50% of the minimum password length.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT…		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(c)	CCI-000196	The information system, for password-based authentication, stores only cryptographically-protected passwords.	The organization being inspected/assessed configures the information system to store only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 196.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to store only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 196.	LOW	X	X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT…		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(c)	CCI-000197	The information system, for password-based authentication, transmits only cryptographically-protected passwords.	The organization being inspected/assessed configures the information system to transmit only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 197.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to transmit only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 197.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT…		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(d)	CCI-000198	The information system enforces minimum password lifetime restrictions.	The organization being inspected/assessed configures the information system to enforce minimum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 198.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce minimum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 198.	LOW		X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT…		CCI's requirement is addressed within paragraph "user identification and authentication"

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-5(1)(d)	CCI-000199	The information system enforces maximum password lifetime restrictions.	The organization being inspected/assessed configures the information system to enforce maximum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 199.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce maximum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 199.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(1)(e)	CCI-000200	The information system prohibits password reuse for the organization defined number of generations.	The organization being inspected/assessed configures the information system to prohibit reuse for a minimum of 5 generations. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 200. DoD has defined the number of generations as a minimum of 5.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prohibit reuse for a minimum of 5 generations. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 200. DoD has defined the number of generations as a minimum of 5.	LOW	X	X	X	X				3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-5(8)	CCI-000204	The organization defines the security safeguards required to manage the risk of compromise due to individuals having accounts on multiple information systems.	DoD has defined the security safeguards as policies and user training including advising users not to use the same password for any of the following: Domains of differing classification levels. More than one domain of a classification level (e.g., internal agency network and Intelink). More than one privilege level (e.g., user, administrator).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security safeguards as policies and user training including advising users not to use the same password for any of the following: Domains of differing classification levels. More than one domain of a classification level (e.g., internal agency network and Intelink). More than one privilege level (e.g., user, administrator).	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-5(1)(a)	CCI-000205	The information system enforces minimum password length.	The organization being inspected/assessed configures the information system to enforce minimum password length. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 205.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce minimum password length. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 205.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI's requirement is addressed within paragraph "user identification and authentication"
N/A	IA-6	CCI-000206	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	The organization being inspected/assessed configures the information system to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 206.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 206.	LOW	X	X		X				3.4.6 Authenticator Feedback		CCI requirements are met within subparagraph "Authenticator Feedback" of UFGS 25 05 11.
N/A	PM-5	CCI-000207	The organization develops and maintains an inventory of its information systems.	DITPR is the inventory for all DoD information systems. The organization being inspected/assessed must register and maintain their information systems in DITPR.	DITPR is the inventory for all DoD information systems. The organization conducting the inspection/assessment obtains and examines the inventory of information systems via DITPR to ensure the organization being inspected/assessed registers their information systems in DITPR.	LOW		X	X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-6	CCI-000209	The organization develops the results of information security measures of performance.	The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance.	The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance. DoD organizations are automatically compliant with this CCI as they are covered at the DoD level by FISMA.	LOW					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-6	CCI-000210	The organization monitors the results of information security measures of performance.	The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance.	The Federal Information Systems Management Act (FISMA) meets the DoD requirements for information security performance measures of performance. DoD organizations are automatically compliant with this CCI as they are covered at the DoD level by FISMA.	LOW					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-6	CCI-000211	The organization reports on the results of information security measures of performance.	The organization being inspected/assessed reports the results of information security measures of performance IAW FISMA reporting guidance.	The organization conducting the inspection/assessment obtains and examines FISMA reporting documentation.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-7	CCI-000212	The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	The GIG IA Architecture meets the DoD requirements for enterprise architecture. DoD components are automatically compliant with this CCI as they covered at the DoD level.	The GIG IA Architecture meets the DoD requirements for enterprise architecture. DoD components are automatically compliant with this CCI as they covered at the DoD level.	LOW			X	X	X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-3	CCI-000213	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	The organization being inspected/assessed configures the information system to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 213.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 213.	LOW		X						3.3.1 User Accounts		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts" within Part 3
N/A	PM-8	CCI-000216	The organization develops and documents a critical infrastructure and key resource protection plan that addresses information security issues.	DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan. DoD components are automatically compliant with this CCI as they are covered by the DoD level, DoDD 3020.40.	DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan. DoD components are automatically compliant with this CCI as they are covered by the DoD level, DoDD 3020.40.	LOW						X	A LOW Control System doesn't deal with critical infrastructure.	---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(3)	CCI-000217	The organization defines a time period after which inactive accounts are automatically disabled.	DoD has defined the time period as 35 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 35 days.	MOD		X		X	X			3.3.1 User Accounts	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-6	CCI-000225	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	The organization being inspected/assessed documents and implements the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	The organization conducting the inspection/assessment obtains and examines the documented processes to ensure that the organization being inspected/assessed implements the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	MOD	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-9(a)	CCI-000227	The organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems.	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by the DoD Risk Management Framework (DoDI 8510.01).	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by DoD Risk Management Framework (DoDI 8510.01).	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-9(b)	CCI-000228	The organization implements a comprehensive strategy to manage risk to organization operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems consistently across the organization.	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by the DoD Risk Management Framework (DoDI 8510.01).	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by DoD Risk Management Framework (DoDI 8510.01).	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-10(a)	CCI-000229	The organization documents the security state of organizational information systems and the environments in which those systems operate through security authorization processes.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-10(a)	CCI-000230	The organization tracks the security state of organizational information systems and the environments in which those systems operate through security authorization processes.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	LOW					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-10(a)	CCI-000231	The organization reports the security state of organizational information systems and the environments in which those systems operate through security authorization processes.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to manage the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AC-14(b)	CCI-000232	The organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.	The organization being inspected/assessed documents supporting rationale in the security plan for the actions defined in AC-14, CCI 61 to not require identification and authentication.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed documents the supporting rationale for the actions defined in AC-14, CCI 61 to not require identification and authentication.	LOW		X						3.3.5 Permitted Actions Without Identific...		CCI requirements are addressed within subparagraph "Permitted Actions Without Identification or Authentication" of UFGS 25 05 11.
N/A	PM-10(b)	CCI-000233	The organization designates individuals to fulfill specific roles and responsibilities within the organizational risk management process.	DoDI 8510.01 meets the DoD requirement to designate roles and responsibilities for the risk management process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to designate roles and responsibilities for the risk management process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-10(c)	CCI-000234	The organization fully integrates the security authorization processes into an organization-wide risk management program.	DoDI 8510.01 meets the DoD requirement to fully integrate the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to fully integrate the security authorization process. DoD components are automatically compliant with this CCI because they are covered at the DoD level, DoDI 8510.01.	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-11(a)	CCI-000235	The organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	DoDI 8510.01 meets the DoD requirement to define mission/business processes. DoD components are automatically complaint with this CCI as they are covered at the DoD level, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement to define mission/business processes. DoD components are automatically complaint with this CCI as they are covered at the DoD level, DoDI 8510.01.	LOW					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-11(b)	CCI-000236	The organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs are obtained.	The organization being inspected/asssessed determines information protection needs IAW CNSSI 1253 and as identified in RA-2.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the security categorization has been documented IAW CNSSI 1253.	LOW	X	X	X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CA-1(b)(1)	CCI-000238	The organization defines the frequency to review and update the current security assessment and authorization policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.	LOW					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CA-1(a)(1)	CCI-000239	The organization develops and documents a security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01.	LOW			X		X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CA-1(a)(1)	CCI-000240	The organization disseminates to organization-defined personnel or roles a security assessment and authorization policy.	DoD disseminates DoDI 8510.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/ins1.html	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01.	LOW			X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CA-1(b)(1)	CCI-000241	The organization reviews and updates the current security assessment and authorization policy in accordance with organization-defined frequency.	DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01.	DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01.	LOW					X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CA-1(a)(2)	CCI-000242	The organization develops and documents procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.	The organization being inspected/assessed develops and documents, IAW DoDI 8510.01, procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.	The organization conducting the inspection/assessment obtains and examines the procedures to ensure the organization being inspected/assessedd evelops and documents procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls IAW DoDI 8510.01	LOW			X						---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CA-1(a)(2)	CCI-000243	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.	The organization being inspected/assessed will require all personnel to register at the DTIC website to receive update notifications to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls. DoD has defined the personnel or roles as all personnel.	The organization conducting the inspection/assessment obtains and examines the AUP (Acceptable Use Policy), appointment orders, or written policy requiring that all personnel register at the DTIC website to receive update notifications. DoD has defined the personnel or roles as all personnel.	LOW			X						---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CA-1(b)(2)	CCI-000244	The organization reviews and updates the current security assessment and authorization procedures in accordance with organization-defined frequency.	The organization being inspected/assessed reviews and updates, IAW DoDI 8510.01, the current security assessment and authorization procedures annually. The organization must maintain an audit trail of review and update activity. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of review and update activity to ensure the organization being inspected/assessed reviews and updates, IAW DoDI 8510.01, the current security assessment and authorization procedures annually.	LOW			X						---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CA-2(a)	CCI-000245	The organization develops a security assessment plan for the information system and its environment of operation. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will document these security assessment plan requirements as part of the DoD approved Security Plan. Security plan templates are provided through eMASS and the Knowledge Service. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment obtains and examines the Security Plan to validate *security assessment blocks* are complete.	LOW			X						---	CS is not publically accessible	
N/A	CA-2(a)(1)	CCI-000246	The organization's security assessment plan describes the security controls and control enhancements under assessment. IG&VP WG Note *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will ensure the Security Plan identifies the security controls and control enhancements under assessment. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment obtains the security assessment plan to verify the plan identifies the security controls and those control enhancements under assessment.	LOW			X						---	CS is not publically accessible	
N/A	CA-2(a)(2)	CCI-000247	The organization's security assessment plan describes assessment procedures to be used to determine security control effectiveness. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The implementation guidance and validation procedures posted on the Knowledge Service constitutes assessment procedures for DoD. If organizations being inspected/assessed use assessment procedures other than those posted on the Knowledge Service, those procedures must be documented. *Comment* The items required within this CCI are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	DoD components are automatically compliant with this CCI if using the implementation guidance and validation procedures on the Knowledge Service. If the organization being inspected/assessed is using alternative implementation guidance and validation procedures, the organization conducting the inspection/assessment will obtain and examine those procedures.	LOW					X				---	CS is not publically accessible	
N/A	CA-2(a)(3)	CCI-000248	The organization's security assessment plan describes assessment environment. *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will provide a description of the authorization boundary in their Security Plan. Authorization boundary can be described via one or more of the following: network diagrams, data flow diagrams, system design documents, or a list of information system components. Authorization boundary as defined in CNSSI 4009. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment obtains and examines the organization's authorization boundary. Authorization boundary can be described via one or more of the following: network diagrams, data flow diagrams, system design documents, or a list of information system components.	LOW			X						---	CS is not publically accessible	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CA-2(b)	CCI-000251	The organization assesses, on an organization-defined frequency, the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	In accordance with DoD's published guidance, the organization being inspected/assessed will utilize the implementation guidance and validation procedures published on the Knowledge Service to evaluate the implementation status of the applicable controls. DoD has defined the frequency as annually for technical controls, annually for a portion of management and operational controls, such that all are reviewed in a 3 year period, except for those requiring more frequent review as defined in other site or overarching policy. (NOTE: Technical, Management and Operational is IAW NIST SP 800-53 Table 1-1). *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	See CA-2 c "The organization conducting the inspection/assessment obtains and examines the security assessment report to verify that it includes the compliance/non-compliance status of all controls and specific deficiencies for all non-compliant controls."	LOW			X					---	CS is not publically accessible	
N/A	CA-2(b)	CCI-000252	The organization defines the frequency on which the security controls in the information system and its environment of operation are assessed. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	DoD has defined the frequency as annually for technical controls, annually for a portion of management and operation controls such that all are reviewed in a 3 year period except for those requiring more frequent review as defined in other site or overarching policy. NOTE: Technical, Management and Operational is IAW NIST SP 800-53 Table 1-1. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually for technical controls, annually for a portion of management and operation controls such that all are reviewed in a 3 year period except for those requiring more frequent review as defined in other site or overarching policy. NOTE: Technical, Management and Operational is IAW NIST SP 800-53 Table 1-1.	LOW					X			---	CS is not publically accessible	
N/A	CA-2(c)	CCI-000253	The organization produces a security assessment report that documents the results of the assessment against the information system and its environment of operation. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will develop a SAR that includes the compliance/non-compliance status of all controls and specific deficiencies for all non-compliant controls using the template available on the Knowledge Service. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment obtains and examines the SAR to verify that it includes the compliance/non-compliance status of all controls and specific deficiencies for all non-compliant controls.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-2(d)	CCI-000254	The organization provides the results of the security control assessment against information system and its environment of operation to organization-defined individuals or roles. IG&VP WG Note: *For DoD, the security assessment plan information is included in the Security Plan and the security assessment report and is not a separate document/artifact.*	The organization being inspected/assessed will provide the SAR to at a minimum, the ISSO and ISSM. DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM. *Comment* The items required within this control are being split into the security plan and security assessment report to eliminate creation of an additional artifact.	The organization conducting the inspection/assessment interviews at a minimum, the ISSO and ISSM to ensure the SAR has been received. DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-2(1)	CCI-000255	The organization employs assessors or assessment teams with organization-defined level of independence to conduct security control assessments of organizational information systems.	The organization being inspected/assessed will employ assessors and assessor teams with the level of independence defined in CA-2 (1), CCI 2064 to conduct security control assessments of organizational information systems.	The organization conducting the inspection/assessment obtains and examines the level of independence defined in CA-2 (1), CCI 2064 to ensure that they, as the assessor, meet the required level of independence.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-3(a)	CCI-000257	The organization authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements.	The organization being inspected/assessed will develop and certify, by appropriate signatures (e.g. AO, network managers), Interconnection Security Agreements (e.g., MOU, MOA, SLA) authorizing the connection of its information systems to other information systems. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	The organization conducting the inspection/assessment obtains and examines documentation of the Interconnection Security Agreements to include appropriate signatures. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-3(b)	CCI-000258	The organization documents, for each interconnection, the interface characteristics.	The organization being inspected/assessed will document the interface characteristics for each interconnection. Use of external reporting databases for these characteristics when tied to the specific interconnection is acceptable (e.g., ports, protocols, and services). Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	The organization conducting the inspection/assessment obtains and examines interconnection security agreement documentation. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	LOW	X	X	X					1.9.2 Cybersecurity Interconnection Sched... 1.11 CYBERSECURITY DURING CONSTRUCTION		Cybersecurity requirements will be documented by the contractor in the Cybersecurity Interconnection Schedule and is addressed withing Sub-Paragraphs "Cybersecurity During Construction" and "Cybersecurity Interconnection Schedule" within Part 1.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CA-3(b)	CCI-000259	The organization documents, for each interconnection, the security requirements.	The organization being inspected/assessed will, for each interconnection, identify and document any additional security controls to be implemented to protect the confidentiality, integrity, and availability of the connected systems and the data passing between them. Controls should be appropriate for the systems to be connected and the environment in which the interconnection will operate. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	The organization conducting the inspection/assessment obtains and examines interconnection security agreement documentation, specifically looking at any additional security controls identified for implementation. Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-3(b)	CCI-000260	The organization documents, for each interconnection, the nature of the information communicated.	The organization being inspected/assessed will document in the interconnection security agreement the type of information being transferred/transmitted. Characteristics will include but are not limited to: classification, information type (e.g. PII, HIPAA, FOUO, financial data, etc.) Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	The organization conducting the inspection/assessment obtains and examines the interconnection security agreement documentation, specifically to identify the type of information being transferred/transmitted. Characteristics will include but are not limited to: classification, information type (e.g. PII, HIPAA, FOUO, financial data, etc.) Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-5(a)	CCI-000264	The organization develops a plan of action and milestones for the information system to document the organizations planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.	The organization being inspected/assessed will develop a security POA&M in accordance with DoDI 8510.01 Enclosure 6. POA&M templates are available on the Knowledge Service.	The organization conducting the inspection/assessment obtains and examines the security POA&M for compliance with DoDI 8510.01.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-5(b)	CCI-000265	The organization defines the frequency to update existing plan of action and milestones for the information system.	DoD has defined the frequency as at least every 90 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least every 90 days.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CA-5(b)	CCI-000266	The organization updates, on an organization-defined frequency, existing plan of action and milestones based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	The organization being inspected/assessed will update the POA&M at least every 90 days. The updates are to be based upon the assessment of the identified vulnerabilities and weaknesses, prioritization of the vulnerabilities and weaknesses, progress being made in addressing and resolving the security weaknesses and vulnerabilities found in programs and systems, and continuous monitoring activities. DoD has defined the frequency as at least every 90 days.	The organization conducting the inspection/assessment obtains and examines current POA&M. The objective is to validate the organization is providing updates to the POA&M at least every 90 days. Review of POA&M without change must be documented (i.e., adding review date to the POA&M header information). DoD has defined the frequency as at least every 90 days.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-6(a)	CCI-000270	The organization assigns a senior-level executive or manager as the authorizing official for the information system.	The organization being inspected/assessed will assign a senior-level executive or manager as the official role, and the responsibility, for authorizing the information system(s). Assignment must be in writing and IAW with DoDI 8510.01 (i.e. Appointment memorandum).	The organization conducting the inspection/assessment obtains and examines the written appointment memorandum.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CA-6(b)	CCI-000271	The organization ensures the authorizing official authorizes the information system for processing before commencing operations.	The organization being inspected/assessed will ensure that an authorization document (e.g. authorization to operate (ATO), interim authorization to operate (IATO)) has been issued by the authorizing official (AO) prior to placing the information system into an operational status.	The organization conducting the inspection/assessment obtains and examines the authorization document to ensure the information system is authorized prior to being placed into operational status.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-6(c)	CCI-000272	The organization updates the security authorization on an organization-defined frequency.	The organization being inspected/assessed updates the security authorization at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates. DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.	The organization conducting the inspection/assessment obtains and examines the security authorization documentation to confirm the security authorization has been updated within the last three years, when there was a significant change to the system, or if there was a change to the environment in which the system operates. DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-6(c)	CCI-000273	The organization defines the frequency of updating the security authorization.	DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CA-7	CCI-000274	The organization develops a continuous monitoring strategy.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-7(c)	CCI-000279	The organization implements a continuous monitoring program that includes ongoing security control assessments in accordance with the organizational continuous monitoring strategy.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CA-7(g)	CCI-000280	The organization implements a continuous monitoring program that includes reporting the security status of organization and the information system to organization-defined personnel or roles on an organization-defined frequency.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-7(g)	CCI-000281	The organization defines the frequency to report the security status of organization and the information system to organization-defined personnel or roles.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-7(1)	CCI-000282	The organization employs assessors or assessment teams with organization-defined level of independence to monitor the security controls in the information system on an ongoing basis.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(b)(1)	CCI-000286	The organization defines a frequency to review and update the configuration management policies.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-1(a)(1)	CCI-000287	The organization develops and documents a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization being inspected/assessed develops and documents a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization conducting the inspection/assessment obtains and examines the configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(b)(1)	CCI-000289	The organization reviews and updates, on an organization defined frequency, the configuration management policy.	The organization being inspected/assessed reviews and updates, annually, the configuration management policy. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the configuration management policy to ensure annual review and necessary updates are occurring. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(a)(2)	CCI-000290	The organization develops and documents procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(b)(2)	CCI-000292	The organization reviews and updates, on an organization defined frequency, the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization being inspected/assessed reviews and updates, annually, the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls to ensure annual review and necessary updates are occurring. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-2	CCI-000293	The organization develops and documents a current baseline configuration of the information system.	The organization being inspected/assessed develops and documents a current baseline configuration of the information system.	The organization conducting the inspection/assessment obtains and examines the documented baseline configuration.	LOW		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-2	CCI-000295	The organization maintains under configuration control, a current baseline configuration of the information system.	The organization being inspected/assessed maintains a current baseline configuration of the information system.	The organization conducting the inspection/assessment obtains and examines the current baseline to ensure the current configuration matches the current documented baseline.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-2(1)(a)	CCI-000296	The organization reviews and updates the baseline configuration of the information system at an organization-defined frequency.	The organization being inspected/assessed reviews and updates the baseline configuration of the information system annually. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines documentation of organizational reviews and update actions for the baseline configuration to ensure annual review and necessary updates are occurring. DoD has defined the frequency as annually.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-2(1)(b)	CCI-000297	The organization reviews and updates the baseline configuration of the information system when required due to organization-defined circumstances.	The organization being inspected/assessed reviews and updates the baseline configuration of the information system when required due to baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber attacks. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the circumstances as baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber attacks.	The organization conducting the inspection/assessment obtains and examines documentation of organizational reviews and update actions for the baseline configuration of the information system when required due to baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber attacks to ensure review and necessary updates are occurring. DoD has defined the circumstances as baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber attacks.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-2(1)(c)	CCI-000298	The organization reviews and updates the baseline configuration of the information system as an integral part of information system component installations.	The organization being inspected/assessed reviews and updates the baseline configuration of the information system as an integral part of information system component installations. The organization must document each occurrence of the reviews and update actions as an audit trail.	The organization conducting the inspection/assessment obtains and examines documentation of organizational reviews and update actions for the baseline configuration of the information system as an integral part of information system component installations to ensure review and necessary updates are occurring.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-2(1)(c)	CCI-000299	The organization reviews and updates the baseline configuration of the information system as an integral part of information system component upgrades.	The organization being inspected/assessed reviews and updates the baseline configuration of the information system as an integral part of information system component upgrades. The organization must document each occurrence of the reviews and update actions as an audit trail.	The organization conducting the inspection/assessment obtains and examines documentation of organizational reviews and update actions for the baseline configuration of the information system as an integral part of information system component upgrades to ensure review and necessary updates are occurring.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-2(3)	CCI-000304	The organization retains organization-defined previous versions of baseline configurations of the information system to support rollback.	The organization being inspected/assessed retains the previous approved baseline configuration of IS components for a minimum of 3 months and documents baseline configuration to support rollback. The goal is to verify that the IS can roll back components to previous versions. DoD has defined the previous versions as the previous approved baseline configuration of IS components for a minimum of 3 months.	The organization conducting the inspection/assessment obtains and examines the documentation of the previous version of the baseline configuration to determine if all IS components necessary for rollback are retained. DoD has defined the previous versions as the previous approved baseline configuration of IS components for a minimum of 3 months.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-3(a)	CCI-000313	The organization determines the types of changes to the information system that are configuration controlled.	The organization being inspected/assessed determines the types of changes to the information system that are to be configuration controlled. This action will be implemented by the CCB as defined in CM-3, CCI 1586.	The organization conducting the inspection/assessment obtains and examines the configuration management policy and plan to ensure the organization identifies the types of changes to the information system that are configuration controlled.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-3(b)	CCI-000314	The organization approves or disapproves configuration controlled changes to the information system with explicit consideration for security impact analysis.	The organization being inspected/assessed approves or disapproves configuration controlled changes to the information system with explicit consideration for security impact analysis. The organization must maintain an audit trail of approval/disapproval of configuration controlled changes. This action will be implemented by the CCB as defined in CM-3, CCI 1586.	The organization conducting the inspection/assessment obtains and examines the audit trail of the approval/disapproval of configuration controlled changes to ensure a security impact analysis was conducted.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-3(e)	CCI-000316	The organization retains records of configuration-controlled changes to the information system for an organization-defined time period.	The organization being inspected/assessed retains records of all configuration-controlled changes to the information system, as a result of CM-3, CCI 1819, for a time period defined by the organization's CCB. DoD has defined the time period as a time period defined by the organization's CCB.	The organization conducting the inspection/assessment obtains and examines the records of all configuration-controlled changes to the information system to ensure the organization being inspected/assessed retains the records of all configuration controlled changes for a time period defined by the organization's CCB. DoD has defined the time period as a time period defined by the organization's CCB.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-3(f)	CCI-000318	The organization audits and reviews activities associated with configuration controlled changes to the system.	The organization being inspected/assessed audits and reviews activities associated with configuration controlled changes to the information system. The organization must maintain an audit trail to include review activities associated with configuration-controlled changes.	The organization conducting the inspection/assessment obtains and examines the audit trail documenting the review activities associated with configuration-controlled changes to the information system to ensure the organization being inspected/assessed audits and reviews activities associated with the changes.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-3(g)	CCI-000319	The organization coordinates and provides oversight for configuration change control activities through an organization defined configuration change control element (e.g., committee, board) that convenes at the organization defined frequency and/or for any organization defined configuration change conditions.	The organization being inspected/assessed coordinates and provides oversight for configuration change control activities through a configuration control board (CCB) that convenes at a frequency determined by the CCB and/or for any configuration change conditions determined by the CCB. DoD has defined the configuration change control element as a configuration control board. DoD has defined the frequency as at a frequency determined by the CCB. DoD has defined the configuration change conditions as configuration change conditions determined by the CCB.	The organization conducting the inspection/assessment obtains and examines the organization's configuration management policy and plan; document/charter establishing the organization's CCB; meeting minutes; information system change control records; and any other relevant documents or records. The objective of the review is to validate the organization is coordinating and overseeing the configuration change control activities through a CCB.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-3(g)	CCI-000320	The organization defines frequency to convene configuration change control element.	The organization being inspected/assessed defines within their CCB Charter, the frequency for configuration change control review. DoD has defined the frequency as at a frequency determined by the CCB.	The organization conducting the inspection/assessment obtains and examines the CCB Charter to ensure the frequency for configuration change control review is defined. DoD has defined the frequency as at a frequency determined by the CCB.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-3(g)	CCI-000321	The organization defines configuration change conditions that prompt the configuration change control element to convene.	The organization being inspected/assessed defines within their CCB Charter, the configuration change conditions that prompt the configuration change control element to convene. DoD has defined the configuration change conditions as configuration change conditions determined by the CCB.	The organization conducting the inspection/assessment obtains and examines the CCB Charter to ensure the configuration change conditions that prompt the configuration change control element to convene are defined. DoD has defined the configuration change conditions as configuration change conditions determined by the CCB.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-3(2)	CCI-000327	The organization tests changes to the information system before implementing the changes on the operational system.	The organization being inspected/assessed documents and implements a process to test changes to the information system before implementing the changes on the operational system. The organization must maintain an audit trail of testing activity.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of testing activity to ensure the organization being inspected/assessed tests changes to the information system before implementing the changes on the operational system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-3(2)	CCI-000328	The organization validates changes to the information system before implementing the changes on the operational system.	The organization being inspected/assessed documents and implements a process to validate changes to the information system before implementing the changes on the operational system. The organization must maintain an audit trail of validation activity.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of validation activity to ensure the organization being inspected/assessed validates changes to the information system before implementing the changes on the operational system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-3(2)	CCI-000329	The organization documents changes to the information system before implementing the changes on the operational system.	The organization being inspected/assessed documents and implements a process to document changes to the information system before implementing the changes on the operational system.	The organization conducting the inspection/assessment obtains and examines the documented process as well as documentation of changes to the information system to ensure the organization has established, published, and is complying with the requirement to document all changes to be made to its operational information system(s) prior to their implementation.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-3(4)	CCI-000332	The organization requires an information security representative to be a member of the organization-defined configuration change control element.	The organization being inspected/assessed requires an information security representative to be a member of the configuration control board. DoD has defined the configuration change control element as the configuration control board.	The organization conducting the inspection/assessment obtains and examines the membership list of the organization's configuration control board to ensure an information security representative is a member of the organization's configuration control board.	MOD			X		X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-4	CCI-000333	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	The organization being inspected/assessed analyzes changes to the information system to determine potential security impacts prior to change implementation. The organization must maintain records of analysis of changes to the information system.	The organization conducting the inspection/assessment obtains and examines the records of analyses to ensure the organization is conducting a security impact analysis of changes to the information system(s) prior to their implementation.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-5	CCI-000338	The organization defines physical access restrictions associated with changes to the information system.	The organization being inspected/assessed defines and documents in the configuration management policy, physical access restrictions associated with changes to the information system.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed defines physical access restrictions associated with changes to the information system.	MOD	X		X	X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-5	CCI-000339	The organization documents physical access restrictions associated with changes to the information system.	The organization being inspected/assessed documents, in the configuration management policy, physical access restrictions associated with changes to the information system.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed documents physical access restrictions associated with changes to the information system.	MOD	X		X	X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-5	CCI-000340	The organization approves physical access restrictions associated with changes to the information system.	The organization being inspected/assessed documents and implements a process to approve physical access restrictions associated with changes to the information system. The organization must maintain an audit trail of approvals.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of approvals to ensure the organization being inspected/assessed approves physical access restrictions associated with changes to the information system.	MOD	X		X	X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-5	CCI-000341	The organization enforces physical access restrictions associated with changes to the information system.	The organization being inspected/assessed documents and implements a process to enforce physical access restrictions associated with changes to the information system.	The organization conducting the inspection/assessment the documented process to ensure the organization being inspected/assessed enforces physical access restrictions associated with changes to the information system as documented in the configuration management policy.	MOD	X		X	X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-5	CCI-000342	The organization defines logical access restrictions associated with changes to the information system.	The organization being inspected/assessed defines and documents in the configuration management policy, logical access restrictions associated with changes to the information system.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed defines logical access restrictions associated with changes to the information system.	MOD	X		X	X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-5	CCI-000343	The organization documents logical access restrictions associated with changes to the information system.	The organization being inspected/assessed documents, in the configuration management policy, logical access restrictions associated with changes to the information system.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed documents logical access restrictions associated with changes to the information system.	MOD	X		X	X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-5	CCI-000344	The organization approves logical access restrictions associated with changes to the information system.	The organization being inspected/assessed documents and implements a process to approve logical access restrictions associated with changes to the information system. The organization must maintain an audit trail of approvals.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of approvals to ensure the organization being inspected/assessed approves logical access restrictions associated with changes to the information system.	MOD	X		X	X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-5	CCI-000345	The organization enforces logical access restrictions associated with changes to the information system.	The organization being inspected/assessed documents and implements a process to enforce logical access restrictions associated with changes to the information system. The information system must maintain an audit trail of logical access to the information system pertaining to information system changes.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the logical access audit trail to ensure the organization being inspected/assessed enforces logical access restrictions associated with changes to the information system as documented in the configuration management policy.	MOD	X		X	X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-5(2)	CCI-000348	The organization defines a frequency to conduct reviews of information system changes.	DoD has defined the frequency as every 90 days or more frequently as the organization defines for high systems AND at least annually or more frequently as the organization defines for low and moderate systems.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 90 days or more frequently as the organization defines for high systems AND at least annually or more frequently as the organization defines for low and moderate systems.	MOD			X		X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-5(2)	CCI-000349	The organization reviews information system changes per organization defined frequency to determine whether unauthorized changes have occurred.	The organization being inspected/assessed documents in the configuration management policy and implements a process to review information system changes every 90 days or more frequently as the organization defines for high systems AND at least annually or more frequently as the organization defines for low and moderate systems to determine whether unauthorized changes have occurred. The organization must maintain this review as an audit trail. DoD has defined the frequency as every 90 days or more frequently as the organization defines for high systems AND at least annually or more frequently as the organization defines for low and moderate systems.	The organization conducting the inspection/assessment obtains and examines the documented process for information system change review as well as the audit trail of reviews to ensure the organization being inspected/assessed reviews IS changes every 90 days or more frequently as the organization defines for high systems AND at least annually or more frequently as the organization defines for low and moderate systems to determine whether unauthorized changes have occurred. DoD has defined the frequency as every 90 days or more frequently as the organization defines for high systems AND at least annually or more frequently as the organization defines for low and moderate systems.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-5(2)	CCI-000350	The organization reviews information system changes upon organization-defined circumstances to determine whether unauthorized changes have occurred.	The organization being inspected/assessed documents and implements a process to review the information system changes when there is an incident or when planned changes have been performed to determine whether unauthorized changes have occurred. The organization must maintain this review as an audit trail. DoD has defined the circumstances as when there is an incident or when planned changes have been performed.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reviews to ensure the organization being inspected/assessed reviews the information system changes when there is an incident or when planned changes have been performed to determine whether unauthorized changes have occurred. DoD has defined the circumstances as when there is an incident or when planned changes have been performed.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-6(a)	CCI-000363	The organization defines security configuration checklists to be used to establish and document configuration settings for the information system technology products employed.	DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.). The organization being inspected/assessed documents in the security plan, the configuration guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) which apply to their information system components.	DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.). The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed has documented the configuration guidance which apply to their information system components. The organization conducting the inspection/assessment reviews the list of documented guidance to ensure that all applicable guidance is identified given the information system components within the authorization boundary.	LOW		X						3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity requires the contractor to submit the Software and Configuration Backups and ensuring all STIGs/SRGs area applied where applicable. The contractor is responsible to for the configuration and software that are only strictly necessary for operation an maintenance of system. This design requirement is captured in Sub-Paragraph "Requirements for Lease Functionality" within Part 3.
N/A	CM-6(a)	CCI-000364	The organization establishes configuration settings for information technology products employed within the information system using organization-defined security configuration checklists.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for establishing configuration settings. DoD Components are automatically compliant with this CCI because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for establishing configuration settings. DoD Components are automatically compliant with this CCI because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	LOW		X						3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity requires the contractor to submit the Software and Configuration Backups and ensuring all STIGs/SRGs area applied where applicable. The contractor is responsible to for the configuration and software that are only strictly necessary for operation an maintenance of system. This design requirement is captured in Sub-Paragraph "Requirements for Lease Functionality" within Part 3.
N/A	CM-6(a)	CCI-000365	The organization documents configuration settings for information technology products employed within the information system using organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for documenting configuration settings. DoD Components are automatically compliant with this CCI because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for documenting configuration settings. DoD Components are automatically compliant with this CCI because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	LOW		X	X	X	X			3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity design requires the contractor to configure and document that the control system follow any applicable STIG/SRG and/or only provide essential capabilities. This design requirement is captured in Sub-Paragraph "Requirements for Lease Functionality" within Part 3.
N/A	CM-6(b)	CCI-000366	The organization implements the security configuration settings.	The organization being inspected/assessed must develop and document a process for implementing DoD security configuration or implementation guidance (e.g. STIGs, NSA configuration guides, CTOs, DTMs etc.). DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, NSA configuration guides, CTOs, DTMs etc.).	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements DoD security configuration or implementation guidance (e.g. STIGs, NSA configuration guides, CTOs, DTMs etc.). The organization conducting the inspection/assessment tests a sampling of information system components to ensure they comply with the required settings. DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, NSA configuration guides, CTOs, DTMs etc.).	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-6(c)	CCI-000367	The organization identifies any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.	The organization being inspected/assessed documents in the security plan and POA&M, if applicable, the information system components as defined in CM-6, CCI 1755 which deviate from configuration settings, and which settings as defined in CM-6, CCI 1756.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed has documented deviations from configuration settings for information system components.	LOW			X	X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-6(c)	CCI-000368	The organization documents any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.	The organization being inspected/assessed documents in the security plan and POA&M, if applicable, all configurable information system components which deviate from configuration settings, and which settings as defined in CM-6, CCI 1756. DoD has defined the information system components as all configurable information system components.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed has documented deviations from configuration settings for information system components.	LOW			X	X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-6(c)	CCI-000369	The organization approves any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.	The organization being inspected/assessed manages and approves changes to the security plan documenting deviations IAW CM-3, CCI 314. The organization must maintain an audit trail of approved changes to the security plan.	The organization conducting the inspection/assessment obtains and examines the security plan and the audit trail of approved changes to ensure the deviations are approved IAW CM-3, CCI 314.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-6(1)	CCI-000370	The organization employs automated mechanisms to centrally manage configuration settings for organization-defined information system components.	The organization being inspected/assessed identifies, documents in the configuration management policy, and implements automated mechanisms to centrally manage configuration settings.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed identifies automated mechanisms to centrally manage configuration settings. The organization being inspected/assessed may be required to demonstrate use of their identified automated mechanisms.	MOD			X						---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CM-6(1)	CCI-000371	The organization employs automated mechanisms to centrally apply configuration settings for organization-defined information system components.	The organization being inspected/assessed identifies, documents in the configuration management policy, and implements automated mechanisms to centrally apply configuration settings.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed identifies automated mechanisms to centrally apply configuration settings. The organization being inspected/assessed may be required to demonstrate use of their identified automated mechanisms.	MOD			X						---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CM-6(1)	CCI-000372	The organization employs automated mechanisms to centrally verify configuration settings for organization-defined information system components.	The organization being inspected/assessed identifies, documents in the configuration management policy, and implements automated mechanisms to centrally verify configuration settings.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed identifies automated mechanisms to centrally verify configuration settings. The organization being inspected/assessed may be required to demonstrate use of their identified automated mechanisms.	MOD			X						---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CM-7(b)	CCI-000380	The organization defines for the information system prohibited or restricted functions, ports, protocols, and/or services.	DoD has defined the information system prohibited or restricted functions, ports, protocols, and/or services as IAW DoDI 8551.01.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system prohibited or restricted functions, ports, protocols, and/or services as IAW DoDI 8551.01.	LOW		X						3.2.3 IP Control Networks 3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enriched	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-7(a)	CCI-000381	The organization configures the information system to provide only essential capabilities.	The organization being inspected/assessed documents in the security plan, essential capabilities which the information system must provide. The organization being inspected/assessed configures the information system to provide only those documented essential capabilities.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed has identified essential capabilities. The organization conducting the inspection/assessment inspects the information system to ensure that it provides only those documented essential capabilities.	LOW		X						3.2.3 IP Control Networks 3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.
N/A	CM-7(b)	CCI-000382	The organization configures the information system to prohibit or restrict the use of organization-defined functions, ports, protocols, and/or services.	The organization being inspected/assessed configures the information system to prohibit or restrict the use of functions, ports, protocols, and/or services IAW DoDI 8551.01. DoD has defined the information system prohibited or restricted functions, ports, protocols, and/or services as IAW DoDI 8551.01.	The organization conducting the inspection/assessment inspects the information system to ensure the organization being inspected/assessed prohibits or restricts the use of functions, ports, protocols, and/or services IAW DoDI 8551.01. DoD has defined the information system prohibited or restricted functions, ports, protocols, and/or services as IAW DoDI 8551.01.	LOW		X						3.2.3 IP Control Networks 3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.
N/A	CM-7(1)(a)	CCI-000384	The organization reviews the information system per organization defined frequency to identify unnecessary and nonsecure functions, ports, protocols, and services.	The organization being inspected/assessed documents and implements a process to review the information system every 30 days to identify unnecessary and nonsecure functions, ports, protocols, and services. The organization must maintain an audit trail of the reviews. DoD has defined the frequency as every 30 days.	The organization conducting the inspection/assessment obtains and examines the documented process and audit trail of reviews to ensure the organization being inspected/assessed reviews the information system every 30 days to identify unnecessary and nonsecure functions, ports, protocols, and services. DoD has defined the frequency as every 30 days.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-7(3)	CCI-000387	The organization defines registration requirements for functions, ports, protocols, and services.	DoD has defined the registration requirements as IAW DoDI 8551.01.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the registration requirements as IAW DoDI 8551.01.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-7(3)	CCI-000388	The organization ensures compliance with organization-defined registration requirements for functions, ports, protocols, and services.	The organization being inspected/assessed implements DoDI 8551.01. DoD has defined the registration requirements as IAW DoDI 8551.01.	The organization conducting the inspection/assessment obtains and examines a documented listing of ports, protocols, and services in use, and reviews a sampling of those ports, protocols, and services to ensure the organization being inspected/assessed is compliant with DoDI 8551.01. DoD has defined the registration requirements as IAW DoDI 8551.01.	MOD		X	X					1.9.3 Network Communication Report		Requirements met in UFGS 25 05 11 within "Network Communications Requirement" submission
N/A	CM-8(a)(1)	CCI-000389	The organization develops and documents an inventory of information system components that accurately reflects the current information system.	The organization being inspected/assessed documents inventory of information system components that accurately reflects the current information system.	The organization conducting the inspection/assessment obtains and examines the documented inventory and examines a sampling of information system components to ensure inventory accurately reflects the current information system.	LOW		X						1.9.4 Control System Inventory Report		Cybersecurity design requires the contractor to document the inventory of components within the control system through the submission of a Control System Inventory Report. This design requirement is captured in Sub-Paragraph "Control System Inventory Report" within Part 1.
N/A	CM-8(a)(2)	CCI-000392	The organization develops and documents an inventory of information system components that includes all components within the authorization boundary of the information system.	The organization being inspected/assessed documents inventory of information system components that includes all components within the authorization boundary of the information system.	The organization conducting the inspection/assessment obtains and examines the documented inventory and examines a sampling of information system components to ensure inventory includes all components within the authorization boundary of the information system.	LOW		X						1.9.4 Control System Inventory Report		Cybersecurity design requires the contractor to document the inventory of components within the control system with components through the submission of a Control System Inventory Report. This design requirement is captured in Sub-Paragraph "Control System Inventory Report" within Part 1.
N/A	CM-8(a)(3)	CCI-000395	The organization develops and documents an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting.	The organization being inspected/assessed documents inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting.	The organization conducting the inspection/assessment obtains and examines the documented inventory and examines a sampling of information system components to ensure inventory is at the level of granularity deemed necessary for tracking and reporting.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(a)(4)	CCI-000398	The organization defines information deemed necessary to achieve effective information system component accountability.	DoD has defined the information as hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information as hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name.	LOW		X	X	X	X			1.9.4 Control System Inventory Report		Cybersecurity design requires the contractor to document the inventory of components within the control system and submit a Control System Inventory Report. This design requirement is captured in Sub-Paragraph "Control System Inventory Report" within Part 1.
N/A	CM-8(a)(4)	CCI-000399	The organization develops and documents an inventory of information system components that includes organization defined information deemed necessary to achieve effective information system component accountability.	The organization being inspected/assessed documents inventory of information system components that includes organization defined information deemed necessary to achieve effective information system component accountability.	The organization conducting the inspection/assessment obtains and examines the documented inventory and examines a sampling of information system components to ensure inventory includes organization defined information deemed necessary to achieve effective information system component accountability.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(1)	CCI-000408	The organization updates the inventory of information system components as an integral part of component installations.	The organization being inspected/assessed documents and implements a process to update the inventory of information system components as an integral part of component installations. The organization must maintain an audit trail of updates. The audit trail may be recorded within the inventory itself.	The organization conducting the inspection/assessment obtains and examines the documented process for updates as well as the audit trail of updates and the log of changes to the information system to ensure the organization being inspected/assessed updates the inventory of information system components as an integral part of component installations.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(1)	CCI-000409	The organization updates the inventory of information system components as an integral part of component removals.	The organization being inspected/assessed documents and implements a process to update the inventory of information system components as an integral part of component removals. The organization must maintain an audit trail of updates. The audit trail may be recorded within the inventory itself.	The organization conducting the inspection/assessment obtains and examines the documented process for updates as well as the audit trail of updates and the log of changes to the information system to ensure the organization being inspected/assessed updates the inventory of information system components as an integral part of component removals.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(1)	CCI-000410	The organization updates the inventory of information system components as an integral part of information system updates.	The organization being inspected/assessed documents and implements a process to update the inventory of information system components as an integral part of information system updates. The organization must maintain an audit trail of updates. The audit trail may be recorded within the inventory itself.	The organization conducting the inspection/assessment obtains and examines the documented process for updates as well as the audit trail of updates and the log of changes to the information system to ensure the organization being inspected/assessed updates the inventory of information system components as an integral part of information system updates.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(2)	CCI-000411	The organization employs automated mechanisms to help maintain an up-to-date inventory of information system components.	The organization being inspected/assessed documents and implements automated mechanisms to help maintain an up-to-date inventory of information system components. An automated mechanism implemented IAW CM-2 (2) satisfies the requirements of this CCI if the automated mechanism maintains an up-to-date inventory.	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanism used to help maintain an up-to-date inventory of information system components and examines the mechanism to ensure the organization being inspected/assessed employs automated mechanisms to help maintain an up-to-date inventory of information system components.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-8(2)	CCI-000412	The organization employs automated mechanisms to help maintain a complete inventory of information system components.	The organization being inspected/assessed documents and implements automated mechanisms to help maintain a complete inventory of information system components. An automated mechanism implemented IAW CM-2 (2) satisfies the requirements of this CCI if the automated mechanism maintains a complete inventory.	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanism used to help maintain a complete inventory of information system components and examines the mechanism to ensure the organization being inspected/assessed employs automated mechanisms to help maintain a complete inventory of information system components.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(2)	CCI-000413	The organization employs automated mechanisms to help maintain a accurate inventory of information system components.	The organization being inspected/assessed documents and implements automated mechanisms to help maintain an accurate inventory of information system components. An automated mechanism implemented IAW CM-2 (2) satisfies the requirements of this CCI if the automated mechanism maintains an accurate inventory.	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanism used to help maintain an accurate inventory of information system components and examines the mechanism to ensure the organization being inspected/assessed employs automated mechanisms to help maintain an accurate inventory of information system components.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(2)	CCI-000414	The organization employs automated mechanisms to help maintain a readily available inventory of information system components.	The organization being inspected/assessed documents and implements automated mechanisms to help maintain a readily available inventory of information system components. An automated mechanism implemented IAW CM-2 (2) satisfies the requirements of this CCI if the automated mechanism maintains a readily available inventory.	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanism used to help maintain a readily available inventory of information system components and examines the mechanism to ensure the organization being inspected/assessed employs automated mechanisms to help maintain a readily available inventory of information system components.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(3)(a)	CCI-000415	The organization defines the frequency of employing automated mechanism to detect the presence of unauthorized hardware, software, and firmware components within the information system.	DoD has defined the frequency as continuously.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as continuously.	MOD			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(3)(a)	CCI-000416	The organization employs automated mechanisms, per organization defined frequency, to detect the presence of unauthorized hardware, software, and firmware components within the information system.	The organization being inspected/assessed documents and implements automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system continuously. DoD has defined the frequency as continuously.	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanisms and examines the implemented automated mechanisms to ensure the organization being inspected/assessed employs automated mechanisms, continuously, to detect the presence of unauthorized hardware, software, and firmware components within the information system. DoD has defined the frequency as continuously.	MOD			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(5)	CCI-000419	The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.	The organization being inspected/assessed verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.	The organization conducting the inspection/assessment obtains and examines the inventory list of the authorized information system and verifies that all components identified during the inspection are not duplicated in other information system inventories.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-9(a)	CCI-000421	The organization develops and documents a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.	The organization being inspected/assessed will develop and document a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to verify that it addresses and documents roles, responsibilities, and configuration management processes and procedures	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-9(a)	CCI-000423	The organization implements a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.	The organization being inspected/assessed will implement a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.	The organization conducting the inspection/assessment obtains and examines the configuration management plan as well as evidence of implementation (e.g., completed change requests, meeting minutes, and other relevant documents) to ensure the organization being inspected/assessed implements a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-9(c)	CCI-000424	The organization develops and documents a configuration management plan for the information system that defines the configuration items for the information system.	The organization being inspected/assessed will develop and document a configuration management plan for the information system that defines the configuration items.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure it defines and documents the configuration items for the information system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-9(c)	CCI-000426	The organization implements a configuration management plan for the information system that defines the configuration items for the information system.	The organization being inspected/assessed will implement a configuration management plan for the information system that defines the configuration items.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure the organization being inspected/assessed implements a configuration management plan for the information system that defines the configuration items.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-1(b)(1)	CCI-000437	The organization defines the frequency to review and update the current contingency planning policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-1(a)(1)	CCI-000438	The organization develops and documents a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-1(a)(1)	CCI-000439	The organization disseminates a contingency planning policy to organization-defined personnel or roles.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html NIST disseminates NIST SP 800-34 via http://csrc.nist.gov/publications/PubsSPs.html	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-1(b)(1)	CCI-000440	The organization reviews and updates the current contingency planning policy in accordance with organization-defined frequency.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CP-1(a)(2)	CCI-000441	The organization develops and documents procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-2(a)(1)	CCI-000443	The organization develops a contingency plan for the information system that identifies essential missions.	The organization being inspected/assessed must clearly and accurately document essential missions for its information system(s). Impact of loss of essential mission functions must be defined using CNSSI 1253.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents essential missions for its information system(s).	LOW			X			X	A LOW CS doesn't have any "essential" mission	---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(1)	CCI-000444	The organization develops a contingency plan for the information system that identifies essential business functions.	The organization being inspected/assessed must clearly and accurately document essential business functions for its information system(s). Impact of loss of essential business functions must be defined using CNSSI 1253.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents essential business functions for its information system(s).	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(1)	CCI-000445	The organization develops a contingency plan for the information system that identifies associated contingency requirements.	The organization being inspected/assessed must clearly and accurately document associated contingency requirements for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents associated contingency requirements for its information system(s).	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(2)	CCI-000446	The organization develops a contingency plan for the information system that provides recovery objectives.	The organization being inspected/assessed must clearly and accurately document recovery objectives for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents recovery objectives for its information system(s).	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(2)	CCI-000447	The organization develops a contingency plan for the information system that provides restoration priorities.	The organization being inspected/assessed must clearly and accurately document restoration priorities for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents restoration priorities for its information system(s).	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-2(a)(2)	CCI-000448	The organization develops a contingency plan for the information system that provides metrics.	The organization being inspected/assessed must clearly and accurately document metrics for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents metrics for its information system(s).	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-2(a)(3)	CCI-000449	The organization develops a contingency plan for the information system that addresses contingency roles, responsibilities, assigned individuals with contact information.	The organization being inspected/assessed must clearly and accurately document contingency roles, responsibilities, assigned individuals with contact information for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents contingency roles, responsibilities, assigned individuals with contact information for its information system(s).	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-2(a)(4)	CCI-000450	The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system disruption.	The organization being inspected/assessed must clearly and accurately document maintaining essential missions despite an information system disruption for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential missions despite an information system disruption for its information system(s).	LOW			X			X	A LOW CS doesn't have any "essential" mission	---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(4)	CCI-000451	The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system disruption.	The organization being inspected/assessed must clearly and accurately document maintaining business functions despite an information system disruption for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining business functions despite an information system disruption for its information system(s).	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(4)	CCI-000452	The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system compromise.	The organization being inspected/assessed must clearly and accurately document maintaining essential missions despite an information system compromise for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential missions despite an information system compromise for its information system(s).	LOW			X			X	A LOW CS doesn't have any "essential" mission	---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-2(a)(4)	CCI-000453	The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system compromise.	The organization being inspected/assessed must clearly and accurately document maintaining business functions despite an information system compromise for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining business functions despite an information system compromise for its information system(s).	LOW								---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-2(a)(4)	CCI-000454	The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system failure.	The organization being inspected/assessed must clearly and accurately document maintaining essential missions despite an information system failure for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining essential missions despite an information system failure for its information system(s).	LOW			X			X	A LOW CS doesn't have any "essential" mission	---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-2(a)(4)	CCI-000455	The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system failure.	The organization being inspected/assessed must clearly and accurately document maintaining business functions despite an information system failure for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents maintaining business functions despite an information system failure for its information system(s).	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(5)	CCI-000456	The organization develops a contingency plan for the information system that addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.	The organization being inspected/assessed must clearly and accurately document eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented for its information system(s).	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented for its information system(s).	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(6)	CCI-000457	The organization develops a contingency plan for the information system that is reviewed and approved by organization-defined personnel or roles.	The organization being inspected/assessed reviews and approves the contingency plan by at a minimum, the ISSM and ISSO. The organization must maintain an audit trail of the review and approval activity. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization conducting the inspection/assessment obtains and examines the audit trail to ensure the contingency plan has been reviewed and approved by at a minimum, the ISSM and ISSO. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(b)	CCI-000458	The organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan.	DoD has defined the list as all stakeholders identified in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the list as all stakeholders identified in the contingency plan.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(b)	CCI-000459	The organization distributes copies of the contingency plan to an organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements.	The organization being inspected/assessed ensures the contingency plan is disseminated to all stakeholders identified in the contingency plan via an information sharing capibility. DoD has defined the list as all stakeholders identified in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(c)	CCI-000460	The organization coordinates contingency planning activities with incident handling activities.	The organization being inspected/assessed will coordinate the contingency plan and incident response plan (IR-8) to ensure they do not contradict each other's objectives or result in duplicate efforts/activities.	The organization conducting the inspection/assessment obtains and examines the contingency plan and the incident response plan (IR-8) to ensure they do not contradict each other's objectives or result in duplicate efforts/activities.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enriches	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CP-2(d)	CCI-000461	The organization defines the frequency to review the contingency plan for the information system.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-2(d)	CCI-000462	The organization reviews the contingency plan for the information system in accordance with organization-defined frequency.	The organization being inspected/assessed annually reviews the contingency plan. The organization must maintain an audit trail of annual reviews.	The organization conducting the inspection/assessment obtains and examines the audit trail to ensure the contingency plan is reviewed annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(e)	CCI-000463	The organization updates the contingency plan to address changes to the organization.	The organization being inspected/assessed must clearly and accurately update the contingency plan to address organizational changes. The organization must document the update activities as an audit trail.	The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately updates the contingency plan to address organizational changes.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(e)	CCI-000464	The organization updates the contingency plan to address changes to the information system.	The organization being inspected/assessed must clearly and accurately update the contingency plan to address changes to the information system. The organization must document the update activities as an audit trail.	The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately updates the contingency plan to address information system changes.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(e)	CCI-000465	The organization updates the contingency plan to address changes to the environment of operation.	The organization being inspected/assessed must clearly and accurately revise the contingency plan to address changes to the environment of operation. The organization must document the update activities as an audit trail.	The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately revises the contingency plan to address changes to the environment of operation.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(e)	CCI-000466	The organization updates the contingency plan to address problems encountered during contingency plan implementation, execution, or testing.	The organization being inspected/assessed must clearly and accurately revise the contingency plan to address problems encountered during contingency plan implementation, execution, or testing. The organization must document the update activities as an audit trail.	The organization conducting the inspection/assessment obtains and examines the contingency plan and audit trail to ensure the organization clearly and accurately revises the contingency plan to address problems encountered during contingency plan implementation, execution, or testing.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(f)	CCI-000468	The organization communicates contingency plan changes to organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements.	The organization being inspected/assessed communicates contingency plan changes to all stakeholders identified in the contingency plan. DoD has defined the list as all stakeholders identified in the contingency plan.	The organization conducting the inspection/assessment examines the contingency plan via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure the most current version has been communicated.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(1)	CCI-000469	The organization coordinates contingency plan development with organizational elements responsible for related plans.	The organization being inspected/assessed coordinates the development of its contingency plan with other organizational elements responsible for related plans. The organization documents any applicable agreements with responsible internal or external entities. For external entities the agreements could entail MOUs, MOAs, SLAs or contracts.	The organization conducting the inspection/assessment obtains and examines documentation of agreements with entities responsible for the contingency or related plans to ensure there is evidence of coordination of those plans.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(3)	CCI-000473	The organization defines the time period for planning the resumption of essential missions as a result of contingency plan activation.	DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	MOD					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-2(3)	CCI-000474	The organization defines the time period for planning the resumption of essential business functions as a result of contingency plan activation.	DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	MOD					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-2(3)	CCI-000475	The organization plans for the resumption of essential missions within the organization-defined time period of contingency plan activation.	The organization being inspected/assessed shall document within their contingency plan, procedures for resumption of essential missions within 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	The organization conducting the inspection/assessment obtains the contingency plan to ensure it contains procedures for resumption of essential missions within 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(3)	CCI-000476	The organization plans for the resumption of essential business functions within the organization-defined time period of contingency plan activation.	The organization being inspected/assessed shall document within their contingency plan, procedures for resumption of essential business functions within 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	The organization conducting the inspection/assessment obtains the contingency plan to ensure it contains procedures for resumption of essential business functions within 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-3(c)	CCI-000485	The organization defines the frequency of refresher contingency training to information system users.	DoD has defined the frequency as at least annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-3(a)	CCI-000486	The organization provides contingency training to information system users consistent with assigned roles and responsibilities within an organization-defined time period of assuming a contingency role or responsibility.	The organization being inspected/assessed provides initial contingency training to personnel with contingency roles and responsibilities IAW CP-2, CCI 449 at a maximum, 10 working days of assuming a contingency role or responsibility. The organization will maintain documentation of the training activity dates, location, and personnel for audit trail purposes and future reference (e.g., scheduling refresher training, etc.). DoD has defined the time period as at a maximum, 10 working days.	The organization conducting the inspection/assessment obtains and examines the list of contingency personnel and documentation of initial contingency training for the purpose of ensuring that all personnel with contingency roles and responsibilities have received initial contingency training at a maximum, 10 working days of assuming a contingency role or responsibility. DoD has defined the time period as at a maximum, 10 working days.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CP-3(c)	CCI-000487	The organization provides refresher contingency training to information system users consistent with assigned roles and responsibilities in accordance with organization-defined frequency.	The organization being inspected/assessed provides refresher contingency training to personnel with contingency roles and responsibilities IAW CP-2, CCI 449 at least annually. The organization will maintain documentation of the training activity dates, location, and personnel for audit trail purposes and future reference (e.g., scheduling refresher training, etc.). DoD has defined the frequency as at least annually.	The organization conducting the inspection/assessment obtains and examines the list of contingency personnel and documentation of refresher contingency training for the purpose of ensuring that all personnel with contingency roles and responsibilities have received refresher contingency training at least annually. DoD has defined the frequency as at least annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-4(a)	CCI-000490	The organization defines the frequency to test the contingency plan for the information system.	DoD has defined the frequency as at least annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-4(a)	CCI-000492	The organization defines contingency plan tests to be conducted for the information system.	The organization being inspected/assessed defines and documents contingency plan tests to be conducted for the information system. DoD has determined the contingency plan tests are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented contingency plan tests to ensure the organization being inspected/assessed defines contingency plan tests to be conducted for the information system. DoD has determined the contingency plan tests are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-4(a)	CCI-000494	The organization tests the contingency plan for the information system in accordance with organization-defined frequency using organization-defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan.	The organization being inspected/assessed conduct tests defined in CP-4, 492 at least annually to determine the effectiveness of the plan and the organizational readiness to execute the plan. The organization must maintain a record of test results. DoD has defined the frequency as at least annually.	The organization conducting the inspection/assessment obtains and examines the record of test results to ensure the organization being inspected/assessed conduct tests defined in CP-4, 492 at least annually to determine the effectiveness of the plan and the organizational readiness to execute the plan. DoD has defined the frequency as at least annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-4(b)	CCI-000496	The organization reviews the contingency plan test results.	The organization being inspected/assessed will review the contingency plan test results. The organization must maintain an audit trail of issues identified during the reviews of the contingency plan test results.	The organization conducting the inspection/assessment obtains and examines the audit trail of issues identified during the reviews of the contingency plan test results to ensure the organization being inspected/assessed reviews the contingency plan test results.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-4(c)	CCI-000497	The organization initiates corrective actions, if needed, after reviewing the contingency plan test results.	The organization being inspected/assessed identifies and documents any corrective actions required after reviewing the contingency plan test results. The organization initiates corrective actions and tracks those actions within the POA&M.	The organization conducting the inspection/assessment obtains and examines the contingency plan test results as well as any documented corrective actions required and ensures the corrective actions are being implemented and tracked within the POA&M.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-4(1)	CCI-000498	The organization coordinates contingency plan testing with organizational elements responsible for related plans.	The organization being inspected/assessed coordinates the testing of its contingency plan with other organizational elements responsible for related plans. The organization documents any applicable agreements with responsible internal or external entities. For external entities the agreements could entail MOUs, MOAs, SLAs or contracts.	The organization conducting the inspection/assessment obtains and examines documentation of agreements with entities responsible for the contingency or related plans to ensure there is evidence of coordination of those tests.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-6(a)	CCI-000505	The organization establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.	The organization being inspected/assessed establishes an alternate storage site and documents relevant information within the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan to confirm the organization has established an alternate storage site.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-6(1)	CCI-000507	The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.	The organization being inspected/assessed identifies and documents within the contingency plan an alternate storage site not susceptible to the same threats that exist at the primary storage site. The organization must document threats in the risk management strategy IAW PM-9, CCI 000227.	The organization conducting the inspection/assessment obtains and examines the risk management strategy and the contingency plan to ensure the organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same threats identified at the primary site.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-6(3)	CCI-000509	The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.	The organization being inspected/assessed must identify and document in the contingency plan potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure the organization has documented potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-7(a)	CCI-000510	The organization defines the time period consistent with recovery time and recovery point objectives for essential missions/business functions to permit the transfer and resumption of organization-defined information system operations at an alternate processing site when the primary processing capabilities are unavailable.	DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan	MOD	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-7(a)	CCI-000513	The organization establishes an alternate processing site including necessary agreements to permit the transfer and resumption of organization-defined information system operations for essential missions within organization-defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable.	The organization being inspected/assessed documents and gains approval for alternate processing site agreements that permit the transfer and resumption of information system operations for essential missions within 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the approved alternate processing site agreements to ensure the organization has alternate processing site support that will permit the transfer and resumption of information system operations for essential missions within 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CP-7(a)	CCI-000514	The organization establishes an alternate processing site including necessary agreements to permit the transfer and resumption of organization-defined information system operations for essential business functions within organization-defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable.	The organization being inspected/assessed documents and gains approval for alternate processing site agreements that permit the transfer and resumption of information system operations for business functions within 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the approved alternate processing site agreements to ensure the organization has alternate processing site support that will permit the transfer and resumption of information system operations for business functions within 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-7(b)	CCI-000515	The organization ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption.	The organization being inspected/assessed maintains an inventory of equipment and supplies required to transfer and resume operations, or engages contract support that meets required timelines to support 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	The organization conducting the inspection/assessment obtains and examines: 1. Inventory of equipment and supplies or, 2. Contract documentation to ensure the organization has the equipment and supply resources necessary, or provisions to obtain the resources to transfer and resume operations at the alternate processing site within 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-7(1)	CCI-000516	The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.	The organization being inspected/assessed identifies and documents within the contingency plan an alternate processing site not susceptible to the same threats that exist at the primary processing site. The organization must document threats in the risk management strategy IAW PM-9, CCI 000227.	The organization conducting the inspection/assessment obtains and examines the risk management strategy and the contingency plan to ensure the organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same threats identified at the primary site.	MOD	X			X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CP-7(2)	CCI-000517	The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.	The organization being inspected/assessed must identify and document in the contingency plan potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure the organization has documented potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-7(3)	CCI-000518	The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organizational availability requirements (including recovery time objectives).	The organization being inspected/assessed documents and gains approval for alternate processing site agreements that contain priority-of-service provisions in accordance with CP-2, CCI 447 (including recovery time objectives).	The organization conducting the inspection/assessment obtains and examines the approved alternate processing site agreements to ensure they contain priority-of-service provisions in accordance with CP-2, CCI 447 for alternate processing site support (including recovery time objectives).	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-7(c)	CCI-000521	The organization ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.	The organization being inspected/assessed documents the information security safeguards that are in place at both the primary and alternate sites and evidence that the alternate site was approved based on an assessment that security is equivalent at the alternate site.	The organization conducting the inspection/assessment obtains and examines the documentation of the primary/alternate site information security safeguards that are in place as well as evidence that the alternate site was approved based on an assessment that security is equivalent at the alternate site.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-8	CCI-000522	The organization defines the time period to permit the resumption of organization-defined information system operations for essential missions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	MOD	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-8	CCI-000523	The organization defines the time period to permit the resumption of organization-defined information system operations for essential business functions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	MOD								---	CS aren't mobile.	
N/A	CP-8	CCI-000524	The organization establishes alternate telecommunication services including necessary agreements to permit the resumption of organization-defined information system operations for essential missions within organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	The organization being inspected/assessed documents and gains approval for alternate telecommunications service agreements that permit the resumption of telecommunications services for essential missions IAW DoDI 8100.04. DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the approved alternate telecommunications service agreements to ensure they permit the resumption of telecommunications services for essential mission IAW DoDI 8100.04. DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	MOD	X							---	CS aren't mobile.	
N/A	CP-8	CCI-000525	The organization establishes alternate telecommunication services including necessary agreements to permit the resumption of organization-defined information system operations for essential business functions within organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	The organization being inspected/assessed documents and gains approval for alternate telecommunications service agreements that permit the resumption of telecommunications services for business functions IAW DoDI 8100.04. DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the approved alternate telecommunications service agreements to ensure they permit the resumption of telecommunications services for business functions IAW DoDI 8100.04. DoD has defined the time period as 1 hour (Availability High) 12 hours (Availability Moderate) as defined in the contingency plan.	MOD								---	CS aren't mobile.	
N/A	CP-8(1)(a)	CCI-000526	The organization develops primary telecommunications service agreements that contain priority-of-service provisions in accordance with the organizations availability requirements (including recovery time objectives).	The organization being inspected/assessed documents and gains approval for primary telecommunications service agreements that contain priority-of-service provisions IAW DoDI 8100.04 (including recovery time objectives).	The organization conducting the inspection/assessment obtains and examines the approved primary telecommunications service agreements to ensure they contain priority-of-service provisions IAW DoDI 8100.04 (including recovery time objectives).	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-8(1)(a)	CCI-000527	The organization develops alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organizations availability requirements (including recovery time objectives).	The organization being inspected/assessed documents and gains approval for alternate telecommunications service agreements that contain priority-of-service provisions IAW DoDI 8100.04 (including recovery time objectives).	The organization conducting the inspection/assessment obtains and examines the approved alternate telecommunications service agreements to ensure they contain priority-of-service provisions IAW DoDI 8100.04 (including recovery time objectives).	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures		Applies at or Below Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CP-8(1)(b)	CCI-000528	The organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary telecommunications services are provided by a common carrier.	The organization being inspected/assessed identifies and documents within the contingency plan any telecommunications services used for national security emergency preparedness. If the primary telecommunications services are provided by a common carrier, the organization formally requests Telecommunications Service Priority IAW the DHS Telecommunications Service Priority Process http://www.dhs.gov/telecommunications-service-priority-tsp. If the primary telecommunications services are provided by a mid-tier provider instead of a common carrier (for example, DISA) the organization must insure that their provider formally requests Telecommunications Service Priority on their behalf.	The organization conducting the inspection/assessment obtains and examines the contingency plan, the telecommunication service agreement, and any existing formal requests for Telecommunications Service Priority. The purpose of the review is to ensure the organization or the mid-tier provider has requested Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness where the primary telecommunications services are provided by a common carrier.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-8(1)(b)	CCI-000529	The organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the alternate telecommunications services are provided by a common carrier.	The organization being inspected/assessed identifies and documents within the contingency plan telecommunications services used for national security emergency preparedness in the event the alternate telecommunications services are provided by a common carrier. For each service, the organization formally requests Telecommunications Service Priority, IAW the DHS Telecommunications Service Priority Process http://tsp.ncs.gov/request.html.	The organization conducting the inspection/assessment obtains and examines the contingency plan, the telecommunication service agreement, and any existing formal requests for Telecommunications Service Priority. The purpose of the review is to ensure the organization has requested Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event the alternate telecommunications services are provided by a common carrier.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-8(2)	CCI-000530	The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	The organization being inspected/assessed obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services IAW DoDI 8100.04.	The organization conducting the inspection/assessment obtains and examines agreements with their service providers to ensure that a single point of failure is not shared.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-9(a)	CCI-000534	The organization defines frequency of conducting user-level information backups to support recovery time objectives and recovery point objectives.	DoD has defined the frequency as at least weekly as defined in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least weekly as defined in the contingency plan.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-9(a)	CCI-000535	The organization conducts backups of user-level information contained in the information system per organization-defined frequency that is consistent with recovery time and recovery point objectives.	The organization being inspected/assessed must identify user level information within the backup strategy and configure the system to perform backups at least weekly as defined in the contingency plan.	The organization conducting the inspection/assessment obtains and reviews the backup strategy, and examines a sample of systems to ensure they are configured to perform back ups at least weekly as defined in the contingency plan.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-9(b)	CCI-000536	The organization defines frequency of conducting system-level information backups to support recovery time objectives and recovery point objectives.	DoD has defined the frequency as at least weekly and as required by system baseline configuration changes in accordance with the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least weekly and as required by system baseline configuration changes in accordance with the contingency plan.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-9(b)	CCI-000537	The organization conducts backups of system-level information contained in the information system per organization-defined frequency that is consistent with recovery time and recovery point objectives.	The organization being inspected/assessed must identify system-level information within the backup strategy and configure the system to perform backups at least weekly and as required by system baseline configuration changes in accordance with the contingency plan.	The organization conducting the inspection/assessment obtains and reviews the backup strategy, and examines a sample of systems to ensure they are configured to perform back ups at least weekly and as required by system baseline configuration changes in accordance with the contingency plan.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-9(c)	CCI-000538	The organization defines the frequency of conducting information system documentation backups including security-related documentation to support recovery time objectives and recovery point objectives.	DoD has defined the frequency as when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-9(c)	CCI-000539	The organization conducts backups of information system documentation including security-related documentation per organization-defined frequency that is consistent with recovery time and recovery point objectives.	The organization being inspected/assessed conducts backups of information system documentation including security-related documentation when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan.	The organization conducting the inspection/assessment obtains and examines the latest version of the information system documentation including security-related documentation to verify it is the same version as contained in backups.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-9(d)	CCI-000540	The organization protects the confidentiality, integrity, and availability of backup information at storage locations.	The organization being inspected/assessed will protect the confidentiality, integrity, and availability of backup information at the storage location IAW the system security plan.	The organization conducting the inspection/assessment obtains and examines the system security plan and ensures backup information at the storage location is protected IAW the system security plan.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-9(1)	CCI-000541	The organization defines the frequency to test backup information to verify media reliability and information integrity.	DoD has defined the frequency as at least monthly in accordance with contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least monthly in accordance with contingency plan.	MOD	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-9(1)	CCI-000542	The organization tests backup information per organization-defined frequency to verify media reliability and information integrity.	The organization being inspected/assessed tests and logs backup information at least monthly in accordance with contingency plan to verify media reliability and information integrity.	The organization conducting the inspection/assessment obtains and examines the backup plan and verifies that the organization has tested and logged backup information.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-9(5)	CCI-000547	The organization defines the time period and transfer rate of the information system backup information to the alternate storage site consistent with the recovery time and recovery point objectives.	DoD has defined the time period as Continuously (Availability High) 24 hours (Availability Moderate) 7 days (Availability Low) as defined in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as Continuously (Availability High) 24 hours (Availability Moderate) 7 days (Availability Low) as defined in the contingency plan.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-9(5)	CCI-000548	The organization transfers information system backup information to the alternate storage site in accordance with the organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives.	The organization being inspected/assessed performs the transfer of information system backup information to the alternate site Continuously (Availability High) 24 hours (Availability Moderate) 7 days (Availability Low) as defined in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan and related logs to ensure the organization transfers information system backup information to the alternate site Continuously (Availability High) 24 hours (Availability Moderate) 7 days (Availability Low) as defined in the contingency plan.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CP-10	CCI-000550	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption.	The organization being inspected/assessed provides automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a disruption. The organization must identify the selected method in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it identifies the recovery and reconstitution method for its information system to a known state after a disruption.	LOW	X	X	X					1.9.5 Software and Configuration Backups		Cybersecurity Requirements are met by requiring the contractor to submit a "Software and Configuration Backups" report with Part 1
N/A	CP-10	CCI-000551	The organization provides for the recovery and reconstitution of the information system to a known state after a compromise.	The organization being inspected/assessed provides automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a compromise. The organization must identify the selected method in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it identifies the recovery and reconstitution method for its information system to a known state after a compromise.	LOW	X	X	X					1.9.5 Software and Configuration Backups		Cybersecurity Requirements are met by requiring the contractor to submit a "Software and Configuration Backups" report with Part 1
N/A	CP-10	CCI-000552	The organization provides for the recovery and reconstitution of the information system to a known state after a failure.	The organization being inspected/assessed provides automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a failure. The organization must identify the selected method in the contingency plan.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it identifies the recovery and reconstitution method for its information system to a known state after a failure.	LOW	X	X	X					1.9.5 Software and Configuration Backups		Cybersecurity Requirements are met by requiring the contractor to submit a "Software and Configuration Backups" report with Part 1
N/A	CP-10(2)	CCI-000553	The information system implements transaction recovery for systems that are transaction-based.	The organization being inspected/assessed identifies, documents, and implements transaction recovery capability for systems that are transaction-based. The organization must document transaction recovery results as part of contingency plan testing.	The organization conducting the inspection/assessment obtains and examines the contingency plan test results to verify transaction recovery.	MOD		X	X	X				---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-1(a)(1)	CCI-000563	The organization develops and documents a security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 8510.01 meets the requirements for a security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.	DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-1(a)(1)	CCI-000564	The organization disseminates a security planning policy to organization-defined personnel or roles .	DoD disseminates DoDI 8510.01 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) to organizational personnel with planning responsibilities or information security responsibilities. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-1(a)(2)	CCI-000566	The organization develops and documents procedures to facilitate the implementation of the security planning policy and associated security planning controls.	DoDI 8510.01 meets the requirements for developing and documenting procedures to facilitate the implementation of the security planning policy and associated security planning controls. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.	DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-1(b)(2)	CCI-000567	The organization disseminates security planning procedures to organization-defined personnel or roles.	DoD disseminates DoDI 8510.01 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) to organizational personnel with planning responsibilities or information security responsibilities. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the roles as organizational personnel with planning responsibilities or information security responsibilities.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-1(b)(2)	CCI-000568	The organization reviews and updates the current security planning procedures in accordance with organization-defined frequency.	DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the frequency as reviewed annually - updated as appropriate.	DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-2(a)(9)	CCI-000571	The organization's security plan for the information system is reviewed and approved by the authorizing official or designated representative prior to plan implementation.	The organization being inspected/assessed obtains security plan approval by the authorizing official or designated representative prior to plan implementation.	The organization conducting the inspection/assessment obtains and examines the security plan approval to ensure the organization being inspected/assessed obtains security plan approval by the authorizing official or designated representative prior to plan implementation.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-2(c)	CCI-000572	The organization defines the frequency for reviewing the security plan for the information system.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW				X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PL-2(c)	CCI-000573	The organization reviews the security plan for the information system in accordance with organization-defined frequency.	The information system owner as part of the annual security control review will also review the security plan annually. Documentation of security plan reviews is required as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit records of security plan reviews to verify the security plan has been reviewed annually. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-2(d)	CCI-000574	The organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.	The information system owner will update the security plan as necessary to address changes to information system/environment of operation or problems identified during plan implementation or security control assessments. Documentation of security plan updates are required as an audit trail.	The organization conducting the inspection/assessment obtains and examines the audit records of security plan updates to verify the security plan is current. The purpose of the reviews is to validate the organization is updating the Information System (IS) security plan to address changes to the IS, its environment of operation, or problems identified during plan implementation or security control assessments.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-4(a)	CCI-000592	The organization establishes the rules describing the responsibilities and expected behavior, with regard to information and information system usage, for individuals requiring access to the information system.	The organization being inspected/assessed must develop and document rules that describe information system user responsibilities and expected behavior with regard to information and information system usage, acceptable use policy (AUP). Organizations should reference Joint Ethics Regulations (DoD 5500.7-R) when developing this policy.	The organization conducting the inspection/assessment obtains and examines the organization's AUP to ensure the organization has clearly defined and established rules describing information system user responsibilities and expected behavior with regard to information and information system usage.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-4(b)	CCI-000593	The organization receives a signed acknowledgment from individuals requiring access the system, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	The organization being inspected/assessed will obtain signed acknowledgment (paper or electronic signature) from individuals indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	The organization conducting the inspection/assessment obtains a list of individuals with active accounts and validates the existence of signed acknowledgements (paper or electronic signature) of the organizational AUP associated with a sampling of individuals selected from the list.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-1(b)(1)	CCI-000601	The organization defines the frequency to review and update the current system and services acquisition policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(a)(1)	CCI-000602	The organization develops and documents a system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(a)(1)	CCI-000603	The organization disseminates to organization-defined personnel or roles a system and services acquisition policy.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(b)(1)	CCI-000604	The organization reviews and updates the current system and services acquisition policy in accordance with organization-defined frequency.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(a)(2)	CCI-000605	The organization develops and documents procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(a)(2)	CCI-000606	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-1(b)(2)	CCI-000607	The organization reviews and updates the current system and services acquisition procedures in accordance with organization-defined frequency.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1 meet the DoD requirements for system and services acquisition policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDD 5000.01, DoDI 5000.02, and DoDI 8580.1.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-2(b)	CCI-000610	The organization determines the resources required to protect the information system or information system service as part of its capital planning and investment control process.	The organization being inspected/assessed determines the resources (funding, staffing, etc.) required for the cybersecurity requirements to protect the information system or information system service as part of its planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has determined the resources required for cybersecurity requirements to protect the information system or information system service.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-2(b)	CCI-000611	The organization documents the resources required to protect the information system or information system service as part of its capital planning and investment control process.	The organization being inspected/assessed documents the resources (funding, staffing, etc.) required for the cybersecurity requirements to protect the information system or information system service as part of its planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has documented the resources required for cybersecurity requirements to protect the information system or information system service.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-2(b)	CCI-000612	The organization allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process.	The organization being inspected/assessed allocates the resources (funding, staffing, etc.) required for the cybersecurity requirements to protect the information system or information system service as part of its planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has allocated the resources required for cybersecurity requirements to protect the information system or information system service.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-2(c)	CCI-000613	The organization establishes a discrete line item for information security in organizational programming documentation.	The organization being inspected/assessed identifies and establishes an individual line item for cybersecurity requirements to protect the information system as part of the planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has identified and established an individual line item for cybersecurity requirements to protect the information system.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-2(c)	CCI-000614	The organization establishes a discrete line item for information security in organizational budgeting documentation.	The organization being inspected/assessed identifies and establishes an individual line item for cybersecurity requirements to protect the information system as part of the planning, programming, and budget process (PPBE).	The organization conducting the inspection/assessment obtains and examines the planning, programming, and budget documentation to ensure the organization being inspected/assessed has identified and established an individual line item for cybersecurity requirements to protect the information system.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-3(a)	CCI-000615	The organization manages the information system using organization-defined system development life cycle that incorporates information security considerations.	The organization being inspected/assessed documents and implements a process to manage the information system using the system development life cycle defined in SA-3, CCI 3092 that incorporates information security considerations IAW DoDI 8580.1.	The organization conducting the inspection/assessment obtains and examines the documented process and artifacts of the system development life cycle process to ensure the organization being inspected/assessed manages the information system using the system development life cycle defined in SA-3, CCI 3092 that incorporates information security considerations IAW DoDI 8580.1.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-3(b)	CCI-000616	The organization defines and documents information system security roles and responsibilities throughout the system development life cycle.	The organization being inspected/assessed defines and documents information system security roles and responsibilities throughout the system development life cycle IAW DoDI 8580.1 .	The organization conducting the inspection/assessment obtains and examines the information system security roles and responsibilities to ensure the organization being inspected/assessed defines and documents information system security roles and responsibilities throughout the system development life cycle IAW DoDI 8580.1.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-3(c)	CCI-000618	The organization identifies individuals having information system security roles and responsibilities.	The organization being inspected/assessed identifies and documents individuals having information system security roles and responsibilities.	The organization conducting the inspection/assessment obtains and examines the documented individuals having information system security roles and responsibilities to ensure the organization being inspected/assessed identifies individuals having information system security roles and responsibilities.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(1)	CCI-000623	The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	DoDI 8510.01 system categorization meets the DoD requirement for providing a description of the functional properties of the security controls to be employed. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01.	DoDI 8510.01 system categorization meets the DoD requirement for providing a description of the functional properties of the security controls to be employed. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01.	MOD		X	X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(7)(a)	CCI-000634	The organization limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists.	The organization being inspected/assessed, when using commercially provided IA and IA-enabled IT products uses only products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists.	The organization conducting the inspection/assessment obtains and examines the hardware and software lists to ensure the organization being inspected/assessed, when using commercially provided IA and IA-enabled IT products uses only products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(7)(b)	CCI-000635	The organization requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.	The organization being inspected/assessed, when using commercially provided IA or IA enabled IT products for which there is no NIAP-approved protection profile, relies on FIPS-validated cryptographic modules.	The organization conducting the inspection/assessment obtains and examines the hardware and software lists to ensure the organization being inspected/assessed, when using commercially provided IA or IA enabled IT products for which there is no NIAP-approved protection profile, relies on FIPS-validated cryptographic modules.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-5(c)	CCI-000642	The organization documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.	The organization being inspected/assessed documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.	The organization conducting the inspection/assessment obtains and examines the documented attempts to ensure the organization being inspected/assessed documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-8	CCI-000664	The organization applies information system security engineering principles in the specification of the information system.	The organization managing the acquisition/development of the information system (e.g. PM) applies and documents system security engineering (SSE) principles as part of the overall systems engineering process IAW DoDD 5000.01 and DoDI 5000.02. The primary source of general and DoD-specific guidance on SSE can be found in the NIST SP 800-160 - Systems Security Engineering, currently in draft form, and can be found here: http://csrc.nist.gov/publications/PubsSPs.html. Additional guidance can be found in the Defense Acquisition Guidebook (DAG) Chapters 4 and 13, found here: https://dag.dau.mil/. This CCI does not apply to COTS products. The organization managing the acquisition/development of the information system must ensure that the system requirements documents reflect the system security engineering principles that can be applied to information systems in development, systems undergoing major upgrades and to the extent feasible systems in sustainment. Security engineering principles include: 1. Developing layered protections; 2. Establishing sound security policy, architecture	The organization conducting the inspection/assessment obtains and examines the system requirements documents to ensure that the organization being inspected/assessed applies information system security engineering principles in the specification of the information system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-8	CCI-000665	The organization applies information system security engineering principles in the design of the information system.	The organization managing the acquisition/development of the information system (e.g. PM) applies and documents system security engineering (SSE) principles as part of the overall systems engineering process IAW DoDD 5000.01 and DoDI 5000.02. The primary source of general and DoD-specific guidance on SSE can be found in the NIST SP 800-160 - Systems Security Engineering, currently in draft form, and can be found here: http://csrc.nist.gov/publications/PubsSPs.html. Additional guidance can be found in the Defense Acquisition Guidebook (DAG) Chapters 4 and 13, found here: https://dag.dau.mil/. This CCI does not apply to COTS products. The organization managing the acquisition/development of the information system must ensure that the design documents reflect the system security engineering principles that can be applied to information systems in development, systems undergoing major upgrades and to the extent feasible systems in sustainment. Security engineering principles include: 1. Developing layered protections; 2. Establishing sound security policy, architecture,	The organization conducting the inspection/assessment obtains and examines the design documents to ensure that the organization being inspected/assessed applies information system security engineering principles in the design of the information system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-8	CCI-000666	The organization applies information system security engineering principles in the development of the information system.	The organization managing the acquisition/development of the information system (e.g. PM) applies and documents system security engineering (SSE) principles as part of the overall systems engineering process IAW DoDD 5000.01 and DoDI 5000.02. The primary source of general and DoD-specific guidance on SSE can be found in the NIST SP 800-160 - Systems Security Engineering, currently in draft form, and can be found here: http://csrc.nist.gov/publications/PubsSPs.html. Additional guidance can be found in the Defense Acquisition Guidebook (DAG) Chapters 4 and 13, found here: https://dag.dau.mil/. This CCI does not apply to COTS products. The organization managing the acquisition/development of the information system must ensure that the development procedures reflect the system security engineering principles that can be applied to information systems in development, systems undergoing major upgrades and to the extent feasible systems in sustainment. Security engineering principles include: 1. Developing layered protections; 2. Establishing sound security policy, architecture,	The organization conducting the inspection/assessment obtains and examines the system development procedures (e.g. configuration management plans, code review procedures, and coding style guides) to ensure that the organization being inspected/assessed applies information system security engineering principles in the development of the information system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-8	CCI-000667	The organization applies information system security engineering principles in the implementation of the information system.	The organization managing the acquisition/development of the information system (e.g. PM) applies and documents system security engineering (SSE) principles as part of the overall systems engineering process IAW DoDD 5000.01 and DoDI 5000.02. The primary source of general and DoD-specific guidance on SSE can be found in the NIST SP 800-160 - Systems Security Engineering, currently in draft form, and can be found here: http://csrc.nist.gov/publications/PubsSPs.html. Additional guidance can be found in the Defense Acquisition Guidebook (DAG) Chapters 4 and 13, found here: https://dag.dau.mil/. This CCI does not apply to COTS products. The organization managing the acquisition/development of the information system must employ the procedures identified in SA-8, CCI, 000666 during the implementation of the information system. The system owner must maintain an audit trail of the activities conducted IAW SA-8, CCI 000666. An example of artifacts is CCB minutes, code review results, and source code analysis results	The organization conducting the inspection/assessment obtains and examines the audit trail artifacts that were created during the implementation of SA-8, CCI 000666 to ensure that the organization being inspected/assessed applies information system security engineering principles in the implementation of the information system and that changes are made IAW the configuration management plan (CM-9, CCI 001790).	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enriched	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-8	CCI-000668	The organization applies information system security engineering principles in the modification of the information system.	The organization managing the acquisition/development of the information system (e.g. PM) applies and documents system security engineering (SSE) principles as part of the overall systems engineering process IAW DoDD 5000.01 and DoDI 5000.02. The primary source of general and DoD-specific guidance on SSE can be found in the NIST SP 800-160 - Systems Security Engineering, currently in draft form, and can be found here: http://csrc.nist.gov/publications/PubsSPs.html. Additional guidance can be found in the Defense Acquisition Guidebook (DAG) Chapters 4 and 13, found here: https://dag.dau.mil/. This CCI does not apply to COTS products. The organization managing the acquisition/development of the information system must employ the procedures identified in SA-8, CCI, 000666 during the modification of the information system. The system owner must maintain an audit trail of the activities conducted IAW SA-8, CCI 000666. An example of artifacts is CCB minutes, code review results, and source code analysis results.	The organization conducting the inspection/assessment obtains and examines the audit trail artifacts that were created during the modification of SA-8, CCI 000666 to ensure that the organization being inspected/assessed applies information system security engineering principles in the modification of the information system and that changes are made IAW the configuration management plan (CM-9, CCI 001790).	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-9(a)	CCI-000669	The organization requires that providers of external information system services comply with organizational information security requirements.	The organization being inspected/assessed documents within contracts/agreements, requirements that providers of external information system services comply with any organization-specific information security requirements.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that providers of external information system services comply with any organization-specific information security requirements.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-9(a)	CCI-000670	The organization requires that providers of external information system services employ organization-defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The organization being inspected/assessed documents within contracts/agreements, the requirement that providers of external information system services employ security controls defined in CNSSI 1253. DoD has defined the security controls as security controls defined by CNSSI 1253.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that providers of external information system services employ security controls defined in CNSSI 1253. DoD has defined the security controls as security controls defined by CNSSI 1253.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-9(b)	CCI-000671	The organization defines government oversight with regard to external information system services.	The organization being inspected/assessed must define in the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) the government oversight to be conducted on external information system services and service provider.	The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly defined the government oversight to be conducted on external information system services and service providers.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-9(b)	CCI-000672	The organization documents government oversight with regard to external information system services.	The organization being inspected/assessed must establish in the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) the government oversight to be conducted on external information system services and service provider.	The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly established the government oversight to be conducted on external information system services and service providers.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-9(b)	CCI-000673	The organization defines user roles and responsibilities with regard to external information system services.	The organization being inspected/assessed must define in the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) the roles and responsibilities of all types of users of the external information system services.	The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly defined the roles and responsibilities of all types of users of the external information system services.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-9(b)	CCI-000674	The organization documents user roles and responsibilities with regard to external information system services.	The organization being inspected/assessed must establish in the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) the roles and responsibilities of all types of users of the external information system services.	The organization conducting the inspection/assessment obtains and examines the official documentation governing the provision of the external IT services (e.g. contract, MOU, MOA, SLA, etc.) to confirm the organization has clearly established the roles and responsibilities of all types of users of the external information system services.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-10(c)	CCI-000692	The organization requires the developer of the information system, system component, or information system service to implement only organization-approved changes to the system, component, or service.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service implement only organization-approved changes to the system, component, or service throughout its life cycle.	The organization conducting the inspection/assessment obtains and examines contracts/agreements between the organization and the IS developer to confirm the organization has established in its acquisition contracts/agreements the requirement that the IS developer implement only organization-approved changes to the system, component, or service throughout its life cycle.	MOD		X	X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-10(d)	CCI-000694	The organization requires the developer of the information system, system component, or information system service to document approved changes to the system, component, or service.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service document approved changes to the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document approved changes to the system, component, or service.	MOD		X	X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-10(1)	CCI-000698	The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service enable integrity verification of software and firmware components. The organization being inspected/assessed requires the developer to enable integrity verification of software and firmware that may include: 1. Stipulating and monitoring logical delivery of products and services, requiring downloading from approved, verification-enhanced sites; 2. Encrypting elements (software, software patches, etc.) and supply chain process data in transit (motion) and at rest throughout delivery; 3. Requiring suppliers to provide their elements "secure by default", so that additional configuration is required to make the element insecure; 4. Implementing software designs using programming languages and tools that reduce the likelihood of weaknesses; 5. Implementing cryptographic hash verification; and 6. Establishing performance and sub-element baseline for the system and system elements to help detect unauthorized tampering/modification during repairs/refurbishing.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service enable integrity verification of software and firmware components.	MOD			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-12	CCI-000722	The organization defines the security safeguards to employ to protect against supply chain threats to the information system, system component, or information system service.	DoD has defined the requirements to protect against supply chain threats in DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements to protect against supply chain threats in DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)."	MOD			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-12	CCI-000723	The organization protects against supply chain threats to the information system, system component, or information system service by employing organization-defined security safeguards as part of a comprehensive, defense-in-breadth information security strategy.	The organization being inspected/assessed must identify and document in the Security Plan whether the system is a "covered system" IAW DoDI 5200.44. If it is a covered system, the organization must implement the requirements below: 1. Conduct a criticality analysis to identify mission critical functions and critical components and reduce the vulnerability of such functions and components through secure system design; 2. Request threat analysis of suppliers of critical components from the TSN focal point and manage access to and control of threat analysis products containing U.S. person information; 3. Engage TSN focal points for guidance on managing identified risk using DoD Components and Enterprise risk management resources; and 4. Apply TSN best practices, processes, techniques, and procurement tools prior to the acquisition of critical components or their integration into applicable systems, at any point in the system lifecycle. Such tools and practices include contract requirements and the SCRM key practices Guide.	The organization conducting the inspection/assessment obtains and examines the Security Plan for the system to determine whether the system is a "covered system" IAW DoDI 5200.44. If it is a covered system, the organization conducting the inspection/assessment obtains and examines documentation of compliance with DoDI 5200.44, to ensure the organization being inspected/assessed has: 1. Conducted a criticality analysis to identify mission critical functions and critical components and reduced the vulnerability of such functions and components through secure system design; 2. Requested threat analysis of suppliers of critical components from the TSN focal point and managed access to and control of threat analysis products containing U.S. person information; 3. Engaged TSN focal points for guidance on managing identified risk using DoD Components and Enterprise risk management resources; and 4. Applied TSN best practices, processes, techniques, and procurement tools prior to the acquisition of critical components or their integration into applicable systems, at any point in the system lifecycle. Such tools and practices include contract requirements and the SCRM key practices Guide.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-1(a)(1)	CCI-000756	The organization develops and documents an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoD developed DoDI 8520.02 and DoDI 8520.03 as the identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-1(a)(1)	CCI-000757	The organization disseminates to organization defined personnel or roles an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoD disseminates the DoDI 8520.02 and DoDI 8520.03 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) to the ISSO and ISSM and others as the local organization deems appropriate as an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03. DoD has defined the personnel or roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. DoD has defined the personnel or roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-1(b)(1)	CCI-000758	The organization reviews and updates identification and authentication policy in accordance with the organization defined frequency.	DoD reviews and updates identification and authentication policy (DoDI 8520.02 and DoDI 8520.03) annually. DoD Components are automatically compliant with this CCI because they are covered at the DoD level policies, DoDI 8520.02 and DoDI 8520.03. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-1(b)(1)	CCI-000759	The organization defines a frequency for reviewing and updating the identification and authentication policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IA-1(a)(2)	CCI-000760	The organization develops and documents procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	DoD develops within DoDI 8520.02 and DoDI 8520.03, procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-1(a)(2)	CCI-000761	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	DoD disseminates the DoDI 8520.02 and DoDI 8520.03 to the ISSO and ISSM and others as the local organization deems appropriate via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html). DoDI 8520.02 and DoDI 8520.03 are procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. DoD has defined the personnel or roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-1(b)(2)	CCI-000762	The organization reviews and updates identification and authentication procedures in accordance with the organization defined frequency.	DoD reviews and updates identification and authentication procedures (DoDI 8520.02 and DoDI 8520.03) annually. The organization being inspected/assessed is automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03. DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-1(b)(2)	CCI-000763	The organization defines a frequency for reviewing and updating the identification and authentication procedures.	DoD has defined the frequency as review annually - update as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as review annually - update as appropriate.	LOW	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IA-2	CCI-000764	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	The organization being inspected/assessed configures the information system to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 764.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 764.	LOW	X	X		X				3.3.1 User Accounts 3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION"within Part 3
N/A	IA-2(1)	CCI-000765	The information system implements multifactor authentication for network access to privileged accounts.	The organization being inspected/assessed configures the information system to implement multifactor authentication for network access to privileged accounts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 765.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement multifactor authentication for network access to privileged accounts. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 765.	LOW	X	X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity requirements are met for user accounts (withing device capabilities) within Sub-Paragraph "USER IDENTIFICATION AND AUTHENTICATION" within Part 3
N/A	IA-2(2)	CCI-000766	The information system implements multifactor authentication for network access to non-privileged accounts.	The organization being inspected/assessed configures the information system to implement multifactor authentication for network access to non-privileged accounts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 766.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement multifactor authentication for network access to non-privileged accounts. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 766.	MOD	X	X		X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	IA-2(3)	CCI-000767	The information system implements multifactor authentication for local access to privileged accounts.	The organization being inspected/assessed configures the information system to implement multifactor authentication for local access to privileged accounts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 767.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement multifactor authentication for local access to privileged accounts. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 767.	MOD	X	X		X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enriched	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-2(4)	CCI-000768	The information system implements multifactor authentication for local access to non-privileged accounts.	The organization being inspected/assessed configures the information system to implement multifactor authentication for local access to non-privileged accounts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 768.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement multifactor authentication for local access to non-privileged accounts. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 768.	MOD		X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI requirements are addressed within subparagraph "USER IDENTIFICATION AND AUTHENTICATION" of UFGS 25 05 11.
N/A	IA-2(5)	CCI-000770	The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.	The organization being inspected/assessed requires individuals or configures the information system to require individuals to be authenticated with an individual authenticator when a group authenticator is employed. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 770.	The organization conducting the inspection/assessment obtains and examines standard operating procedures or system documentation to ensure the organization being inspected/assessed requires individuals to be authenticated with an individual authenticator when a group authenticator is employed. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 770.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-3	CCI-000777	The organization defines a list of specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system.	DoD has defined the value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	LOW	X	X		X	X			1.9.4 Control System Inventory Report 3.2.7 Device Identification and Authentic...		Cybersecurity requirement is met by requiring the contractor to document the inventory of components within the control system and submit a Control System Inventory Report. This design requirement is captured in Sub-Paragraph "Control System Inventory Report" within Part 1 and "Device Identification and Authentication" within Part 3
N/A	IA-3	CCI-000778	The information system uniquely identifies an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.	The organization being inspected/assessed configures the network infrastructure to identify all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 778. DoD has defined the value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	The organization conducting the inspection/assessment examine a sampling of the network infrastructure device configurations to ensure devices connecting to the infrastructure are uniquely identified. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 778.	LOW	X	X		X				1.9.4 Control System Inventory Report 3.2.7 Device Identification and Authentic...		Cybersecurity requirement is met by requiring the contractor to document the inventory of components within the control system and submit a Control System Inventory Report. This design requirement is captured in Sub-Paragraph "Control System Inventory Report" within Part 1 and "Device Identification and Authentication" within Part 3
N/A	IA-4(e)	CCI-000794	The organization defines a time period of inactivity after which the identifier is disabled.	DoD has defined the time period as 35 days of inactivity.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 35 days of inactivity.	LOW	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IA-4(e)	CCI-000795	The organization manages information system identifiers by disabling the identifier after an organization defined time period of inactivity.	The organization being inspected/assessed configures the information system to disable identifiers after 35 days of inactivity. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 795. DoD has defined the time period as 35 days of inactivity.	The organization conducting the inspection/assessment examines the information system configuration to ensure that identifiers are disabled after 35 days of inactivity. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 795. DoD has defined the time period as 35 days of inactivity.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-4(4)	CCI-000800	The organization defines characteristics for identifying individual status.	DoD has defined the characteristics as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the characteristics as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil	MOD			X		X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-4(4)	CCI-000801	The organization manages individual identifiers by uniquely identifying each individual as organization-defined characteristic identifying individual status.	The organization being inspected/assessed documents and implements a process to manage individual identifiers by uniquely identifying each individual as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil. DoD has defined the characteristics as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages individual identifiers by uniquely identifying each individual as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil. DoD has defined the characteristics as contractor or government employee and by nationality. User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil.	MOD			X		X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-7	CCI-000803	The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	The organization being inspected/assessed configures the information system to implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 803.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 803.	LOW	X	X		X				3.2.8 Cryptographic Module Authentication		Cybersecurity requirements are met in "Cryptographic Module Authentication"
N/A	IA-8	CCI-000804	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	The organization being inspected/assessed configures the information system to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 804.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 804.	LOW	X			X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	IR-1(a)(1)	CCI-000805	The organization develops and documents an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	LOW					X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-1(a)(1)	CCI-000806	The organization disseminates an incident response policy to organization-defined personnel or roles.	DoD disseminates via http://www.dtic.mil/cjcs_directives/, CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 to all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	LOW					X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-1(b)(1)	CCI-000807	The organization reviews and updates the current incident response policy in accordance with organization-defined frequency.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-1(b)(1)	CCI-000808	The organization defines the frequency to review and update the current incident response policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of issuance.	LOW					X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IR-1(a)(2)	CCI-000809	The organization develops and documents procedures to facilitate the implementation of the incident response policy and associated incident response controls.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meets the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-1(a)(2)	CCI-000810	The organization disseminates incident response procedures to organization-defined personnel or roles.	DoD disseminates via http://www.dtic.mil/cjcs_directives/, CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 to all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-1(b)(2)	CCI-000811	The organization reviews and updates the current incident response procedures in accordance with organization-defined frequency.	DoD (in conjunction with Joint Staff for CJCSIs) reviews and updates current incident response procedures (CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2) annually. DoD Components are automatically compliant with this CCI because they are covered at the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. DoD has defined the frequency as reviewed annually - updated as appropriate.	CJCSI 6510.01F "Information Assurance and Support to Computer Network Defense," CJCSM 6510.01B, "Cyber Incident Handling Program," DoDD O-8530.1, and DoDI O-8530.2 meet the DoD requirements for incident response policy and procedures. DoD Components are automatically compliant with this CCI because they are covered at the DoD level with the following policies: CJCSI 6510.01F, CJCSM 6510.01B, DoDD O-8530.1, and DoDI O-8530.2. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-1(b)(2)	CCI-000812	The organization defines the frequency to review and update the current incident response procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-2(a)	CCI-000813	The organization provides incident response training to information system users consistent with assigned roles and responsibilities within an organization-defined time period of assuming an incident response role or responsibility.	The organization being inspected/assessed documents and implement a process to provide incident response training to information system users consistent with assigned roles and responsibilities within 30 working days of assuming an incident response role or responsibility. The organization must maintain a record of training. DoD has defined the time period as 30 working days.	The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of information system users to ensure the organization being inspected/assessed provides incident response training to information system users consistent with assigned roles and responsibilities within 30 working days of assuming an incident response role or responsibility. DoD has defined the time period as 30 working days.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-2(c)	CCI-000814	The organization provides refresher incident response training in accordance with organization-defined frequency.	The organization being inspected/assessed documents and implements a process to provide incident response training to information system users, other than general users, consistent with assigned roles and responsibilities annually. For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training. The organization must maintain a record of training. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of information system users to ensure the organization being inspected/assessed provides incident response training to information system users, other than general users, consistent with assigned roles and responsibilities annually. For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-2(c)	CCI-000815	The organization defines a frequency for refresher incident response training.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-3	CCI-000818	The organization tests the incident response capability for the information system on an organization-defined frequency using organization-defined tests to determine the incident response effectiveness.	The organization being inspected/assessed documents and implements a process to test its incident response capability for the information system at least every six months for high availability and at least annually for low/med availability using tests and as defined in the incident response plan. The organization must maintain a record of test results. DoD has defined the frequency as at least every six months for high availability and at least annually for low/med availability. DoD has defined the tests as tests as defined in the incident response plan.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of test results to ensure the organization being inspected/assessed tests its incident response capability for the information system at least every six months for high availability and at least annually for low/med availability using tests and as defined in the incident response plan. DoD has defined the frequency as at least every six months for high availability and at least annually for low/med availability. DoD has defined the tests as tests as defined in the incident response plan.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IR-3	CCI-000819	The organization defines a frequency for incident response tests.	DoD has defined the frequency as at least every six months for high availability and at least annually for low/med availability.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least every six months for high availability and at least annually for low/med availability.	MOD					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-3	CCI-000820	The organization defines tests for incident response.	DoD has defined the tests as tests as defined in the incident response plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the tests as tests as defined in the incident response plan.	MOD					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-4(a)	CCI-000822	The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	The organization being inspected/assessed must have a documented and certified CNDSP and documented procedures for information system users and site security personnel to handle incidents until they are transferred to the responsibility of the CNDSP.	The organization conducting the inspection/assessment obtains and examines the documentation identifying the CNDSP leveraged as well as the documented procedures for incident handling to ensure that there is a certified CNDSP in use and that there are procedures implemented to handle incidents until they are transferred to the responsibility of the CNDSP.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-4(b)	CCI-000823	The organization coordinates incident handling activities with contingency planning activities.	The organization being inspected/assessed will coordinate the incident response plan (IR-8) and contingency plan (CP-2) to ensure they allow for an effective transfer of information system activity and maintain confidentiality and integrity of the contigency assets.	The organization conducting the inspection/assessment obtains and examines the incident response plan (IR-8) and contingency plan (CP 2) to ensure they allow for an effective transfer of information system activity and maintain confidentiality and integrity of the contigency assets.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-4(c)	CCI-000824	The organization incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises.	The organization being inspected/assessed will conduct after action reviews from incidents to identify lessons learned and will incorporate them into procedures, training, and testing/exercises. The organization must maintain records of after action reviews.	The organization conducting the inspection/assessment obtains and examines after action reports or meeting minutes to identify actionable lessons learned to verify that lessons learned are incorporated into the plan as changes are necessary.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-4(1)	CCI-000825	The organization employs automated mechanisms to support the incident handling process.	The organization being inspected/assessed will document within their incident handling plan, procedures to leverage the Joint Incident Management System (JIMS). For the DoD, JIMS is the automated mechanism.	The organization conducting the inspection/assessment obtains and examines the incident handling plan to ensure that there are procedures identified to leverage the JIMS.	MOD			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	IR-4(3)	CCI-000827	The organization defines and identifies classes of incidents for which organization-defined actions are to be taken to ensure continuation of organizational mission and business functions.	CJCSM 6510.01B has already identified DoD's classes of incidents. DoD Components are automatically compliant with this CCI because DoD has defined the classes of incidents as classes of incidents defined in CJCSM 6510.01B Appendix A- Enclosure B.	CJCSM 6510.01B has already identified DoD's classes of incidents. The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the classes of incidents as classes of incidents defined in CJCSM 6510.01B Appendix A- Enclosure B.6510.01M	MOD			X		X			---	CS are not business systems	
N/A	IR-4(3)	CCI-000828	The organization defines and identifies actions to take in response to organization-defined classes of incidents to ensure continuation of organizational missions and business functions.	CJCSM 6510.01B has already identified DoD's actions to take in response to classes of incidents. DoD Components are automatically compliant with this CCI because DoD has defined the actions as actions defined in CJCSM 6510.01B.	CJCSM 6510.01B has already identified DoD's actions to take in response to classes of incidents. The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the actions as actions defined in CJCSM 6510.01B.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-4(4)	CCI-000829	The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	The organization being inspected/assessed defines procedures to examine incident information gathered and the actual actions taken by both the individuals affected and the incident response personnel. These procedures shall be defined IAW CJCSM 6510.01B. The end goal is to achieve a top level perspective of the effectiveness of the incident response and awareness.	The organization conducting the inspection/assessment obtains and examines proof of the analysis (such as minutes from an incident response after action meeting or other similar activity) to ensure that incident information is being examined and correlated.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-5	CCI-000832	The organization tracks and documents information system security incidents.	The organization being inspected/assessed will document within their incident handling plan, procedures to leverage the Joint Incident Management System (JIMS). For the DoD, JIMS is the automated mechanism.	The organization conducting the inspection/assessment obtains and examines the incident handling plan to ensure that there are procedures identified to leverage the JIMS.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-6(a)	CCI-000834	The organization defines a time period for personnel to report suspected security incidents to the organizational incident response capability.	DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance. If organizations decide to be more restrictive than the guidance in the CJCSM, then they should address the more restrictive response time requirements in their incident response plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance. The organization conducting the inspection/assessment obtains and examines the incident response plan to determine if more stringent response time requirements have been identified.	LOW			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-6(a)	CCI-000835	The organization requires personnel to report suspected security incidents to the organizational incident response capability within the organization-defined time period.	The organization being inspected/assessed documents within the user agreement the requirement for all system users to report suspected security incidents to the organizational incident response capability within the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance. DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance.	The organization conducting the inspection/assessment obtains and examines the user agreement to ensure users are required to report suspected security incidents to the organizational incident response capability within the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance. DoD has defined the time period as the timeframes specified by CJCSM 6510.01B (Table C-A-1) unless the data owner provides more restrictive guidance.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IR-6(b)	CCI-000836	The organization reports security incident information to organization-defined authorities.	The organization being inspected/assessed documents and implements a process to report to the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).any security incidents IAW the incident response plan (IR-8). Reporting shall be conducted IAW CJCSM 6510.01B. DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).	The organization conducting the inspection/assessment obtains and examines a sample of previous security incidents to ensure the incidents were reported to the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT). any security incidents IAW the incident response plan (IR-8). Reporting shall be conducted IAW CJCSM 6510.01B. DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-6(1)	CCI-000837	The organization employs automated mechanisms to assist in the reporting of security incidents.	The organization being inspected/assessed will document within their incident handling plan, procedures to leverage the Joint Incident Management System (JIMS). For the DoD, JIMS is the automated mechanism.	The organization conducting the inspection/assessment obtains and examines the incident handling plan to ensure that there are procedures identified to leverage the JIMS.	MOD			X					---	CS are not business systems	
N/A	IR-6(2)	CCI-000838	The organization reports information system vulnerabilities associated with reported security incidents to organization-defined personnel or roles.	The organization being inspected/assessed documents and implements a process to report to personnel defined in IR-6 (2), CCI 2792 information system vulnerabilities associated with reported security incident IAW the incident response plan (IR 8). Reporting shall be conducted IAW CJCSM 6510.01B.	The organization conducting the inspection/assessment obtains and examines a sample of previous security incidents to ensure the associated vulnerabilities were reported to personnel defined in IR-6 (2), CCI 2792 IAW the incident response plan (IR-8). Reporting shall be conducted IAW CJCSM 6510.01B.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-7	CCI-000839	The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	The organization being inspected/assessed will establish an incident response support service, analogous to an IT help desk, to provide advice and assistance to users for handling and reporting of security incidents.	The organization conducting the inspection/assessment will interview organizational users to determine awareness of incident response support services and quality of assistance of those services when used. If interviewing organizational users is not feasible, then review users manuals/documentation to ensures it identifies an incident response support service to contact.	LOW			X					---	CS are not business systems	
N/A	IR-7(1)	CCI-000840	The organization employs automated mechanisms to increase the availability of incident response-related information and support.	The organization being inspected/assessed will implement an automated intra-organization incident response information sharing capability to provide the following incident related information and support, for example: 1. SOP for incident reporting 2. Incident handling FAQ 3. Current incident activity awareness information 4. Incident response contact information 5. Incident report submission	The organization conducting the inspection/assessment obtains and examines the incident response information sharing capability to validate the information sharing capability is available to organizational users.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-7(2)(a)	CCI-000841	The organization establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability.	The organization being inspected/assessed must establish a formal agreement with a computer network defense service provider (CNDSP).	The organization conducting the inspection/assessment obtains and examines the formal agreement document between the organization and CNDSP to validate it is current and valid.	MOD			X					---	CS are not business systems	
N/A	IR-7(2)(b)	CCI-000842	The organization identifies organizational incident response team members to the external providers.	The organization being inspected/assessed must provide and update the list of internal incident response team members as necessary throughout the lifecycle of the CNDSP agreement, in conjunction with the CNDSP agreement.	The organization conducting the inspection/assessment obtains and examines the list of internal incident response team members to validate it is accurate and current. Interviews with CNDSP personnel and organizational incident response team members may also be conducted.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(a)(8)	CCI-000844	The organization develops an incident response plan that is reviewed and approved by organization-defined personnel or roles.	The organization being inspected/assessed will have an incident response plan signed and approved by at a minimum, the ISSM and ISSO. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization conducting the inspection/assessment obtains and examines the incident response plan to validate it has been properly signed by at a minimum, the ISSM and ISSO. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(b)	CCI-000845	The organization defines incident response personnel (identified by name and/or by role) and organizational elements to whom copies of the incident response plan is distributed.	DoD has defined the list as all stakeholders identified in the incident response plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the list as all stakeholders identified in the incident response plan.	LOW				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-8(b)	CCI-000846	The organization distributes copies of the incident response plan to organization-defined incident response personnel (identified by name and/or by role) and organizational elements.	The organization being inspected/assessed makes available to all stakeholders identified in the incident response plan via organizationally approved information sharing mechanism. DoD has defined the list as all stakeholders identified in the incident response plan.	The organization conducting the inspection/assessment obtains and examines organizationally approved information sharing mechanism to validate all stakeholders identified in the incident response plan have adequate access to the incident response plan. DoD has defined the list as all stakeholders identified in the incident response plan.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(c)	CCI-000847	The organization defines the frequency for reviewing the incident response plan.	DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).	LOW				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-8(c)	CCI-000848	The organization reviews the incident response plan on an organization-defined frequency.	The organization being inspected/assessed will conduct reviews of its incident response plan at least annually. DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).	The organization conducting the inspection/assessment obtains and examines the incident response plan to validate it is current and has been reviewed within the last year. DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).	LOW				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-8(d)	CCI-000849	The organization updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	The organization being inspected/assessed must update the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing and incorporate lessons learned from past incidents (IR-4a). The organization must document the update actions as an audit trail.	The organization conducting the inspection/assessment obtains and examines documentation of the update actions for the incident response plan to ensure the organization is updating the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing and incorporating lessons learned from past incidents (IR-4a).	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(e)	CCI-000850	The organization communicates incident response plan changes to organization-defined incident response personnel (identified by name and/or by role) and organizational elements.	The organization being inspected/assessed communicates incident response plan changes to all stakeholders identified in the incident response plan, not later than 30 days after the change is made. DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made.	The organization conducting the inspection/assessment examines the incident response plan via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been communicated to all stakeholders identified in the incident response plan, not later than 30 days after the change is made. DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	MA-1(b)(1)	CCI-000851	The organization defines the frequency to review and update the current system maintenance policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.	LOW				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	MA-1(a)(1)	CCI-000852	The organization develops and documents a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization being inspected/assessed develops and documents a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	The organization conducting the inspection/assessment obtains and examines the documented maintenance policy to ensure the organization being inspected/assessed develops and documents a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-1(a)(1)	CCI-000853	The organization disseminates to organization-defined personnel or roles a system maintenance policy.	The organization being inspected/assessed ensures the maintenance policy is disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	The organization conducting the inspection/assessment obtains and examines the maintenance policy via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-1(b)(1)	CCI-000854	The organization reviews and updates the current system maintenance policy in accordance with organization-defined frequency.	The organization being inspected/assessed reviews the current system maintenance policy every 5 years and revises as necessary to comply with DoD regulations. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as every 5 years.	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the maintenance policy to ensure review is occurring every 5 years and updates are made as necessary. DoD has defined the frequency as every 5 years.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-1(a)(2)	CCI-000855	The organization develops and documents procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.	The organization being inspected/assessed documents the maintenance procedures within the Security Plan. The maintenance procedures shall be developed IAW maintenance policy provided in DoDI 8500.01..	The organization conducting the inspection/assessment obtains and examines the Security Plan to ensure maintenance procedures are documented and are developed IAW maintenance policy provided in DoDI 8500.01..	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-1(a)(2)	CCI-000856	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.	The organization being inspected/assessed ensures the maintenance procedures are disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system via an information sharing capability. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	The organization conducting the inspection/assessment examines the maintenance procedures via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-1(b)(2)	CCI-000857	The organization reviews and updates the current system maintenance procedures in accordance with organization-defined frequency.	The organization being inspected/assessed reviews the current system maintenance procedures annually and revises as needed to comply with DoD regulations. The organization must document each occurrence of the reviews and update actions as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the maintenance procedures to ensure annual review and necessary updates are occurring. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(b)	CCI-000859	The organization approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.	The organization being inspected/assessed approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. The organization must maintain records of all approvals and monitoring activities.	The organization conducting the inspection/assessment obtains and examines records of all approvals and monitoring activities to ensure the organization being inspected/assessed approves and monitors all maintenance activities whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(c)	CCI-000860	The organization requires that organization-defined personnel or roles explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.	The organization being inspected/assessed documents within their risk management strategy personnel or roles defined in MA-2, CCI 2874 who must explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs. The organization must maintain written records of approval for the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.	The organization conducting the inspection/assessment obtains and examines: 1. the organization's risk management strategy to ensure the personnel or roles defined in MA-2, CCI 2874 have been designated to approve the removal of the information system or system components; 2. and written records of approval for the removal of the information system or system components from organizational facilities for off-site maintenance or repairs to ensure the removal is explicitly approved.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(d)	CCI-000861	The organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.	The organization being inspected/assessed sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs IAW DoDM 5200.01-V3 for classified media and DoDM 5200.01-V4 for unclassified media. The organization must maintain written records of media sanitization.	The organization conducting the inspection/assessment obtains and examines written records of media sanitization to ensure the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.	LOW			X					---	CS are not business systems	
N/A	MA-2(e)	CCI-000862	The organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	The organization being inspected/assessed identifies and documents the impacted security controls and takes steps to verify that the controls are still functioning properly following maintenance or repair actions.	The organization conducting the inspection/assessment obtains and examines documented evidence of the verification of security controls following maintenance and repair actions to ensure that the organization being inspected/assessed checks all potentially impacted security controls to verify that they are still functioning properly.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	MA-3	CCI-000865	The organization approves information system maintenance tools.	The organization being inspected/assessed documents the approved maintenance tools within the Security Plan.	The organization conducting the inspection/assessment: 1. obtains and examines the Security Plan to ensure the list of approved maintenance tools is documented; 2. ensures only the approved maintenance tools are used within the system.	MOD		X	X					3.9 SYSTEM MAINTENANCE TOOL SOFTWARE		CCI requirements are addressed within subparagraph "System Maintenance Tool Software" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	MA-3	CCI-000866	The organization controls information system maintenance tools.	The organization being inspected/assessed controls information system maintenance tools that are approved IAW MA-3, CCI 865.	The organization conducting the inspection/assessment: 1. obtains and examines the Security Plan to identify the list of approved maintenance tools; 2. ensures the organization being inspected/assessed controls the approved information system maintenance tools.	MOD			X	X				---	CS are not business systems	
N/A	MA-3	CCI-000867	The organization monitors information system maintenance tools.	The organization being inspected/assessed develops and implements procedures to monitor the use of the approved information system maintenance tools IAW MA-3, CCI 865. Records of monitoring activity must be maintained.	The organization conducting the inspection/assessment obtains and examines: 1. the Security Plan to identify the list of approved maintenance tools; and 2. documented procedures to identify how the use of maintenance tools is monitored; and 3. reviews evidence that the monitoring is conducted IAW the documented procedures.	MOD			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	MA-3(1)	CCI-000869	The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	The organization being inspected/assessed documents the procedures for and implements inspections of the maintenances tools carried into a facility by maintenance personnel for improper or unauthorized modifications. Records of inspection must be maintained.	The organization conducting the inspection/assessment obtains and examines procedures for, and records of inspection of the maintenance tools carried into a facility by maintenance personnel to ensure the tools are inspected for improper or unauthorized modifications.	MOD			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	MA-3(2)	CCI-000870	The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.	The organization being inspected/assessed: 1. documents and implements procedures to check all media containing diagnostic and test programs for malicious code before the media are used in the information system; and 2. Runs an automated tool set to check all media containing diagnostic and test programs for malicious code before the media are used in the information system. The organization must maintain configuration files for the automated tool set and audit logs of the tool set used to check media.	The organization conducting the inspection/assessment obtains and examines the procedures for checking all diagnostic and test media for malicious code, and a sampling of configuration files and audit logs of the tool set used to check media. The purpose of the review is to ensure the organization being inspected/assessed checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(a)	CCI-000873	The organization approves nonlocal maintenance and diagnostic activities.	The organization being inspected/assessed documents the procedures for approving non-local maintenance and diagnostic activities within the Security Plan. The organization must maintain records of approved non-local maintenance and diagnostic activities.	The organization conducting the inspection/assessment obtains and examines: 1. the Security Plan to ensure the procedures for approving non-local maintenance and diagnostic activities are documented; and 2. records approving non-local maintenance and diagnostic activities.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(a)	CCI-000874	The organization monitors nonlocal maintenance and diagnostic activities.	The organization being inspected/assessed develops and implements procedures to monitor non-local maintenance and diagnostic activities. Records of monitoring activity must be maintained.	The organization conducting the inspection/assessment obtains and examines: 1. the Security Plan to identify the authorized non-local maintenance and diagnostic activities; and 2. documented procedures to identify how the use of non-local maintenance and diagnostic activities are monitored; and 3. reviews evidence that the monitoring is conducted IAW the documented procedures.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(b)	CCI-000876	The organization allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system.	The organization being inspected/assessed: 1. documents within the Security Plan the non-local maintenance and diagnostic tools that are allowed; and 2. allows the use of non-local maintenance and diagnostic tools IAW the tools identified in the Security Plan and MA-4, CCI 873.	The organization conducting the inspection/assessment obtains and examines: 1. the Security Plan to ensure non-local maintenance and diagnostic tools have been identified; and 2. maintenance records to ensure only those tools allowed are used IAW MA-4, CCI 873.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(c)	CCI-000877	The organization employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.	The organization being inspected/assessed configures the information system to employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 877.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 877.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(d)	CCI-000878	The organization maintains records for nonlocal maintenance and diagnostic activities.	The organization being inspected/assessed maintains records of authorized non-local maintenance and diagnostic activities.	The organization conducting the inspection/assessment obtains records of authorized non-local maintenance and diagnostic activities, and examines a sampling to verify the organization is maintaining records for all non-local maintenance and diagnostic activities.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(e)	CCI-000879	The organization terminates sessions and network connections when nonlocal maintenance is completed.	The organization being inspected/assessed terminates session and network connections when non-local maintenance is completed. The organization must retain audit logs of session and network connections termination for non-local maintenance.	The organization conducting the inspection/assessment obtains and examines audit logs of session and network connections termination for non-local maintenance to ensure session and network connections are terminated when non-local maintenance is completed.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(2)	CCI-000881	The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.	The organization being inspected/assessed documents within the Security Plan the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.	The organization conducting the inspection/assessment obtains and examines the Security Plan to ensure the plan identifies the establishment and use of non-local maintenance and diagnostic connections.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(3)(a)	CCI-000882	The organization requires that nonlocal maintenance and diagnostic services to be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced.	The organization being inspected/assessed clearly defines in its contracts and/or service level agreements the requirement that any IS used to conduct non-local maintenance and diagnostic services will have a security level at least as high as the security level implemented on the IS being serviced. Alternatively, the organization being inspected/assessed complies with MA-4 (3) CCIs 883 and 1631.	The organization conducting the inspection/assessment obtains and examines contracts and/or service level agreements for all non-local maintenance and diagnostic services to ensure that any IS used for those services is required to have security level at least as high as the security level implemented on the IS being serviced. Alternatively, the organization conducting the inspection/assessment ensures the organization being inspected/assessed complies with MA-4 (3) CCIs 883 and 1631.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	MA-4(3)(b)	CCI-000883	The organization removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities.	The organization being inspected/assessed removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities. Alternatively, the organization being inspected/assessed complies with MA-4 (3) CCI 882.	The organization conducting the inspection/assessment obtains and examines maintenance procedures for all non-local maintenance and diagnostic services to ensure that the organization being inspected/assessed sanitizes components before removal from organizational facilities. Alternatively, the organization conducting the inspection/assessment ensures the organization being inspected/assessed complies with MA-4 (3) CCI 882.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-5(a)	CCI-000890	The organization establishes a process for maintenance personnel authorization.	The organization being inspected/assessed clearly defines, documents, and establishes a process for the authorization of maintenance personnel.	The organization conducting the inspection/assessment obtains and examines procedures addressing maintenance personnel to ensure that the organization being inspected/assessed has established processes for the authorization of maintenance personnel.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-5(a)	CCI-000891	The organization maintains a list of authorized maintenance organizations or personnel.	The organization being inspected/assessed maintains a current list of authorized maintenance organizations or personnel.	The organization conducting the inspection/assessment obtains and examines the current list of authorized maintenance organizations or personnel to ensure the organization being inspected/assessed is maintaining the list.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-6	CCI-000903	The organization obtains maintenance support and/or spare parts for organization-defined information system components within an organization-defined time period of failure.	The organization being inspected/assessed obtains maintenance support and/or spare parts for information system components defined in MA-6, CCI 2896 within 24 hours (Low and Moderate Availability) or immediately upon failure for (High Availability). DoD has defined the time period as within 24 hours (Low and Moderate Availability) or immediately upon failure for (High Availability).	The organization conducting the inspection/assessment obtains evidence that maintenance support is available for information system components defined in MA-6, CCI 2896 and that the support will be provided within 24 hours (Low and Moderate Availability) or immediately upon failure for (High Availability). Evidence can include maintenance support contracts, inventories of spare parts, etc. DoD has defined the time period as within 24 hours (Low and Moderate Availability) or immediately upon failure for (High Availability).	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-1(a)(1)	CCI-000904	The organization develops and documents a physical and environment protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-1(a)(1)	CCI-000905	The organization disseminates a physical and environmental protection policy to organization-defined personnel or roles.	DoD disseminates DoDI 5200.08 and DoD 5200.08-R organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html DoD has defined the personnel or roles as organizational personnel with physical and environmental protection responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 5200.08 and DoD 5200.08-R DoD has defined the personnel or roles as organizational personnel with physical and environmental protection responsibilities.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-1(b)(1)	CCI-000906	The organization reviews and updates the current physical and environmental protection policy in accordance with organization-defined frequency.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-1(b)(1)	CCI-000907	The organization defines the frequency to review and update the physical and environmental protection policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW				X				---	CS are not business systems	
N/A	PE-1(a)(2)	CCI-000908	The organization develops and documents procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-1(a)(2)	CCI-000909	The organization disseminates physical and environmental protection procedures to organization-defined personnel or roles.	DoD disseminates DoDI 5200.08 and DoD 5200.08-R organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html DoD has defined the personnel or roles as organizational personnel with physical and environmental protection responsibilities.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 5200.08 and DoD 5200.08-R DoD has defined the personnel or roles as organizational personnel with physical and environmental protection responsibilities.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-1(b)(2)	CCI-000910	The organization reviews and updates the current physical and environmental protection procedures in accordance with organization-defined frequency.	DoDI 5200.08 and DoD 5200.08-R meet the requirement for Physical and Environmental Policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R. DoD has defined the frequency as reviewed annually - updated as appropriate.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.08 and DoD 5200.08-R. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-1(b)(2)	CCI-000911	The organization defines the frequency to review and update the physical and environmental protection procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW				X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PE-2(a)	CCI-000912	The organization develops a list of individuals with authorized access to the facility where the information system resides.	The organization being inspected/assessed will develop and maintain a list of personnel with authorized access to the facilities where information systems reside. The organization will also take action to identify and officially designate its publicly accessible areas where access authorization is not required.	The organization conducting the inspection/assessment obtains and examines the list of personnel with authorized access to facilities where information systems reside to ensure it is current within every 90 days. The review process should also determine if the organization has identified and officially designated its publicly accessible areas where access authorization is not required. DoD has defined the frequency as every 90 days.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-2(b)	CCI-000913	The organization issues authorization credentials for facility access.	The organization being inspected/assessed utilizes the list of personnel with authorized access (IAW PE-2, CCI-000912) and issues credentials accordingly. The organization must document the credential issuing activity as an audit trail.	The organization conducting the inspection/assessment obtains and examines documentation of credential issuing activities to ensure credentials are issued to personnel with authorized access.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-2(c)	CCI-000914	The organization reviews the access list detailing authorized facility access by individuals in accordance with organization-defined frequency.	The organization being inspected/assessed will review the access list and authorization credentials every 90 days and document these review and approval actions as an audit trail. DoD has defined the frequency as every 90 days.	The organization conducting the inspection/assessment obtains and examines the audit records of the review actions to ensure that reviews are conducted every 90 days. DoD has defined the frequency as every 90 days.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-2(c)	CCI-000915	The organization defines the frequency to review the access list detailing authorized facility access by individuals.	DoD has defined the frequency as every 90 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 90 days.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-3(a)	CCI-000919	The organization enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides.	The organization being inspected/assessed will implement physical access authorizations at entry/exit points defined in PE-3, CCI 2915 and secure those physical access points (i.e. doors and/or windows) that are not intended for normal access.	The organization conducting the inspection/assessment performs a physical inspection of facility entry/exit points defined in PE-3, CCI 2915 to ensure that either physical access authorization controls are in place for those access points considered normal access points or are properly secured. Physical access points that are not documented or are not secured would be a failure of this control.	LOW			X	X				---	CS are not business systems	
N/A	PE-3(a)(1)	CCI-000920	The organization verifies individual access authorizations before granting access to the facility.	The organization being inspected/assessed verifies and grants access to facilities based upon individual access authorizations.	The organization conducting the inspection/assessment obtains and examines the access authorization list of personnel that have access to the facility (per access list implemented through PE-2, CCI 000912) where the information system resides. Inspect selected facilities to confirm the inspected organization is granting access at all physical access points to only authorized personnel.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-3(a)(2)	CCI-000921	The organization controls ingress/egress to the facility using one or more organization-defined physical access control systems/devices or guards.	The organization being inspected/assessed will control ingress/egress to the facility using the physical access control devices and/or guards defined in PE-3, CCI 2916.	The organization conducting the inspection/assessment obtains and examines the list of physical access control devices and/or guards in use defined in PE-3, CCI 2916 and conducts random inspections of entry points. The purpose is to determine whether the organization is using those physical access devices and/or guards to control entry of personnel into the facility hosting the information system.	LOW			X	X				---	CS are not business systems	
N/A	PE-3(e)	CCI-000923	The organization secures keys, combinations, and other physical access devices.	The organization being inspected/assessed will secure as appropriate (in safes or secure containers) items used for physical access control such as keys, combinations, portable locks, etc. Fixed access control devices such as card readers, installed locks, key pads, etc. should be protected from tampering.	The organization conducting the inspection/assessment conducts physical inspections and interviews physical security/safety personnel to validate the organization has taken the proper precautions, and established the proper procedures to ensure it has adequately secured its keys, combinations, and other physical devices.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-3(f)	CCI-000924	The organization inventories organization-defined physical access devices every organization-defined frequency.	The organization being inspected/assessed conducts and documents an inventory of minimally keys or any other physical token used to gain access annually. Inventory documents must be retained for at least one year beyond the completion of the next inventory. DoD has defined the frequency as annually. DoD has defined the physical access devices as minimally keys or any other physical token used to gain access.	The organization conducting the inspection/assessment obtains and examines the records of inventory of minimally keys or any other physical token used to gain access to ensure the inventory is being conducted annually. DoD has defined the frequency as annually. DoD has defined the physical access devices as minimally keys or any other physical token used to gain access.	LOW			X	X				---	CS are not business systems	
N/A	PE-3(f)	CCI-000925	The organization defines the frequency for conducting inventories of organization-defined physical access devices.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW				X	X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-3(g)	CCI-000926	The organization changes combinations and keys in accordance with organization-defined frequency and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.	The organization being inspected/assessed will document each occurrence of these change actions, with the reason for the action, as an audit trail for future reference. DoD has defined the frequency as required by security relevant events.	The organization conducting the inspection/assessment obtains and examines documentation of these change actions to validate the organization is changing its keys and combinations upon occurrence of security relevant events and when keys are lost, combinations are compromised, or individuals are transferred or terminated. DoD has defined the frequency as required by security relevant events.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-3(g)	CCI-000927	The organization defines a frequency for changing combinations and keys.	DoD has defined the frequency as required by security relevant event.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as required by security relevant event.	LOW				X	X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PE-3(1)	CCI-000928	The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at organization-defined physical spaces containing one or more components of the information system.	The organization being inspected/assessed will provide documentation of additional physical access authorizations for the facility/facilities at physical spaces containing one or more components of the information system defined in PE-3 (1), CCI 2926. The organization will ensure that these controls are separate from, and independent of, the physical access controls established for the facility.	The organization conducting the inspection/assessment obtains and examines the documented list of additional physical access authorizations for the facility/facilities at physical spaces containing one or more components of the information system. The objective of the examination is to determine if the organization is enforcing additional physical access authorizations to areas of the facility at physical spaces containing one or more components of the information system defined in PE-3 (1), CCI 2926. These controls are independent of the physical access controls established for the facility.	MOD		X	X					3.3.6 Pysical Security in MODERATE Impact...		CCI requirements are addressed within subparagraph "Physical Security in MODERATE Impact Systems" of UFGS 25 05 11.
N/A	PE-4	CCI-000936	The organization controls physical access to organization-defined information system distribution and transmission lines within organizational facilities using organization-defined security safeguards.	The organization being inspected/assessed controls physical access to information system distribution and transmission lines defined in PE-4, CCI 2930 within organizational facilities using security safeguards defined in PE-4, CCI 2931.	The organization conducting the inspection/assessment inspects the information system distribution and transmission lines defined in PE-4, CCI 2930 to ensure the security safeguards defined in PE-4, CCI 2931 are in place.	MOD		X	X					3.3.6 Pysical Security in MODERATE Impact...		CCI requirements are addressed within subparagraph "Physical Security in MODERATE Impact Systems" of UFGS 25 05 11.
N/A	PE-6(b)	CCI-000939	The organization reviews physical access logs in accordance with organization-defined frequency.	The organization being inspected/assessed will review physical access logs every 30 days. The organization must document each occurrence the physical access log review, with results of any necessary incident analysis and action taken, as an audit trail for future reference. DoD has defined the frequency as every 30 days.	The organization conducting the inspection/assessment obtains and examines the inspected organization's physical access logs or records; physical access incident reports; and any other relevant documents or records. The purpose of the reviews is to determine if the organization is conducting reviews of the physical access logs every 30 days. DoD has defined the frequency as every 30 days.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-6(b)	CCI-000940	The organization defines a frequency for reviewing physical access logs.	DoD has defined the frequency as every 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 30 days.	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-6(c)	CCI-000941	The organization coordinates results of reviews and investigations with the organizations incident response capability.	The organization being inspected/assessed will coordinate the results of reviews and investigations of physical security incidents with the organization's incident response capability (for physical security incidents).	The organization conducting the inspection/assessment obtains and examines documentation of physical security incidents to ensure coordination with the inspected organization's incident response capability occurred.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-6(1)	CCI-000942	The organization monitors physical intrusion alarms and surveillance equipment.	The organization being inspected/assessed will actively monitor physical intrusion alarms and surveillance equipment.	The organization conducting the inspection/assessment will observe and interview security personnel conducting monitoring activities to validate the organization is actively monitoring all physical intrusion alarms and surveillance equipment.	MOD			X	X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-8(a)	CCI-000947	The organization maintains visitor access records to the facility where the information system resides for organization-defined time period.	The organization being inspected/assessed must maintain visitor access records for their facilities for at least one year. DoD has defined the time period as at least one year.	The organization conducting the inspection/assessment obtains and examines visitor access records to determine if the organization is maintaining visitor access records to the facility where the information system resides for at least one year. DoD has defined the time period as at least one year.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-8(b)	CCI-000948	The organization reviews visitor access records in accordance with organization-defined frequency.	The organization being inspected/assessed conducts reviews of visitor access records every 30 days and must establish and maintain a documented audit trail within the authorization lifecycle. DoD has defined the frequency as every 30 days.	The organization conducting the inspection/assessment obtains and examines the audit documentation of visitor access record review to ensure the inspected organization is conducting reviews every 30 days. DoD has defined the frequency as every 30 days.	LOW			X	X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-8(b)	CCI-000949	The organization defines the frequency to review the visitor access records for the facility where the information system resides.	DoD has defined the frequency as every 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 30 days.	LOW				X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-9	CCI-000952	The organization protects power equipment and power cabling for the information system from damage and destruction.	The organization being inspected/assessed provides a list of protective measures in place to prevent damage and/or destruction of power equipment and power cabling for their information system environment, IAW CP-2 (1), CCI 469.	The organization conducting the inspection/assessment obtains and examines the list of protective measures. Physical inspection of power equipment and power cabling will be done to ensure identified protective measures are in place.	MOD		X	X					3.10 DEVICE POWER		CCI requirements are addressed within subparagraph "Device Power" of UFGS 25 05 11.
N/A	PE-10(a)	CCI-000956	The organization provides the capability of shutting off power to the information system or individual system components in emergency situations.	This control does not apply to individual workstations, laptops, printers, etc. This control only applies to facilities containing concentrations of information system resources (e.g., datacenters, server rooms, mainframe computer rooms). The organization being inspected/assessed will establish and document the capability to shut off the power to facilities or areas within facilities containing concentrations of information system resources (e.g., datacenters, server rooms, mainframe computer rooms) in emergency situations.	The organization conducting the inspection/assessment obtains and examines documentation of the capability to shut off the power to facilities or areas within facilities containing concentrations of information system resources (e.g., datacenters, server rooms, mainframe computer rooms) in emergency situations. The purpose is to validate the organization has provided the capability of shutting off power in emergency situations.	MOD	X			X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-10(b)	CCI-000957	The organization places emergency shutoff switches or devices in an organization-defined location by information system or system component to facilitate safe and easy access for personnel.	This control does not apply to individual workstations, laptops, printers, etc. This control only applies to facilities containing concentrations of information system resources (e.g., datacenters, server rooms, mainframe computer rooms). The organization being inspected/assessed places emergency shutoff switches or devices near more than one egress point of the IT area and ensure it is labeled and protected by a cover to prevent accidental shut-off to facilitate safe and easy access for personnel. DoD has defined the location as near more than one egress point of the IT area and ensure it is labeled and protected by a cover to prevent accidental shut-off.	The organization conducting the inspection/assessment will physically inspect emergency shutoff switches or devices for placement to validate the organization has installed the emergency shutoff switches or devices near more than one egress point of the IT area and ensure it is labeled and protected by a cover to prevent accidental shut-off to facilitate safe and easy access for personnel. DoD has defined the location as near more than one egress point of the IT area and ensure it is labeled and protected by a cover to prevent accidental shut-off.	MOD	X			X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PE-10(b)	CCI-000958	The organization defines a location for emergency shutoff switches or devices by information system or system component.	DoD has defined the location as near more than one egress point of the IT area and ensures it is labeled and protected by a cover to prevent accidental shut-off.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the location as near more than one egress point of the IT area and ensures it is labeled and protected by a cover to prevent accidental shut-off.	MOD	X			X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-10(c)	CCI-000959	The organization protects emergency power shutoff capability from unauthorized activation.	The organization being inspected/assessed will protect emergency power shutoff capability. DoD has defined the location as near more than one egress point of the IT area and ensures it is labeled and protected by a cover to prevent accidental shut-off.	The organization conducting the inspection/assessment will ensure that the inspected organization has protected emergency power shutoff capability. DoD has defined the location as near more than one egress point of the IT area and ensures it is labeled and protected by a cover to prevent accidental shut-off.	MOD	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-11(1)	CCI-000961	The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	The organization being inspected/assessed will: 1. implement alternate power supply capable of supporting minimal operational capability over the long term. 2. Provide a list of physical IT assets within the boundary of the information system that require a long term alternate power supply. This list may come from the inspected organization's security plan, continuity plan, or other documentation.	The organization conducting the inspection/assessment obtains and examines the list of physical IT assets within the boundary of the information system that require a long term alternate power supply. Physically inspect a sample from the list to ensure that long term power supply capability supporting minimal operational capability has been provided.	LOW	X	X				X	NIST 800-53 does not have this in a LOW baseline. NIST 800-82 included it with the rationale "ICS may support critical activities....". By definition, a CS supporting "critical activities" is not a LOW system.	3.10 DEVICE POWER		CCI requirements are addressed within subparagraph "Device Power" of UFGS 25 05 11.
N/A	PE-12	CCI-000963	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	The organization being inspected/assessed must install and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility in compliance with established OSHA requirements.	The organization conducting the inspection/assessment conducts visual inspections and interviews physical security personnel to validate the organization is in compliance with established OSHA requirements by employing and maintaining emergency lighting for the information system, the emergency lighting activates in the event of a power outage or disruption, and it covers emergency exits and evacuation routes within the facility	LOW								---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-13	CCI-000965	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	The organization being inspected/assessed must implement and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source. An independent energy source is some source other than the primary energy source for that facility. Examples include sprinkler systems, hand held fire extinguishers, fixed fire hoses, and smoke detectors.	The organization conducting the inspection/assessment will conduct visual observation and interview organizational personnel with responsibilities for fire detection and suppression devices/systems. The purpose of the reviews and interviews is to validate the fire suppression and detection devices/systems for the information system are supported by an independent energy source.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-14(a)	CCI-000971	The organization maintains temperature and humidity levels within the facility where the information system resides at organization-defined acceptable levels.	Humidity controls are not required for general office areas where information system components may be in use and are only required where there are concentrations of information systems such as server farms, mainframes, etc. The organization being inspected/assessed must maintain temperature and where applicable humidity levels of for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications. DoD has defined the acceptable levels as for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications.	The organization conducting the inspection/assessment reviews temperature and humidity controls to validate that they are set within DoD specified guidelines. DoD has defined the acceptable levels as for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-14(a)	CCI-000972	The organization defines acceptable temperature and humidity levels to be maintained within the facility where the information system resides.	DoD has defined the acceptable levels as for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the acceptable levels as for commercial grade information systems: 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing; for other systems, levels within manufacturer specifications.	LOW	X			X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-14(b)	CCI-000973	The organization monitors temperature and humidity levels in accordance with organization-defined frequency.	The organization being inspected/assessed will maintain an independent monitor device for temperature and humidity levels not located in the immediate vicinity of the controller continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required. Records of monitoring must be maintained as an audit trail within the authorization lifecycle. DoD has defined the frequency as continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required.	The organization conducting the inspection/assessment will visually observe the inspected organization's independent monitoring device, obtain and examine audit logs, and interview physical security/safety personnel to validate the inspected organization monitors temperature and humidity levels continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required. DoD has defined the frequency as continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-14(b)	CCI-000974	The organization defines a frequency for monitoring temperature and humidity levels.	DoD has defined the frequency as continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as continuously unless manufacturer specifications allow for a wide enough tolerance that control is not required.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-15	CCI-000977	The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible.	The organization being inspected/assessed must provide master shutoff valves that are accessible to protect the information system from damage resulting from water leakage.	The organization conducting the inspection/assessment will inspect the master shutoff valves to ensure they are installed and accessible.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures		Applies at or Below Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PE-15	CCI-000978	The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are working properly.	The organization being inspected/assessed will ensure that master shutoff valves are working properly and have been inspected by the appropriate organization (e.g., fire marshal, department of public works).	The organization conducting the inspection/assessment will visually inspect master shutoff valve inspection documentation (e.g., inspection form, tag attached to valve).	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-15	CCI-000979	Key personnel have knowledge of the master water shutoff or isolation valves.	The organization being inspected/assessed will identify and document key personnel and will provide training on the location and procedures for use of master shutoff valves.	The organization conducting the inspection/assessment obtains and examines list of key personnel with knowledge of location and activation procedures for master shutoff valves and any other relevant documents or records. Interview key personnel from the list to determine if identified key personnel within the organization have knowledge of the master shutoff valves.	LOW	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-16	CCI-000981	The organization authorizes organization-defined types of information system components entering and exiting the facility.	The organization being inspected/assessed authorizes and maintains authorization records of all system components entering and exiting the facility. DoD has defined the types of information system components as all system components.	The organization conducting the inspection/assessment obtains and examines records authorizing all system components entering and exiting the facility. DoD has defined the types of information system components as all system components.	LOW	X		X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-16	CCI-000982	The organization monitors organization-defined types of information system components entering and exiting the facility.	The organization being inspected/assessed monitors all system components entering and exiting the facility. DoD has defined the types of information system components as all system components.	The organization conducting the inspection/assessment obtains and examines records monitoring all system components entering and exiting the facility. DoD has defined the types of information system components as all system components.	LOW	X		X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-16	CCI-000983	The organization controls organization-defined types of information system components entering and exiting the facility.	The organization being inspected/assessed: 1. Documents in their physical and environmental protection plan (PE-1) controls for all system components entering and exiting the facility. 2. Implements documented controls for system components entering and exiting the facility. DoD has defined the types of information system components as all system components.	The organization conducting the inspection/assessment obtains and examines the physical and environmental protection plan to determine if controls have been documented for all system components entering and exiting the facility and visually inspects the controls (e.g., logs, scans, etc.) to ensure implementation. DoD has defined the types of information system components as all system components.	LOW	X		X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-16	CCI-000984	The organization maintains records of information system components entering and exiting the facility.	The organization being inspected/assessed will maintain records of all information system components entering and exiting the facility. If the organization is following General Records Schedule (GRS) 18, Section 12 they are automatically compliant.	The organization conducting the inspection/assessment obtains and examines records of physical entry and exit events to the facility. The purpose of the reviews is to ensure the organization is maintaining detailed and accurate records of information system components that enter and exit the facility. If the organization is following GRS 18, Section 12 they are automatically compliant.	LOW	X		X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-1(a)(1)	CCI-000995	The organization develops and documents a media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	LOW	X				X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-1(a)(1)	CCI-000996	The organization disseminates to organization-defined personnel or roles a media protection policy.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures and is disseminated to all users via http://www.dtic.mil/whs/directives/corres/ins1.html. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	LOW	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-1(b)(1)	CCI-000997	The organization reviews and updates the current media protection policy in accordance with organization-defined frequency.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	LOW	X				X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-1(b)(1)	CCI-000998	The organization defines a frequency for reviewing and updating the current media protection policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW	X				X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-1(a)(2)	CCI-000999	The organization develops and documents procedures to facilitate the implementation of the media protection policy and associated media protection controls.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	LOW	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	MP-1(a)(2)	CCI-001000	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the media protection policy and associated media protection controls.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures and is disseminated to all users via http://www.dtic.mil/whs/directives/corres/ins1.html. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	LOW	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	MP-1(b)(2)	CCI-001001	The organization reviews and updates the current media protection procedures in accordance with organization-defined frequency.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4.	LOW	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	MP-1(b)(2)	CCI-001002	The organization defines a frequency for reviewing and updating the current media protection procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	MP-2	CCI-001003	The organization restricts access to organization-defined types of digital and/or non-digital media to organization-defined personnel or roles.	The organization being inspected/assessed restricts access to all types of digital and/or non-digital media containing information not cleared for public release to the personnel or roles defined in MP-2, CCI 1005. DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.	The organization conducting the inspection/assessment interviews organizational personnel with information system media protection responsibilities to ensure the organization being inspected/assessed restricts access to all types of digital and/or non-digital media containing information not cleared for public release to the personnel or roles defined in MP-2, CCI 1005. DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-2	CCI-001004	The organization defines types of digital and/or non-digital media for which the organization restricts access.	DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-2	CCI-001005	The organization defines personnel or roles to restrict access to organization-defined types of digital and/or non-digital media.	The organization being inspected/assessed will define and document personnel or roles to restrict access to media IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level, but personnel must be identified IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to restrict access to media to ensure the access is granted IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level, but personnel must be identified IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-4(a)	CCI-001014	The organization physically controls and securely stores organization-defined types of digital and/or non-digital media within organization-defined controlled areas.	The organization being inspected/assessed physically controls and securely stores all digital and non-digital media containing sensitive, controlled, and/or classified information within areas approved for processing or storing data IAW the sensitivity and/or classification level of the information contained on/within the media. DoD has defined the digital and non-digital media types as all digital and non-digital media containing sensitive, controlled, and/or classified information. DoD has defined the controlled areas as areas approved for processing or storing data IAW the sensitivity and/or classification level of the information contained on/within the media.	The organization conducting the inspection/assessment obtains and examines the list of all digital and non-digital media containing sensitive, controlled, and/or classified information within areas approved for processing or storing data IAW the sensitivity and/or classification level of the information contained on/within the media to ensure that physical controls are in place and that it is securely stored as defined in PE-3. DoD has defined the digital and non-digital media types as all digital and non-digital media containing sensitive, controlled, and/or classified information. DoD has defined the controlled areas as areas approved for processing or storing data IAW the sensitivity and/or classification level of the information contained on/within the media.	MOD	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-4(a)	CCI-001015	The organization defines types of digital and/or non-digital media to physically control and securely store within organization-defined controlled areas.	DoD has defined the digital and non-digital media types as all digital and non-digital media containing sensitive, controlled, and/or classified information.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the digital and non-digital media types as all digital and non-digital media containing sensitive, controlled, and/or classified information.	MOD	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-4(a)	CCI-001016	The organization defines controlled areas where organization-defined types of digital and/or non-digital media are physically controlled and securely stored.	DoD has defined the controlled areas as areas approved for processing or storing data IAW the sensitivity and/or classification level of the information contained on/within the media.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the controlled areas as areas approved for processing or storing data IAW the sensitivity and/or classification level of the information contained on/within the media.	MOD	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-4(b)	CCI-001018	The organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	The organization being inspected/assessed protects information system media IAW DoDM 5200.01 M Vol. 1-4.	The organization conducting the inspection/assessment obtains and examines the list of media and verifies it is being stored and protected IAW DoDM 5200.01 M Vol. 1-4.	MOD	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-5(a)	CCI-001020	The organization protects and controls organization-defined types of information system media during transport outside of controlled areas using organization-defined security safeguards.	The organization being inspected/assessed protects and controls information system media during transport outside of controlled areas using security measures defined in DoDM 5200.01 M Vol. 1-4 and DoDD 5015.2.	The organization conducting the inspection/assessment obtains and examines the organization's records management policy or process to ensure appropriate protection of information according to its classification or designation during transport outside of controlled areas, IAW security measures defined in DoDM 5200.01 M Vol. 1-4 and DoDD 5015.2.	MOD	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-5(a)	CCI-001021	The organization defines types of information system media protected and controlled during transport outside of controlled areas.	DoD has defined the types of information system media as all digital and non-digital media containing sensitive, controlled, and/or classified information.	DoD has defined the types of information system media as all digital and non-digital media containing sensitive, controlled, and/or classified information. The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.	MOD	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	MP-5(a)	CCI-001022	The organization defines security safeguards to be used to protect and control organization-defined types of information system media during transport outside of controlled areas.	DoD has defined the security safeguards as DoDI 5200.1R and other organizationally defined security safeguards.	DoD has defined the security safeguards as DoDI 5200.1R and other organizationally defined security safeguards. The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.	MOD	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	MP-5(b)	CCI-001023	The organization maintains accountability for information system media during transport outside of controlled areas.	The organization being inspected/assessed ensures the organization defined security measures (MP-2) includes method of accountability for information system media during transport outside of controlled areas, IAW DoDM 5200.01 M Vol. 1-4 and DoDD 5015.2.	The organization conducting the inspection/assessment obtains and examines the list of organization defined security measures (MP-2) to ensure method of accountability for information system media during transport outside of controlled areas has been identified.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	MP-5(d)	CCI-001024	The organization restricts the activities associated with the transport of information system media to authorized personnel.	The organization being inspected/assessed ensures the organization defined security measures (MP-2) includes a requirement to develop and maintain a list of personnel authorized to transport information system media outside of controlled areas, IAW DoDM 5200.01 M Vol. 1-4 and DoDD 5015.2. Develop and maintain the list of personnel authorized to transport information system media outside of controlled areas.	The organization conducting the inspection/assessment obtains and examines the list of personnel authorized to transport information system media outside of controlled areas. Organizational personnel with information system media transport responsibilities and security management personnel are to be interviewed. The purpose of the reviews and reviews is to determine if the organization has established restrictions associated with the transport of information system media to authorized personnel only.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-5(c)	CCI-001025	The organization documents activities associated with the transport of information system media.	The organization being inspected/assessed documents activities associated with the transport of information system media.	The organization conducting the inspection/assessment obtains and examines the documented activities to ensure the organization being inspected/assessed documents activities associated with the transport of information system media.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-5(4)	CCI-001027	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	The organization being inspected/assessed shall document within their Security Plan, and implement, FIPS 140-2 or other NSA approved cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	The organization conducting the inspection/assessment obtains and examines the Security Plan to ensure the organization being inspected has identified FIPS 140-2 or other NSA approved cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-6(a)	CCI-001028	The organization sanitizes organization-defined information system media prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies.	The organization being inspected/assessed sanitizes all media prior to disposal, release out of organizational control, or release for reuse IAW DoDM 5200.01 Vol. 1-4 using techniques and procedures IAW NIST SP 800-88. DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88. DoD has defined the information system media as all media.	The organization conducting the inspection/assessment obtains and examines media sanitization records, audit records, any other relevant documents or records, and sanitization tools to ensure sanitization is in compliance with DoDM 5200.01 Vol. 1-4 and uses techniques and procedures IAW NIST SP 800-88. The objective of the review is to verify the organization is sanitizing its digital and non-digital information system media prior to disposal, release for reuse, or release out of the organizational control. DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88. DoD has defined the information system media as all media.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-1(a)(1)	CCI-001037	The organization develops and documents a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(a)(1)	CCI-001038	The organization disseminates a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to organization-defined personnel or roles.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures and is disseminated via the NIST publications site: http://csrc.nist.gov/publications/PubsSPs.html DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(b)(1)	CCI-001039	The organization reviews and updates the current risk assessment policy in accordance with organization-defined frequency.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(b)(1)	CCI-001040	The organization defines the frequency to review and update the current risk assessment policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(a)(2)	CCI-001041	The organization develops and documents procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(a)(2)	CCI-001042	The organization disseminates risk assessment procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls to organization-defined personnel or roles.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures and is disseminated via the NIST publications site: http://csrc.nist.gov/publications/PubsSPs.html DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(b)(2)	CCI-001043	The organization reviews and updates the current risk assessment procedures in accordance with organization-defined frequency.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(b)(2)	CCI-001044	The organization defines the frequency to review and update the current risk assessment procedures.	DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.	DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy. DoD has defined the frequency as annually - updated as appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures		Applies at or Below Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	RA-2(a)	CCI-001045	The organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The organization being inspected/assessed documents and implements a process to categorize information and the information system in accordance with CNSSI 1253 and applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed categorizes information and the information system in accordance with CNSSI 1253 and applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-2(b)	CCI-001046	The organization documents the security categorization results (including supporting rationale) in the security plan for the information system.	The organization being inspected/assessed documents the security categorization results (including supporting rationale) in the security plan for the information system IAW CNSSI 1253.	The organization conducting the inspection/assessment obtains and examines the documented security categorization results to ensure the organization being inspected/assessed documents the security categorization results (including supporting rationale) in the security plan for the information system IAW CNSSI 1253.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-2(c)	CCI-001047	The organization ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	The organization being inspected/assessed documents and implements a process IAW CNSSI 1253 to ensure the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-3(a)	CCI-001048	The organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction.	The organization being inspected/assessed conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction. The organization must maintain an audit trail of assessments.	The organization conducting the inspection/assessment obtains and examines the audit trail of assessments to ensure the organization being inspected/assessed conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction.	LOW		X	X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	RA-3(b)	CCI-001049	The organization documents risk assessment results in the organization-defined document.	The organization being inspected/assessed documents risk assessment results in the risk assessment report. DoD has defined the document as a risk assessment report.	The organization conducting the inspection/assessment obtains and examines the risk assessment report to ensure the organization being inspected/assessed documents risk assessment results in the risk assessment report. DoD has defined the document as a risk assessment report.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	RA-3(c)	CCI-001050	The organization reviews risk assessment results on an organization-defined frequency.	The organization being inspected/assessed reviews risk assessment results upon re-accreditation. The organization must maintain a record of reviews. DoD has defined the frequency as upon re-accreditation.	The organization conducting the inspection/assessment obtains and examines the record of reviews to ensure the organization being inspected/assessed reviews risk assessment results upon re-accreditation. DoD has defined the frequency as upon re-accreditation.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	RA-3(c)	CCI-001051	The organization defines a frequency for reviewing risk assessment results.	DoD has defined the frequency as upon re-accreditation.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as upon re-accreditation.	LOW					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	RA-3(e)	CCI-001052	The organization updates the risk assessment on an organization-defined frequency or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	The organization being inspected/asssessed updates the risk assessment upon re-accreditation or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. DoD has defined the frequency as upon re-accreditation.	The organization conducting the inspection/assessment obtains and examines historical versions of the risk assessment as well as records of changes to the system to ensure the organization being inspected/assessed updates the risk assessment upon re-accreditation or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. DoD has defined the frequency as upon re-accreditation.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	RA-3(e)	CCI-001053	The organization defines a frequency for updating the risk assessment.	DoD has defined the frequency as upon re-accreditation.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as upon re-accreditation.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-5(a)	CCI-001054	The organization scans for vulnerabilities in the information system and hosted applications on an organization-defined frequency.	The organization being inspected/assessed will define, document, and implement procedures for vulnerability scans of the information system and hosted applications; and scan for vulnerabilities in the information system and hosted applications every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). This control is not targeted at security control compliance scanning. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines the organization's vulnerability scanning procedures and results for the 90 days preceding the inspection/assessment. If the system in question has not been operational for more than 90 days the organization will provide all available scan(s).	LOW	X	X	X					3.11 VULNERABILITY SCANNING	FRCS has no IP devices to scan	
N/A	RA-5(a)	CCI-001055	The organization defines a frequency for scanning for vulnerabilities in the information system and hosted applications.	DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	LOW	X	X		X	X			3.11 VULNERABILITY SCANNING	FRCS has no IP devices to scan	
N/A	RA-5(a)	CCI-001056	The organization scans for vulnerabilities in the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported.	The organization being inspected/assessed will conduct vulnerability scans of the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported via authoritative sources (e.g., IAVM, CTO, DTM, STIG, product vendor).	The organization conducting the inspection/assessment obtains and examines the organization's vulnerability scanning procedures and results in order to validate the organization conducts vulnerability scans of its Information System (IS) and hosted applications when new vulnerabilities potentially affecting the IS and/or applications are identified and reported.	LOW	X	X	X					3.11 VULNERABILITY SCANNING	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-5(b)	CCI-001057	The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: enumerating platforms, software flaws, and improper configurations; formatting checklists and test procedures; and measuring vulnerability impact.	The organization being inspected/assessed employs the DoD Enterprise scanning tool.	The organization conducting the inspection/assessment obtains and examines the software list or vulnerability scanning procedures to ensure the organization being inspected/assessed employs the DoD Enterprise scanning tool.	LOW	X	X	X	X				3.11 VULNERABILITY SCANNING	FRCS has no IP devices to scan	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	RA-5(c)	CCI-001058	The organization analyzes vulnerability scan reports and results from security control assessments.	The organization being inspected/assessed analyzes vulnerability scan reports and security control assessment results with the intent of identifying legitimate vulnerabilities and the relationship between vulnerabilities and security controls.	The organization conducting the inspection/assessment will interview organizational personnel with security control assessment and vulnerability scanning responsibilities. The purpose of the reviews and interviews is to validate the organization is conducting an analysis of the vulnerability scan reports and results from the security control assessments.	LOW	X	X	X					3.11 VULNERABILITY SCANNING	FRCS has no IP devices to scan	
N/A	RA-5(d)	CCI-001059	The organization remediates legitimate vulnerabilities in organization-defined response times in accordance with an organizational assessment risk.	The organization being inspected/assessed takes corrective actions as appropriate on legitimate vulnerabilities identified in RA-5, CCI 001058 IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). Audit records of actions must be maintained IAW applicable DoD, CYBERCOM, and/or component policies. DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines audit records to validate the organization is taking action to remediate legitimate vulnerabilities within the required response times (IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). The organization conducting the inspection/assessment may conduct independent vulnerability scans to compare those scan results with audit records of remediation actions. DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	LOW	X	X	X	X				3.11 VULNERABILITY SCANNING	FRCS has no IP devices to scan	
N/A	RA-5(d)	CCI-001060	The organization defines response times for remediating legitimate vulnerabilities in accordance with an organization assessment of risk.	DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs).	LOW				X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	RA-5(e)	CCI-001061	The organization shares information obtained from the vulnerability scanning process and security control assessments with organization-defined personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	The organization being inspected/assessed documents and implements a process to share information obtained from the vulnerability scanning process and security control assessments with at a minimum, the ISSM and ISSO to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed shares information obtained from the vulnerability scanning process and security control assessments with at a minimum, the ISSM and ISSO to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-5(1)	CCI-001062	The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.	The organization being inspected/assessed will employ scanning tools that maintain currency with industry standard information system vulnerabilities to ensure that scanning activities are conducted with the most up to date list of known vulnerabilities to include USCYBERCOM issued IAVMs. DoD has provided an enterprise scanning tool that fully meets this requirement. Organizations that choose not to use the enterprise scanning tool must identify which scanning tool they are using and ensure that it meets these requirements.	The organization conducting the inspection/assessment will: 1. If the inspected organization is using the DoD provided enterprise scanning tool, compliance with this control is complete. 2. Validate the identified tool in use by the inspected organization is able to maintain current up to date information system vulnerability data.	MOD	X	X						2.3 DATABASE AND WEB SERVER SOFTWARE FO... 3.11 VULNERABILITY SCANNING	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	RA-5(2)	CCI-001063	The organization updates the information system vulnerabilities scanned on an organization-defined frequency, prior to a new scan and/or when new vulnerabilities are identified and reported.	The organization being inspected/assessed will update the list of information system vulnerabilities scanned for prior to running scans. The organization must maintain a record of scans including the list of vulnerabilities scanned for. DoD has defined the frequency as prior to running scans.	The organization conducting the inspection/assessment obtains and examines the record of scans to ensure the latest most up to date scanning policies are present.	MOD	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	RA-5(2)	CCI-001064	The organization defines a frequency for updating the information system vulnerabilities scanned.	DoD has defined the frequency as prior to running scans.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as prior to running scans.	MOD					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-5(5)	CCI-001067	The information system implements privileged access authorization to organization-identified information system components for selected organization-defined vulnerability scanning activities.	The organization being inspected/assessed configures the information system to implement privileged access authorization to all information systems and infrastructure components for selected vulnerability scanning activities defined in RA-5 (5), CCI 2906. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1067. DoD has defined the information system components as all information systems and infrastructure components.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement privileged access authorization to all information systems and infrastructure components for selected vulnerability scanning activities defined in RA-5 (5), CCI 2906. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1067. DoD has defined the information system components as all information systems and infrastructure components.	MOD	X	X						2.3 DATABASE AND WEB SERVER SOFTWARE FO... 3.11 VULNERABILITY SCANNING	FRCS has no computer-based databases in scope. FRCS has no IP devices to scan.	
N/A	SC-1(a)(1)	CCI-001074	The organization develops and documents a system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for developing a system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for developing a system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(a)(1)	CCI-001075	The organization disseminates to organization-defined personnel or roles the system and communications protection policy.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enriched	Designed	Non-Designed	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-1(b)(1)	CCI-001076	The organization reviews and updates the system and communications protection policy in accordance with organization-defined frequency.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(b)(1)	CCI-001077	The organization defines the frequency for reviewing and updating the system and communications protection policy.	DoD has defined the frequency as every 5 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(a)(2)	CCI-001078	The organization develops and documents system and communications protection procedures to facilitate the implementation of the system and communications protection policy and communications protection controls and associated system and communications protection controls.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for developing system and communications protection procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for developing system and communications protection procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(a)(2)	CCI-001079	The organization disseminates to organization-defined personnel or roles the procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the procedures to facilitate the implementation of the system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for disseminating the procedures to facilitate the implementation of the system and communications protection policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(b)(2)	CCI-001080	The organization reviews and updates the system and communications protection procedures in accordance with organization-defined frequency.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	DoDI 8523.01 "Communications Security (COMSEC)"meets the DoD requirement for reviewing and updating the system and communications protection procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8523.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(b)(2)	CCI-001081	The organization defines the frequency of system and communications protection procedure reviews and updates.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-2	CCI-001082	The information system separates user functionality (including user interface services) from information system management functionality.	The organization being inspected/assessed configures the information system to separate user functionality (including user interface services) from information system management functionality. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1082.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to separate user functionality (including user interface services) from information system management functionality. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1082.	MOD	X	X	X					3.7.2 Denial of Service Protection<TAI OP...		CCI requirements are addressed within subparagraph "Denial of Service Protection" of UFGS 25 05 11.
N/A	SC-5	CCI-001093	The organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system.	The organization being inspected/assessed defines and documents the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system. DoD has determined the types of denial of service attacks are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented types of denial of service attacks to ensure the organization being inspected/assessed defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system. DoD has determined the types of denial of service attacks are not appropriate to define at the Enterprise level.	LOW	X	X						3.7.2 Denial of Service Protection<TAI OP...		CCI requirements are addressed within subparagraph "Denial of Service Protection" of UFGS 25 05 11.
N/A	SC-5(1)	CCI-001094	The information system restricts the ability of individuals to launch organization-defined denial of service attacks against other information systems.	The organization being inspected/assessed configures the information system to restrict the ability of individuals to launch denial of service attacks defined in SC-5 (1), CCI 2387 against other information systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1094.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to restrict the ability of individuals to launch denial of service attacks defined in SC-5 (1), CCI 2387 against other information systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1094.	MOD	X	X						3.2.5 IP Control Networks		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "IP Control Networks" within Part 3.
N/A	SC-5(2)	CCI-001095	The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.	The organization being inspected/assessed configures the information system to manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1095.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1095.	MOD		X						3.2.5 IP Control Networks		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "IP Control Networks" within Part 3.
N/A	SC-7(a)	CCI-001097	The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.	The organization being inspected/assessed documents and implements processes to monitor and control communications at the external boundary of the system and at key internal boundaries within the system. The organization must maintain an audit trail of monitoring activities.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring activities to ensure the organization being inspected/assessed monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.	LOW	X	X		X	X			3.3.6 Pysical Security in MODERATE Impact... 3.7.2 Denial of Service Protection<TAI OP... 3.7.5 Process Isolation and Boundary Prot...		CCI requirements are addressed within subparagraph "Denial of Service Protection" and "Physical Security in MODERATE Impact Systems" and "Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures		Applies at or Below Enclave	Enclave Designer	Non-Designer Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-7(c)	CCI-001098	The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	The organization being inspected/assessed designs the information system to enforce requirements that components connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component connectivity to ensure the organization being inspected/assessed connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	LOW	X							3.7.5 Process Isolation and Boundary Prot...		CCI requirements are addressed within subparagraph "Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems" of UFGS 25 05 11.
N/A	SC-7(3)	CCI-001101	The organization limits the number of external network connections to the information system.	The organization being inspected/assessed documents and implements information system access control mechanisms to limit the number of external connections to the information system.	The organization conducting the inspection/assessment obtains and examines the documented access control mechanisms to ensure that the organization being inspected/assessed limits the number of external network connections to the information system.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-7(4)(a)	CCI-001102	The organization implements a managed interface for each external telecommunication service.	The organization being inspected/assessed designs the information system to have a managed interface for each telecommunication service.	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying system interfaces to ensure the organization being inspected/assessed implements a managed interface for each external telecommunication service.	MOD	X							3.7.5 Process Isolation and Boundary Prot...		CCI requirements are addressed within subparagraph "Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems" of UFGS 25 05 11.
N/A	SC-7(4)(b)	CCI-001103	The organization establishes a traffic flow policy for each managed interface for each external telecommunication service.	The organization being inspected/assessed defines and documents a traffic flow policy for each managed interface for each external telecommunication service.	The organization conducting the inspection/assessment obtains and examines the documented traffic flow policy to ensure the organization being inspected/assessed establishes a traffic flow policy for each managed interface for each external telecommunication service.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-7(4)(d)	CCI-001105	The organization documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need for each external telecommunication service.	The organization being inspected/assessed documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need for each external telecommunication service.	The organization conducting the inspection/assessment obtains and examines the documented exceptions to the traffic flow policy to ensure the organization being inspected/assessed identifies each exception with supporting mission/business need and duration of that need for each external telecommunication service.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-7(4)(e)	CCI-001106	The organization reviews exceptions to the traffic flow policy on an organization-defined frequency for each external telecommunication service.	The organization being inspected/assessed implements a process to review exceptions to the traffic flow policy every 180 days for each external telecommunication service. The organization must maintain an audit trail of reviews. DoD has defined the frequency as every 180 days.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organization being inspected/assessed reviews exceptions to the traffic flow policy every 180 days for each external telecommunication service. DoD has defined the frequency as every 180 days.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-7(4)(e)	CCI-001107	The organization defines a frequency for the review of exceptions to the traffic flow policy for each external telecommunication service.	DoD has defined the frequency as every 180 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 180 days.	MOD				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-7(4)(e)	CCI-001108	The organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need for each external telecommunication service.	The organization being inspected/assessed documents and implements a process to remove traffic flow policy exceptions that are no longer supported by an explicit mission/business need for each external telecommunication service.	The organization conducting the inspection/assessment obtains and examines the documented process as well as a sampling of existing exceptions to ensure the organization being inspected/assessed removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need for each external telecommunication service.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-7(5)	CCI-001109	The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).	The organization being inspected/assessed configures the information system to deny network communications traffic at managed interfaces by default and allows network communications traffic by exception (i.e., deny all, permit by exception). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1109.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to deny network communications traffic at managed interfaces by default and allows network communications traffic by exception (i.e., deny all, permit by exception). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1109.	MOD	X	X						1.9.2 Cybersecurity Interconnection Sched... 3.3.6 Pysical Security in MODERATE Impact... 3.7.5 Process Isolation and Boundary Prot...		CCI requirements are addressed within subparagraph "Cybersecurity Interconnection Schedule", "Physical Security in MODERATE Impact Systems" and "Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems" of UFGS 25 05 11.
N/A	SC-7(8)	CCI-001112	The information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers at managed interfaces.	The organization being inspected/assessed configures the information system to route protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP) to any network external to the authorization boundary through authenticated proxy servers at managed interfaces. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1112. DoD has defined the internal communications traffic as protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP). DoD has defined the external networks as any network external to the authorization boundary.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to route protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP) to any network external to the authorization boundary through authenticated proxy servers at managed interfaces. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1112. DoD has defined the internal communications traffic as protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP). DoD has defined the external networks as any network external to the authorization boundary.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-7(8)	CCI-001113	The organization defines the internal communications traffic to be routed to external networks.	DoD has defined the internal communications traffic as protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the internal communications traffic as protocols as designated by PPSM guidance (e.g. HTTPS, HTTP, FTP, SNMP).	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-7(8)	CCI-001114	The organization defines the external networks to which the organization-defined internal communications traffic should be routed.	DoD has defined the external networks as any network external to the authorization boundary.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the external networks as any network external to the authorization boundary.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-7(13)	CCI-001119	The organization isolates organization-defined information security tools, mechanisms, and support components from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.	The organization being inspected/assessed designs the information system to isolate key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc. from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system. DoD has defined the key information security tools, mechanisms, and support components as key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc.	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component partitioning to ensure the organization being inspected/assessed isolates key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc. from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system. DoD has defined the key information security tools, mechanisms, and support components as key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc.	MOD	X		X					3.7.5 Process Isolation and Boundary Prot...		CCI requirements are addressed within subparagraph "Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems" of UFGS 25 05 11.
N/A	SC-7(13)	CCI-001120	The organization defines key information security tools, mechanisms, and support components to be isolated.	DoD has defined the key information security tools, mechanisms, and support components as key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the key information security tools, mechanisms, and support components as key information security tools, mechanisms, and support components such as, but not limited to PKI, Patching infrastructure, HBSS, CND Tools, Special Purpose Gateway, vulnerability tracking systems, honeypots, internet access points (IAPs); network element and data center administrative/management traffic; Demilitarized Zones (DMZs), Server farms/computing centers, centralized audit log servers etc.	MOD	X	X	X					3.7.5 Process Isolation and Boundary Prot...		CCI requirements are addressed within subparagraph "Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems" of UFGS 25 05 11.
N/A	SC-7(14)	CCI-001121	The organization protects against unauthorized physical connections at organization-defined managed interfaces.	The organization being inspected/assessed documents and implements mechanisms to protect against unauthorized physical connections at internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways. DoD has defined the managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.	The organization conducting the inspection/assessment obtains and examines the documented mechanisms to ensure the organization being inspected/assessed protects against unauthorized physical connections at internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways. DoD has defined the managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-7(14)	CCI-001122	The organization defines the managed interfaces where boundary protections against unauthorized physical connections are to be implemented.	DoD has defined the managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-7(18)	CCI-001126	The information system fails securely in the event of an operational failure of a boundary protection device.	The organization being inspected/assessed configures the information system to fail securely in the event of an operational failure of a boundary protection device. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1126.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to fail securely in the event of an operational failure of a boundary protection device. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1126.	MOD		X		X				1.9.2 Cybersecurity Interconnection Sched... 3.7.5 Process Isolation and Boundary Prot...		CCI requirements are addressed within subparagraph "Cybersecurity Interconnection Schedule" and "Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems" of UFGS 25 05 11.
N/A	SC-10	CCI-001133	The information system terminates the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.	The organization being inspected/assessed configures the information system to terminate the network connection associated with a communications session at the end of the session or after 10 minutes in band management and 15 minutes for user sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1133. DoD has defined the time period as 10 minutes in band management and 15 minutes for user sessions.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to terminate the network connection associated with a communications session at the end of the session or after 10 minutes in band management and 15 minutes for user sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1133. DoD has defined the time period as 10 minutes in band management and 15 minutes for user sessions.	MOD	X	X		X				3.3.4 Session Lock and Session Terminatio...		CCI requirements are addressed within subparagraph "Session Lock and Session Termination Requirements In MODERATE Impact Systems:" of UFGS 25 05 11.
N/A	SC-10	CCI-001134	The organization defines the time period of inactivity after which the information system terminates a network connection associated with a communications session.	DoD has defined the time period as 10 minutes in band management and 15 minutes for user sessions.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 10 minutes in band management and 15 minutes for user sessions.	MOD		X		X	X			3.3.4 Session Lock and Session Terminatio...		CCI requirements are addressed within subparagraph "Session Lock and Session Termination Requirements In MODERATE Impact Systems:" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-15(a)	CCI-001150	The information system prohibits remote activation of collaborative computing devices excluding the organization-defined exceptions where remote activation is to be allowed.	The organization being inspected/assessed configures the information system to prohibit remote activation of collaborative computing devices excluding dedicated VTC suites located in approved VTC locations that are centrally managed. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1150. DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prohibit remote activation of collaborative computing devices excluding dedicated VTC suites located in approved VTC locations that are centrally managed. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1150. DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed.	LOW	X			X				3.7.1 Collaborative Computing	FRCS has no computers	
N/A	SC-15(a)	CCI-001151	The organization defines exceptions to the prohibiting of collaborative computing devices where remote activation is to be allowed.	DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed.	LOW	X			X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-15(b)	CCI-001152	The information system provides an explicit indication of use to users physically present at collaborative computing devices.	The organization being inspected/assessed configures the information system to provide an explicit indication of use to users physically present at collaborative computing devices. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1152.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide an explicit indication of use to users physically present at collaborative computing devices. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1152.	LOW	X			X				3.7.1 Collaborative Computing	FRCS has no computers	
N/A	SC-17	CCI-001159	The organization issues public key certificates under an organization-defined certificate policy or obtains public key certificates from an approved service provider.	The organization being inspected/assessed configures the information system to issue public key certificates under DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling" or obtains public key certificates from an approved service provider. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1159. DoD has defined the certificate policy as DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling."	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to issue public key certificates under DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling" or obtains public key certificates from an approved service provider. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1159. DoD has defined the certificate policy as DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling."	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-18(a)	CCI-001160	The organization defines acceptable and unacceptable mobile code and mobile code technologies.	The organization being inspected/assessed defines and documents acceptable and unacceptable mobile code and mobile code technologies IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must define IAW the STIG/SRG guidance that pertains to CCI 1160.	The organization conducting the inspection/assessmenet obtains and examines the documented acceptable and unacceptable mobile code and mobile code technologies to ensure the organization being inspected/assessed defines acceptable and unacceptable mobile code and mobile code technologies IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has defined acceptable and unacceptable mobile code and mobile code technologies IAW the applicable STIGs and SRGs pertaining to CCI 1160.	MOD	X	X						3.7.3 Mobile Code In MODERATE Impact Syst...		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-18(b)	CCI-001161	The organization establishes usage restrictions for acceptable mobile code and mobile code technologies.	The organization being inspected/assessed documents usage restrictions for acceptable mobile code and mobile code technologies IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must establish IAW the STIG/SRG guidance that pertains to CCI 1161.	The organization conducting the inspection/assessmenet obtains and examines the documented usage restrictions to ensure the organization being inspected/assessed establishes usage restrictions for acceptable mobile code and mobile code technologies IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has established usage restrictions IAW the applicable STIGs and SRGs pertaining to CCI 1161.	MOD	X	X						3.7.3 Mobile Code In MODERATE Impact Syst...		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-18(b)	CCI-001162	The organization establishes implementation guidance for acceptable mobile code and mobile code technologies.	The Protection Profile for Web Browsers and Application SRG meet the DoD requirement to establish implementation guidance for acceptable mobile code and mobile code technologies. DoD Components are automatically compliant with this CCI because they are covered by the Protection Profile for Web Browsers and Application SRG.	The Protection Profile for Web Browsers and Application SRG meet the DoD requirement to establish implementation guidance for acceptable mobile code and mobile code technologies. DoD Components are automatically compliant with this CCI because they are covered by the Protection Profile for Web Browsers and Application SRG.	MOD	X	X						3.7.3 Mobile Code In MODERATE Impact Syst...		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-18(c)	CCI-001163	The organizations authorizes the use of mobile code within the information system.	The organization being inspected/assessed documents mobile code which is authorized for use within the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of mobile code which is authorized for use within the information system and examines the information system to ensure that all used mobile code is authorized.	MOD	X	X						3.7.3 Mobile Code In MODERATE Impact Syst...		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-18(c)	CCI-001164	The organization monitors the use of mobile code within the information system.	The organization being inspected/assessed documents and implements a process to monitor the use of mobile code within the information system.	The organization conducting the inspection/assessment obtains and examines the documented process as well as any artifacts applicable to monitoring of mobile code to ensure the organization being inspected/assessed monitors the use of mobile code within the information system.	MOD	X	X						3.7.3 Mobile Code In MODERATE Impact Syst...		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-18(c)	CCI-001165	The organization controls the use of mobile code within the information system.	The organization being inspected/assessed documents and implements a process to control the use of mobile code within the information system.	The organization conducting the inspection/assessment obtains and examines the documented process and examines the information system to ensure the organization being inspected/assessed controls the use of mobile code within the information system.	MOD	X	X						3.7.3 Mobile Code In MODERATE Impact Syst...		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-18(1)	CCI-001166	The information system identifies organization-defined unacceptable mobile code.	The organization being inspected/assessed configures the information system to identify unacceptable mobile code defined in SC-18 (1), CCI 2458. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1166.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to identify unacceptable mobile code defined in SC-18 (1), CCI 2458. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1166.	MOD	X	X	X					3.7.3 Mobile Code In MODERATE Impact Syst...		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-18(2)	CCI-001167	The organization ensures the development of mobile code to be deployed in information systems meets organization-defined mobile code requirements.	The organization being inspected/assessed documents and implements a process to develop mobile code IAW the requirements defined in CCI 1168.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed develops mobile code IAW the requirements defined in CCI 1168.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-18(2)	CCI-001168	The organization defines requirements for the acquisition, development, and use of mobile code.	The organization being inspected/assessed defines and documents requirements for the acquisition, development, and use of mobile code. The requirements must result in the acquisition and development of mobile code which complies with the Protection Profile for Web Browsers and Application SRG. DoD has determined the requirements are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented requirements to ensure the organization being inspected/assessed defines requirements for the acquisition, development, and use of mobile code. DoD has determined the requirements are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-18(3)	CCI-001169	The information system prevents the download of organization-defined unacceptable mobile code.	The organization being inspected/assessed configures the information system to prevent the download of unacceptable mobile code defined in CCI 2459. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1169.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent the download of unacceptable mobile code defined in CCI 2459. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1169.	MOD		X	X					3.7.3 Mobile Code In MODERATE Impact Syst...		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-18(4)	CCI-001170	The information system prevents the automatic execution of mobile code in organization-defined software applications.	The organization being inspected/assessed configures the information system to prevent the automatic execution of unacceptable mobile code in software applications defined in CCI 1171. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1170.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent the automatic execution of unacceptable mobile code in software applications defined in CCI 1171. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1170.	MOD		X						3.7.3 Mobile Code In MODERATE Impact Syst...		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-18(4)	CCI-001171	The organization defines software applications in which automatic mobile code execution is to be prohibited	DoD has defined the software applications in which automatic mobile code execution is to be prohibited as the software applications defined in the Protection Profile for Web Browsers and Application SRG.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the software applications in which automatic mobile code execution is to be prohibited as the software applications defined in the Protection Profile for Web Browsers and Application SRG.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-18(4)	CCI-001172	The organization defines actions to be enforced by the information system before executing mobile code.	DoD has defined the actions as the user be prompted.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the actions as the user be prompted.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-19(a)	CCI-001173	The organization establishes usage restrictions for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.	The organization being inspected/assessed establishes and documents usage restrictions for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.	The organization conducting the inspection/assessment obtains and examines the documented usage restrictions to ensure the organization being inspected/assessed establishes usage restrictions for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.	MOD				X				---	CS does not use VoIP	
N/A	SC-19(a)	CCI-001174	The organization establishes implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.	The Voice and Video over Internet Protocol (V-VoIP) STIG meets the DoD requirement for establishing implementation guidance for Voice over Internet Protocol (VoIP) technologies. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, V-VoIP STIG.	The V-VoIP STIG meets the DoD requirement for establishing implementation guidance for Voice over Internet Protocol (VoIP) technologies. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, V-VoIP STIG.	MOD				X				---	CS does not use VoIP	
N/A	SC-19(b)	CCI-001175	The organization authorizes the use of VoIP within the information system.	The organization being inspected/assessed authorizes any appropriate usage of VoIP within the information system and documents those authorizations.	The organization conducting the inspection/assessment obtains and examines the documented authorizations and *insert language* to ensure the organization being inspected/assessed authorizes any appropriate usage of VoIP within the information system and documents those authorizations.	MOD				X				---	CS does not use VoIP	
N/A	SC-19(b)	CCI-001176	The organization monitors the use of VoIP within the information system.	The organization being inspected/assessed documents and implements a process to monitor the use of VoIP within the information system. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trial of monitoring to ensure the organization being inspected/assessed monitors the use of VoIP within the information system.	MOD				X				---	CS does not use VoIP	
N/A	SC-19(b)	CCI-001177	The organization controls the use of VoIP within the information system.	The organization being inspected/assessed designs the information system to control the use of VoIP within the information system	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying the use of VoIP to ensure the organization being inspected/assessed controls the use of VoIP within the information system.	MOD				X				---	CS does not use VoIP	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-20(a)	CCI-001178	The information system provides additional data origin authentication artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.	The organization being inspected/assessed configures the authoritative name server software for external queries to enable DNSSEC and creates resource records with digital signatures (RRSig) for each A record. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 1178.	The organization conducting the inspection/assessment: 1. inspects the configuration files for the presence of DNSSEC records for each A record hosted in a zone; 2. utilizes DNSSEC diagnostic tools, such as dig; and 3. performs queries which will exercise the data flow path for authoritative name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 1178.	LOW				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-20(b)	CCI-001179	The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child zones.	The organization being inspected/assessed configures the authoritative name server software to enable DNSSEC and creates delegation signer (DS) resource records for each child zone and place those records in the parent zone. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 1179.	The organization conducting the inspection/assessment inspect the configuration files for the presence of Delegation Signer (DS) Records for any child domains. Note: This is only applicable for zones with child domains. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 1179.	LOW				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-22	CCI-001182	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant.	The organization being inspected/assessed implements a name service resolution architecture consisting of primary and secondary servers. The organization must document the architecture in the site security plan. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1182.	The organization conducting the inspection/assessment reviews the sites implementation documentation of the name resolution servers and verifies primary and alternate services are available. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1182.	LOW				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-22	CCI-001183	The information systems that collectively provide name/address resolution service for an organization implement internal/external role separation.	The organization being inspected/assessed implements a name service resolution architecture where recursive and authoritative server software is not installed on the same information system. The organization must document the architecture in the site security plan. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1183.	The organization conducting the inspection/assessment reviews the sites implementation documentation of the name resolution servers and verifies authoritative and recursive services are not hosted on the same information system. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1183.	LOW				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-23	CCI-001184	The information system protects the authenticity of communications sessions.	The organization being inspected/assessed configures the information system to protect the authenticity of communications sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1184.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect the authenticity of communications sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1184.	MOD	X	X		X				3.2.7 Device Identification and Authentic...		CCI requirements are addressed within subparagraph "Device Identification and Authentication" of UFGS 25 05 11.
N/A	SC-23(1)	CCI-001185	The information system invalidates session identifiers upon user logout or other session termination.	The organization being inspected/assessed configures the information system to invalidate session identifiers upon user logout or other session termination. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1185.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to invalidate session identifiers upon user logout or other session termination. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1185.	MOD		X						3.2.6 Cryptographic Protection	FRCS does not contain classified information	
N/A	SC-23(3)	CCI-001188	The information system generates unique session identifiers for each session with organization-defined randomness requirements.	The organization being inspected/assessed configures the information system to generate unique session identifiers for each session with randomness requirements defined in SC-23 (3), CCI 1189. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1188.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to generate unique session identifiers for each session with randomness requirements defined in SC-23 (3), CCI 1189. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1188.	MOD		X						3.2.6 Cryptographic Protection	FRCS does not contain classified information	
N/A	SC-23(3)	CCI-001189	The organization defines randomness requirements for generating unique session identifiers.	The organization being inspected/assessed defines and documents randomness requirements for generating unique session identifiers. DoD has determined the randomness requirements are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented randomness requirements to ensure the organization being inspected/assessed defines randomness requirements for generating unique session identifiers. DoD has determined the randomness requirements are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-24	CCI-001190	The information system fails to an organization-defined known-state for organization-defined types of failures.	The organization being inspected/assessed configures the information system to fail to a secure state for failures during system initialization, shutdown, and aborts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1190. DoD has defined the known state as secure state. DoD has defined the types of failures as failures during system initialization, shutdown, and aborts.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to fail to a secure state for failures during system initialization, shutdown, and aborts. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1190. DoD has defined the known state as secure state. DoD has defined the types of failures as failures during system initialization, shutdown, and aborts.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-24	CCI-001191	The organization defines the known states the information system should fail to in the event of a organization-defined system failure.	DoD has defined the known state as secure state.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the known state as secure state.	MOD		X		X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-24	CCI-001192	The organization defines types of failures for which the information system should fail to an organization-defined known state.	DoD has defined the types of failures as failures during system initialization, shutdown, and aborts.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the types of failures as failures during system initialization, shutdown, and aborts.	MOD		X		X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-24	CCI-001193	The organization defines system state information that should be preserved in the event of a system failure.	DoD has defined system state information as information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined system state information as information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes.	MOD		X		X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-28	CCI-001199	The information system protects the confidentiality and/or integrity of organization-defined information at rest.	The organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of organization-defined information at rest. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1199.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of organization-defined information at rest. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1199.	MOD	X	X		X				3.7.4 Protection of Information at Rest I...	FRCS does not contain PII, CUI, or classified information	
N/A	SI-1(a)(1)	CCI-001217	The organization develops and documents a system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-1(a)(1)	CCI-001218	The organization disseminates the system and information integrity policy to organization-defined personnel or roles.	DoD disseminates DoDI 8510.01 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) that meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-1(b)(1)	CCI-001219	The organization reviews and updates system and information integrity policy in accordance with organization-defined frequency.	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-1(a)(2)	CCI-001220	The organization develops and documents procedures to facilitate the implementation of the system and information integrity policy and associated system integrity controls.	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) .	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-1(a)(2)	CCI-001221	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the system and information integrity policy and associated system integrity controls.	DoD disseminates DoDI 8510.01 via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) that meets the DoD requirement for a system and information integrity policy. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-1(b)(2)	CCI-001222	The organization reviews and updates system and information integrity procedures in accordance with organization-defined frequency.	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	Documenting and implementing the Risk Management Framework (RMF) for DoD IT (DoDI 8510.01) meets the DoD requirement for a system and information integrity procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, Risk Management Framework (RMF) for DoD IT (DoDI 8510.01).	LOW					X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-1(b)(1)	CCI-001223	The organization defines the frequency of system and information integrity policy reviews and updates.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10.	LOW					X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-1(b)(2)	CCI-001224	The organization defines the frequency of system and information integrity procedure reviews and updates	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW					X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-2(a)	CCI-001225	The organization identifies information system flaws.	The organization being inspected/assessed documents and implements a process to identify information system flaws. The process shall include review of the system through automated scans and manual checks to determine the existence of flaws such as IAVM, CVE, or other resources.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed identifies information system flaws.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-2(a)	CCI-001226	The organization reports information system flaws.	The organization being inspected/assessed reports information system flaws according to DoD Cybersecurity policy and organizational roles and responsibilities. The organization must report information system flaws in their POA&M.	The organization conducting the inspection/assessment obtains and examines the authorization package, verifies the POA&M is up to date and includes recently identified information system flaws, and verifies that the organization has notified appropriate personnel as defined by DoD Cybersecurity policy and organizational roles and responsibilities.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-2(a)	CCI-001227	The organization corrects information system flaws.	The organization being inspected/assessed corrects information system flaws within the time period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs). The organization documents the corrections on their POA&M. DoD has defined the time period as within the time period directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines the information system POA&M and examines the information system to ensure the organization being inspected/assessed corrects information system flaws.	LOW	X		X	X					1.10 SOFTWARE LICENSING		CCI requirements are addressed within subparagraph "Software Licensing" of UFGS 25 05 11.
N/A	SI-2(b)	CCI-001228	The organization tests software updates related to flaw remediation for effectiveness before installation.	The organization being inspected/assessed documents and implements a process to test software updates related to flaw remediation for effectiveness before installation. If the software update is being provided by a vendor who has documented the effectiveness of the update in fixing the affected IAVM/CVE, further testing by the organization may not be required.	The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests software updates related to flaw remediation for effectiveness before installation.	LOW	X		X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-2(b)	CCI-001229	The organization tests software updates related to flaw remediation for potential side effects before installation.	The organization being inspected/assessed documents and implements a process for regression testing IAW CM-4 to identify any potential side effects before installation of software updates.	The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests software updates related to flaw remediation for potential side effects before installation.	LOW	X		X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-2(d)	CCI-001230	The organization incorporates flaw remediation into the organizational configuration management process.	The organization being inspected/assessed documents within their configuration management plan, flaw remediation processes.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure that it incorporates flaw remediation.	LOW			X						---		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	SI-2(1)	CCI-001231	The organization centrally manages the flaw remediation process.	The organization being inspected/assessed documents and implements a process to centrally manage the flaw remediation process.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed centrally manages the flaw remediation process.	MOD			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-2(2)	CCI-001233	The organization employs automated mechanisms on an organization-defined frequency to determine the state of information system components with regard to flaw remediation.	The organization being inspected/assessed configures the information system to employ automated mechanisms continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP to determine the state of information system components with regard to flaw remediation. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1233. DoD has defined the frequency as continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to employ automated mechanisms continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP to determine the state of information system components with regard to flaw remediation. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1233. DoD has defined the frequency as continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP.	MOD	X			X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-2(2)	CCI-001234	The organization defines a frequency for employing automated mechanisms to determine the state of information system components with regard to flaw remediation.	DoD has defined the frequency as continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by (Computer Network Defense Service Provider) CNDSP.	MOD	X			X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-3(b)	CCI-001240	The organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures.	The organization being inspected/assessed configures the information system to update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1240.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1240.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-3(c)(1)	CCI-001241	The organization configures malicious code protection mechanisms to perform periodic scans of the information system on an organization-defined frequency.	The organization being inspected/assessed configures malicious code protection mechanisms to perform periodic scans of the information system on every 7 days. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1241. DoD has defined the frequency as every 7 days.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform periodic scans of the information system on every 7 days. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1241. DoD has defined the frequency as every 7 days.	LOW	X	X	X					3.13.1 Malicious Code Protection	FRCS has no computers	
N/A	SI-3(c)(1)	CCI-001242	The organization configures malicious code protection mechanisms to perform real-time scans of files from external sources at endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy.	The organization being inspected/assessed configures malicious code protection mechanisms to perform real-time scans of files from external sources at endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1242.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform real-time scans of files from external sources at endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1242.	LOW	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-3(c)(2)	CCI-001243	The organization configures malicious code protection mechanisms to perform organization-defined action(s) in response to malicious code detection.	The organization being inspected/assessed configures malicious code protection mechanisms to perform block and quarantine malicious code and then send an alert to the administrator immediately in near real-time in response to malicious code detection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1243. DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform block and quarantine malicious code and then send an alert to the administrator immediately in near real-time in response to malicious code detection. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1243. DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-3(c)(2)	CCI-001244	The organization defines one or more actions to perform in response to malicious code detection, such as blocking malicious code, quarantining malicious code, or sending alert to administrator.	DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the actions as block and quarantine malicious code and then send an alert to the administrator immediately in near real-time.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-3(d)	CCI-001245	The organization addresses the receipt of false positives during malicious code detection and eradication, and the resulting potential impact on the availability of the information system.	The organization being inspected/assessed configures the information system to address the receipt of false positives during malicious code detection and eradication, and the resulting potential impact on the availability of the information system. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1245.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to address the receipt of false positives during malicious code detection and eradication, and the resulting potential impact on the availability of the information system. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1245.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-3(1)	CCI-001246	The organization centrally manages malicious code protection mechanisms.	The organization being inspected/assessed documents and implements a process to centrally manage malicious code protection mechanisms.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed centrally manages malicious code protection mechanisms.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-3(2)	CCI-001247	The information system automatically updates malicious code protection mechanisms.	The organization being inspected/assessed configures the information system to automatically update malicious code protection mechanisms. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1247.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically update malicious code protection mechanisms. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1247.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(a)(1)	CCI-001253	The organization defines the objectives of monitoring for attacks and indicators of potential attacks on the information system.	DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	LOW	X	X		X	X			3.13.3 Information System Monitoring	No requirements for Information System Monitoring given by the client	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-4(c)	CCI-001255	The organization deploys monitoring devices strategically within the information system to collect organization determined essential information.	The organization being inspected/assessed documents and implements a process to deploy monitoring devices strategically within the information system to collect organization determined essential information.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed deploys monitoring devices strategically within the information system to collect organization determined essential information.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(c)	CCI-001256	The organization deploys monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization.	The organization being inspected/assessed documents and implements a process to deploy monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed deploys monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(e)	CCI-001257	The organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	The organization being inspected/assessed documents and implements a process to heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(f)	CCI-001258	The organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	The organization being inspected/assessed obtains and documents legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	The organization conducting the inspection/assessment obtains and examines the documented legal opinion to ensure the organization being inspected/assessed obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(2)	CCI-001260	The organization employs automated tools to support near real-time analysis of events.	The organization being inspected/assessed documents and implements automated tools to support near real-time analysis of events.	The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified automated tools to ensure the organization being inspected/assessed employs automated tools to support near real-time analysis of events. The organization being inspected/assessed may be required to demonstrate use of their automated tools.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(5)	CCI-001264	The organization defines indicators of compromise or potential compromise to the security of the information system which will result in information system alerts being provided to organization-defined personnel or roles.	DoD has defined the compromise indicators as real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the compromise indicators as real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(11)	CCI-001273	The organization analyzes outbound communications traffic at the external boundary of the information system to discover anomalies.	The organization being inspected/assessed documents and implements a process to analyze outbound communications traffic at the external boundary of the information system to discover anomalies. The organization must maintain a record of any discovered anomalies.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of any discovered anomalies to ensure the organization being inspected/assessed analyzes outbound communications traffic at the external boundary of the information system to discover anomalies.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(12)	CCI-001274	The organization employs automated mechanisms to alert security personnel of an organization-defined inappropriate or unusual activities with security implications.	The organization being inspected/assessed documents and implements automated mechanisms to alert security personnel when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B. For automated alert mechanisms that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1274. DoD has defined the activities that trigger alerts as when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B.	The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified automated mechanisms used to alert security personnel when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B. For automated alert mechanisms that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1274. The organization being inspected/assessed may be required to demonstrate use of their identified automated mechanisms. DoD has defined the activities that trigger alerts as when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(12)	CCI-001275	The organization defines the activities which will trigger alerts to security personnel of inappropriate or unusual activities.	DoD has defined the activities that trigger alerts as when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the activities that trigger alerts as when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-4(15)	CCI-001282	The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	The organization being inspected/assessed documents and implements an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified intrusion detection system to ensure the organization being inspected/assessed employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks. The organization being inspected/assessed may be required to demonstrate use of the intrusion detection system.	MOD	X		X	X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(16)	CCI-001283	The organization correlates information from monitoring tools employed throughout the information system.	The organization being inspected/assessed documents and implements a process to correlate information from monitoring tools employed throughout the information system.	The organization conducting the inspection/assessment obtains and examines the documented process and the correlated results to ensure the organization being inspected/assessed correlates information from monitoring tools employed throughout the information system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-5(a)	CCI-001285	The organization receives information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis.	The organization being inspected/assessed receives information system security alerts, advisories, and directives from at a minimum, USCYBERCOM on an ongoing basis. DoD has defined the external organizations as at a minimum, USCYBERCOM.	The organization conducting the inspection/assessment obtains and examines alerts, advisories, and directives received by the organization being inspected/assessed to ensure they receive information system security alerts, advisories, and directives from at a minimum, USCYBERCOM on an ongoing basis. DoD has defined the external organizations as at a minimum, USCYBERCOM.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-5(b)	CCI-001286	The organization generates internal security alerts, advisories, and directives as deemed necessary.	The organization being inspected/assessed documents and implements a process to generate internal security alerts, advisories, and directives as deemed necessary.	The organization conducting the inspection/assessment obtains and examines documented process as well as the generated internal security alerts, advisories, and directives to ensure the organization being inspected/assessed generates internal security alerts, advisories, and directives as deemed necessary.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-5(c)	CCI-001287	The organization disseminates security alerts, advisories, and directives to organization-defined personnel or roles, organization-defined elements within the organization, and/or organization-defined external organizations.	The organization being inspected/assessed disseminates security alerts, advisories, and directives to the ISSO and ISSM and/or external organizations defined in SI-5, CCI 2694. DoD has defined the personnel or roles as the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines any applicable artifacts showing dissemination of security alerts, advisories, and directives to ensure the organization being inspected/assessed disseminates security alerts, advisories, and directives to the ISSO and ISSM and/or external organizations defined in SI-5, CCI 2694. DoD has defined the personnel or roles as the ISSO and ISSM.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-5(c)	CCI-001288	The organization defines the personnel or roles to whom the organization will disseminate security alerts, advisories and directives.	DoD has defined the personnel or roles as the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSO and ISSM.	LOW	X				X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-5(d)	CCI-001289	The organization implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	The organization being inspected/assessed implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	The organization conducting the inspection/assessment examines the information system and obtains and examines records of compliance and/or non-compliance reporting to ensure that security directives have been implemented in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	LOW	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-8(b)	CCI-001306	The organization updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	The organization being inspected/assessed documents and implements a process to update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	The organization conducting the inspection/assessment obtains and examines the documented process and examines the spam protection mechanisms to ensure the organization being inspected/assessed updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	MOD								---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-8(1)	CCI-001307	The organization centrally manages spam protection mechanisms.	The organization being inspected/assessed documents and implements a process to centrally manage spam protection mechanisms.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed centrally manages spam protection mechanisms.	MOD				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-8(2)	CCI-001308	The information system automatically updates spam protection mechanisms .	The organization being inspected/assessed configures the information system to automatically update spam protection mechanisms. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1308.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically update spam protection mechanisms. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1308.	MOD				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-10	CCI-001310	The information system checks the validity of organization-defined inputs.	The organization being inspected/assessed configures the information system to check the validity of all inputs except those identified specifically by the organization. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1310. DoD has defined the information inputs as all inputs except those identified specifically by the organization.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to check the validity of all inputs except those identified specifically by the organization. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1310. DoD has defined the information inputs as all inputs except those identified specifically by the organization.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-11(a)	CCI-001312	The information system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.	The organization being inspected/assessed configures the information system to generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1312.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1312.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-11(b)	CCI-001314	The information system reveals error messages only to organization-defined personnel or roles.	The organization being inspected/assessed configures the information system to reveal error messages only to the ISSO, ISSM, and SCA. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1314. DoD has defined the personnel or roles as the ISSO, ISSM, and SCA.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to reveal error messages only to the ISSO, ISSM, and SCA. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1314. DoD has defined the personnel or roles as the ISSO, ISSM, and SCA.	MOD			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-12	CCI-001315	The organization handles information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization being inspected/assessed identifies and documents federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system. The organization documents and implements a process to handle information IAW those documented federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization conducting the inspection/assessment obtains and examines the documented list of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system, as well as the documented process for information handling to ensure the organization being inspected/assessed handles information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AT-4(b)	CCI-001336	The organization retains individual training records for an organization-defined time period.	The organization being inspected/assessed will maintain records training records for at least 5 years or 5 years after completion of a specific training program. DoD has defined the frequency as at least 5 years or 5 years after completion of a specific training program.	The organization conducting the inspection/assessment obtains and examines training records to ensure records have been maintained for at least 5 years or 5 years after completion of a specific training program. DoD has defined the frequency as at least 5 years or 5 years after completion of a specific training program.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-4(b)	CCI-001337	The organization defines a time period for retaining individual training records.	DoD has defined the frequency as at least 5 years or 5 years after completion of a specific training program.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least 5 years or 5 years after completion of a specific training program.	LOW				X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-9(4)(a)	CCI-001351	The organization authorizes access to management of audit functionality to only organization-defined subset of privileged users.	The organization being inspected/assessed authorizes access to the management of audit functionality to only the subset of privileged users defined in AU-9 (4), CCI 1894.	The organization conducting the inspection/assessment obtains and examines the documentation of access authorizations for the management of audit functionality to ensure only the subset of privileged users defined in AU-9 (4), CCI 1894 have been granted access authorization.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(7)(a)	CCI-001358	The organization establishes privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.	The organization being inspected/assessed documents and implements a process to establish privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.	The organization conducting the inspection/assessment obtains and examines documented processes for privileged user account creation to ensure the organization being inspected/assessed establishes privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(7)(b)	CCI-001360	The organization monitors privileged role assignments.	The organization being inspected/assessed implements a process to monitor privileged role assignments. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the audit trail of monitoring to ensure the organization being inspected/assessed monitors privileged role assignments.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(2)	CCI-001361	The organization defines a time period after which temporary accounts are automatically terminated.	DoD has defined the time period as 72 hours. The time period of 72 hours applies to temporary user accounts.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 72 hours. The time period of 72 hours applies to temporary user accounts.	MOD	X	X	X	X	X			3.3.1 User Accounts		CCI requirements are met within subparagraph "User Accounts" of UFGS 25 05 11.
N/A	AC-2(2)	CCI-001365	The organization defines a time period after which emergency accounts are automatically terminated.	DoD has defined the time period as never. The time period of never applies to emergency admin accounts.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as never. The time period of never applies to emergency admin accounts.	MOD	X	X	X	X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-4	CCI-001368	The information system enforces approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.	The organization being inspected/assessed configures the information system to enforce approved authorizations for controlling the flow of information within the system based on information flow control policies defined in AC-4, CCI 1548. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1368.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce approved authorizations for controlling the flow of information within the system based on information flow control policies defined in AC-4, CCI 1548. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1368.	MOD	X	X		X				3.2.1 Information Flow Enforcement In MOD...	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-5(b)	CCI-001380	The organization documents separation of duties of individuals.	The organization being inspected/assessed documents separation of duties of individuals.	The organization conducting the inspection/assessment obtains and examines the documented separation of duties to ensure the organization being inspected/assessed documents separation of duties of individuals.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-8(c)(1)	CCI-001384	The information system, for publicly accessible systems, displays system use information organization-defined conditions before granting further access.	The organization being inspected/assessed configures the information system to display the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," March 2013 before granting further access for publicly accessible systems For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1384. DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," March 2013.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," March 2013 before granting further access for publicly accessible systems For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1384. DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement," March 2013.	LOW								---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-8(c)(2)	CCI-001385	The information system, for publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.	The organization being inspected/assessed configures the information system to display references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1385.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1385.	LOW								---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-8(c)(2)	CCI-001386	The information system for publicly accessible systems displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.	The organization being inspected/assessed configures the information system to display references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1386.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1386.	LOW								---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-8(c)(2)	CCI-001387	The information system for publicly accessible systems displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.	The organization being inspected/assessed configures the information system to display references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1387.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to display references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1387.	LOW								---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-8(c)(3)	CCI-001388	The information system, for publicly accessible systems, includes a description of the authorized uses of the system.	The organization being inspected/assessed configures the information system to include a description of the authorized uses of the system for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1388.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to include a description of the authorized uses of the system for publicly accessible systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1388.	LOW								---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(4)	CCI-001403	The information system automatically audits account modification actions.	The organization being inspected/assessed configures the information system to automatically audit account modification actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1403.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically audit account modification actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1403.	MOD	X	X		X				3.3.1 User Accounts		CCI requirements are met within subparagraph "User Accounts" of UFGS 25 05 11.
N/A	AC-2(4)	CCI-001404	The information system automatically audits account disabling actions.	The organization being inspected/assessed configures the information system to automatically audit account disabling actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1404.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically audit account disabling actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1404.	MOD	X	X		X				3.3.1 User Accounts		CCI requirements are met within subparagraph "User Accounts" of UFGS 25 05 11.
N/A	AC-2(4)	CCI-001405	The information system automatically audits account removal actions.	The organization being inspected/assessed configures the information system to automatically audit account removal actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1405.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically audit account removal actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1405.	MOD	X	X		X				3.3.1 User Accounts		CCI requirements are met within subparagraph "User Accounts" of UFGS 25 05 11.
N/A	AC-2(5)(a)	CCI-001406	The organization defines a time period of expected inactivity when users are required to log out.	DoD has defined the time period as at the end of the users standard work period unless otherwise defined in formal organizational policy.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as at the end of the users standard work period unless otherwise defined in formal organizational policy.	MOD			X		X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(7)(a)	CCI-001407	The organization administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.	The organization being inspected/assessed documents and implements a process to administer privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.	The organization conducting the inspection/assessment obtains and examines documented processes for privileged user account creation to ensure the organization being inspected/assessed administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-4	CCI-001414	The information system enforces approved authorizations for controlling the flow of information between interconnected systems based on organization-defined information flow control policies.	The organization being inspected/assessed configures the information system to enforce approved authorizations for controlling the flow of information between interconnected systems based on information flow control policies defined in AC-4, CCI 1549. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1414.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce approved authorizations for controlling the flow of information between interconnected systems based on information flow control policies defined in AC-4, CCI 1549. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1414.	MOD	X	X		X				3.2.1 Information Flow Enforcement In MOD...	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-6(2)	CCI-001419	The organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access.	DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.	MOD		X		X	X			3.3.1 User Accounts 3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION"within Part 3
N/A	AC-7(a)	CCI-001423	The organization defines the time period in which the organization-defined maximum number of consecutive invalid logon attempts occur.	DoD has defined the time period as 15 minutes.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 15 minutes.	LOW		X		X	X			3.3.2 Unsuccessful Logon Attempts		Cybersecurity requirements are met for log in attempts within Sub-Paragraph "Unsuccessful Logon Attempts" within Part 3
N/A	AC-18(a)	CCI-001438	The organization establishes usage restrictions for wireless access.	The organization being inspected/assessed establishes and documents usage restrictions for wireless access.	The organization conducting the inspection/assessment obtains and examines documented usage restrictions to ensure the organization being inspected/assessed establishes usage restrictions for wireless access.	LOW		X	X					3.2.3 Wireless and Wired Broadcast Commun...	Specification is for Fire Protection systems only, therefore this CCI is not included	
N/A	AC-18(a)	CCI-001439	The organization establishes implementation guidance for wireless access.	The organization being inspected/assessed establishes and documents implementation guidance for wireless access.	The organization conducting the inspection/assessment obtains and examines the documented implementation guidance to ensure the organization being inspected/assessed establishes implementation guidance for wireless access.	LOW		X	X					3.2.3 Wireless and Wired Broadcast Commun...	Specification is for Fire Protection systems only, therefore this CCI is not included	
N/A	AC-18(b)	CCI-001441	The organization authorizes wireless access to the information system prior to allowing such connections.	The organization being inspected/assessed authorizes wireless access to the information system prior to allowing such connections. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes wireless access to the information system prior to allowing such connections.	LOW		X	X					3.2.3 Wireless and Wired Broadcast Commun...	Specification is for Fire Protection systems only, therefore this CCI is not included	
N/A	AC-18(1)	CCI-001443	The information system protects wireless access to the system using authentication of users and/or devices.	The organization being inspected/assessed configures the information system to protect wireless access to the system using authentication of users and/or devices. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1443.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect wireless access to the system using authentication of users and/or devices. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1443.	MOD		X		X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-18(1)	CCI-001444	The information system protects wireless access to the system using encryption.	The organization being inspected/assessed configures the information system to protect wireless access to the system using encryption. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1444.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect wireless access to the system using encryption. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1444.	MOD		X		X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-18(3)	CCI-001449	The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.	The organization being inspected/assessed documents and implements a process to disable wireless networking capabilities internally embedded within information system components prior to issuance and deployment when not intended for use.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment. The organization conducting the inspection/assessment obtains and examines a sampling of information systems to ensure that any internally embedded wireless networking capabilities are disabled unless a documented need exists.	MOD		X						---	Specification is for Fire Protection systems only, therefore this CCI is not included	
N/A	AC-17(2)	CCI-001453	The information system implements cryptographic mechanisms to protect the integrity of remote access sessions.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the integrity of remote access sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1453.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the integrity of remote access sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1453.	MOD	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-12(a)	CCI-001459	The organization defines information system components that provide audit record generation capability.	DoD has defined the information system components as all information system and network components.	DoD has defined the information system components as all information system and network components.	LOW		X		X	X			3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-14(2)	CCI-001462	The information system provides the capability for authorized users to capture/record and log content related to a user session.	The organization being inspected/assessed configures the information system to provide the capability for authorized users to capture/record and log content related to a user session. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1462.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for authorized users to capture/record and log content related to a user session. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1462.	MOD		X	X					3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-14(1)	CCI-001464	The information system initiates session audits at system start-up.	The organization being inspected/assessed configures the information system to initiate session audits at system start-up. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1464.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to initiate session audits at system start-up. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1464.	MOD		X	X					3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-21(a)	CCI-001470	The organization defines information sharing circumstances where user discretion is required.	The organization being inspected/assessed defines and documents information sharing circumstances where user discretion is required. DoD has determined the information sharing circumstances are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information sharing circumstances to ensure the organization being inspected/assessed defines information sharing circumstances where user discretion is required. DoD has determined the information sharing circumstances are not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-21(b)	CCI-001471	The organization employs organization-defined automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions.	The organization being inspected/assessed implements the process defined in AC-21, CCI 1472 to assist users in making information sharing/collaboration decisions.	The organization conducting the inspection/assessment obtains and examines the documented process defined per AC-21, CCI 1472 to ensure the organization being inspected/assessed assists users in making information sharing/collaboration decisions.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-21(b)	CCI-001472	The organization defines the automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions.	The organization being inspected/assessed defines and documents the automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions. DoD has determined the automated mechanisms or manual processes are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented automated mechanisms to ensure the organization being inspected/assessed defines the automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions. DoD has determined the automated mechanisms or manual processes are not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-22(a)	CCI-001473	The organization designates individuals authorized to post information onto a publicly accessible information system.	The organization being inspected/assessed identifies and documents individuals authorized to post information onto a publicly accessible information system.	The organization conducting the inspection/assessment obtains and examines the list of individuals to ensure the organization being inspected/assessed designates individuals authorized to post information onto a publicly accessible information system.	LOW				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AC-22(b)	CCI-001474	The organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information.	The organization being inspected/assessed documents and implements a process to train authorized individuals to ensure that publicly accessible information does not contain nonpublic information. The organization must maintain an audit trail of the training conducted.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of the training conducted to ensure the organization being inspected/assessed trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information.	LOW				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AC-22(c)	CCI-001475	The organization reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.	The organization being inspected/assessed	The organization conducting the inspection/assessment obtains and examines	LOW				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AC-22(d)	CCI-001476	The organization reviews the content on the publicly accessible information system for nonpublic information on an organization-defined frequency.	The organization being inspected/assessed documents and implements a process to review the content on the publicly accessible information system for nonpublic information on an organization-defined frequency. The organization must maintain an audit trail of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reviews to ensure the organization being inspected/assessed reviews the content on the publicly accessible information system for nonpublic information on an organization-defined frequency.	LOW				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AC-22(d)	CCI-001477	The organization defines a frequency for reviewing the content on the publicly accessible information system for nonpublic information.	DoD has defined the frequency as every 90 days or as new information is posted.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 90 days or as new information is posted.	LOW				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AC-22(e)	CCI-001478	The organization removes nonpublic information from the publicly accessible information system, if discovered.	The organization being inspected/assessed documents and implements a process to remove nonpublic information from the publicly accessible information system, if discovered.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed removes nonpublic information from the publicly accessible information system, if discovered.	LOW				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AT-2(c)	CCI-001479	The organization provides refresher security awareness training to all information system users (including managers, senior executives, and contractors) in accordance with the organization-defined frequency.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	DoDD 8570.01 meets the DoD requirement for IA awareness training policy and procedures. DISA's DoD IA awareness CBT is the DoD baseline standard. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDD 8570.01.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-2	CCI-001480	The organization defines the frequency for providing refresher security awareness training to all information system users (including managers, senior executives, and contractors).	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level (DoDD 8570.01). DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-2(d)	CCI-001484	The organization defines frequency of (or situation requiring) auditing for each identified event.	DoD has defined the frequency as all auditable events defined in AU-2 (a) per occurrence.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as all auditable events defined in AU-2 (a) per occurrence.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-2(d)	CCI-001485	The organization defines the events which are to be audited on the information system on an organization-defined frequency of (or situation requiring) auditing for each identified event.	The organization being inspected/assessed defines and documents events which are to be audited on the information system. Events should be selected from the events the information system is capable of auditing as defined in AU-2 (a) and should be based on ongoing risk assessments of current threat information and environment. DoD has determined that the events are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented list of events which are to be audited on the information system to ensure those events have been defined. DoD has determined that the events are not appropriate to define at the Enterprise level.	LOW		X	X					3.5.1 Audit Events, Content of Audit Reco…		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-2(3)	CCI-001486	The organization defines a frequency for reviewing and updating the list of organization-defined auditable events.	DoD has defined the frequency as annually or more frequently upon changes to situational awareness of threats or vulnerabilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually or more frequently upon changes to situational awareness of threats or vulnerabilities.	MOD					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-3	CCI-001487	The information system generates audit records containing information that establishes the identity of any individuals or subjects associated with the event.	The organization being inspected/assessed configures the information system to generate audit records containing information that establishes the identity of any individuals or subjects associated with the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1487.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate audit records containing information that establishes the identity of any individuals or subjects associated with the event. The organization conducting the inspection/assessment reviews the audit records generated to ensure that the records contain information that establishes the identity of any individuals or subjects associated with the event. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1487.	LOW		X		X				3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-3(1)	CCI-001488	The organization defines additional, more detailed information to be included in the audit records.	The organization being inspected/assessed defines and documents additional, more detailed information to be included in the audit records. The additional information must include at a minimum, full-text recording of privileged commands or the individual identities of group account users. The additional information must provide sufficient detail to reconstruct events to determine cause of compromise and magnitude of damage, malfunction, or security violation. DoD has determined that additional, more detailed information must include, at a minimum, full-text recording of privileged commands or the individual identities of group account users. DoD has determined that all additional, more detailed information is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented list of additional more detailed information to be included in the audit records to ensure that: 1. The list is defined; and 2. The list includes full-text recording of privileged commands or the individual identities of group account users. DoD has determined that additional, more detailed information must include, at a minimum, full-text recording of privileged commands or the individual identities of group account users. DoD has determined that it is not appropriate to define at the Enterprise level.	MOD		X	X					3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-5(b)	CCI-001490	The organization defines actions to be taken by the information system upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).	The organization being inspected/assessed will define and document actions to be taken by the information system upon audit failure. The organization shall consider trade-offs between the needs for system availability and audit integrity when defining the actions. Unless availability is an overriding concern, the default action should be to shut down the information system. DoD has determined that the actions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented actions to ensure the organization being inspected/assessed has defined the actions to be taken by the information system upon audit failure. DoD has determined that the actions are not appropriate to define at the Enterprise level.	LOW	X	X	X	X				3.5.5 Response to Audit Processing Failur...	FRCS has no computers in scope	
N/A	AU-8(1)	CCI-001492	The organization defines an authoritative time source for the synchronization of internal information system clocks.	DoD has defined the authoritative time source as an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the authoritative time source as an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS).	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-9	CCI-001493	The information system protects audit tools from unauthorized access.	The organization being inspected/assessed configures the information system to disallow unauthorized access to audit tools. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1493.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized access to audit tools. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1493.	LOW	X			X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AU-9	CCI-001494	The information system protects audit tools from unauthorized modification.	The organization being inspected/assessed configures the information system to disallow unauthorized modification of audit tools. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1494.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized modification of audit tools. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1494.	LOW	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-9	CCI-001495	The information system protects audit tools from unauthorized deletion.	The organization being inspected/assessed configures the information system to disallow unauthorized deletion of audit tools. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1495.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to disallow unauthorized deletion of audit tools. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1495.	LOW	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CM-2(1)(a)	CCI-001497	The organization defines a frequency for the reviews and updates to the baseline configuration of the information system.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	MOD				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-5(6)	CCI-001499	The organization limits privileges to change software resident within software libraries.	The organization being inspected/assessed documents and implements a process to limit privileges to accounts authorized to change software resident within software libraries. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1499.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed limits privileges to change software resident within software libraries. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1499.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-6(d)	CCI-001502	The organization monitors changes to the configuration settings in accordance with organizational policies and procedures.	The organization being inspected/assessed develops and documents a process for monitoring changes to the configuration settings in accordance with organizational policies and procedures.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed monitors changes to the configuration settings in accordance with organizational policies and procedures.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-6(d)	CCI-001503	The organization controls changes to the configuration settings in accordance with organizational policies and procedures.	The organization being inspected/assessed develops and documents a process for controlling changes to the configuration settings in accordance with organizational policies and procedures.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed controls changes to the configuration settings in accordance with organizational policies and procedures.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-1(a)(1)	CCI-001504	The organization develops and documents a personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(a)(1)	CCI-001505	The organization disseminates a personnel security policy to organization-defined personnel or roles.	DoD disseminates DoD 5200.2-R via the DoD Issuance site: http://www.dtic.mil/whs/directives/corres/pub1.html to meet the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(b)(1)	CCI-001506	The organization reviews and updates the current personnel security policy in accordance with organization-defined frequency.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(b)(1)	CCI-001507	The organization defines the frequency to review and update the current personnel security policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(b)(2)	CCI-001508	The organization defines the frequency to review and update the current personnel security procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(a)(2)	CCI-001509	The organization develops and documents procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(a)(2)	CCI-001510	The organization disseminates personnel security procedures to organization-defined personnel or roles.	DoD disseminates DoD 5200.2-R via the DoD Issuance site: http://www.dtic.mil/whs/directives/corres/pub1.html to meet the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-1(b)(2)	CCI-001511	The organization reviews and updates the current personnel security procedures in accordance with organization-defined frequency.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for personnel security policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-2(a)	CCI-001512	The organization assigns a risk designation to all organizational positions.	The organization being inspected/assessed will designate and document all organizational positions, to include government and contract positions, with the appropriate ADP/IT level designation, IAW DoD 5200.2-R.	The organization conducting the inspection/assessment obtains and examines documentation of the ADP/IT level designations.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-2(b)	CCI-001513	The organization establishes screening criteria for individuals filling organizational positions.	DoD 5200.2-R meets the DoD requirements for establishing screening criteria for individuals filling organizational positions. DoD organizations are automatically compliant with this CCI as they are covered at the DoD level by DoD 5200.2-R.	DoD 5200.2-R meets the DoD requirements for establishing screening criteria for individuals filling organizational positions. DoD organizations are automatically compliant with this CCI as they are covered at the DoD level by DoD 5200.2-R.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-2(c)	CCI-001514	The organization reviews and updates position risk designations in accordance with organization-defined frequency.	The organization being inspected/assessed reviews position risk designations annually and revises designations as required based on the reviews. Records of these reviews must be maintained as an audit trail. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment reviews the audit records of the position designation reviews to ensure reviews are done annually. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-2(c)	CCI-001515	The organization defines the frequency to review and update position risk designations.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PS-3(a)	CCI-001516	The organization screens individuals prior to authorizing access to the information system.	The organization being inspected/assessed will screen all government and contract personnel to ensure they meet the appropriate ADP/IT level designation requirements IAW DoD 5200.2-R prior to authorizing access to the information system.	The organization conducting the inspection/assessment obtains and examines the information system access list (AC-2) and compares a sampling of authorized users to manning documents (PS-2) to ensure access was granted appropriately IAW ADP/IT level designation requirements within DoD 5200.2-R.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-3(b)	CCI-001517	The organization rescreens individuals with authorized access to the information system according to organization-defined conditions requiring rescreening, and where rescreening is so indicated, the organization-defined frequency of such rescreening.	The information system owner will rescreen individuals according to system owner defined list of conditions requiring rescreening (CCI-001518) individuals for access to the information system and frequency (CCI - 001519) of such rescreening. Rescreening actions will be maintained as an audit trail (AU-2).	The organization conducting the inspection/assessment obtains and examines audit records of rescreening actions to ensure the system owner is rescreening individuals according to a system owner-defined list of conditions requiring rescreening and, where re-screening is so indicated, based on the system owner-defined frequency of such rescreening.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-3(b)	CCI-001518	The organization defines the conditions requiring rescreening of individuals with authorized access to the information system.	The information system owner will develop and document the list of conditions requiring rescreening individuals for access to the information system. DoD has determined the list of conditions is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documentation of conditions requiring rescreening of individuals for access to the information system. DoD has determined the list of conditions is not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-3(b)	CCI-001519	The organization defines the frequency for rescreening individuals with authorized access to the information system when organization-defined conditions requiring rescreening are met.	The information system owner will define and document the required frequency of rescreening for access to the information system. DoD has determined the frequency is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documentation defining the required frequency for rescreening individuals for access to the system. DoD has determined the frequency is not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(a)	CCI-001522	The organization, upon termination of individual employment, disables information system access within organization-defined time period.	The organization being inspected/assessed upon termination of individual employment, terminates information system access immediately and IAW organization security policy and procedures. The organization must retain an audit trail of account termination actions (AU-2). DoD has defined the time period as immediately.	The organization conducting the inspection/assessment obtains and examines organizational security policy and procedures documentation and audit records of account termination actions to ensure account termination actions are conducted immediately and IAW organizational security policy and procedures. DoD has defined the time period as immediately.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(c)	CCI-001523	The organization, upon termination of individual employment, conducts exit interviews that include a discussion of organization-defined information security topics.	The organization being inspected/assessed, conducts exit interviews that include a discussion of information security topics defined in PS-4, CCI 3024 upon termination of individual employment IAW organization security policy and procedures. The organization must retain an audit trail of conducted exit interviews (AU-2)	The organization conducting the inspection/assessment obtains and examines documentation of departed personnel and the audit trail of conducted exit interviews to ensure all departed personnel had exit interviews conducted that include a discussion of information security topics defined in PS-4, CCI 3024.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(d)	CCI-001524	The organization, upon termination of individual employment, retrieves all security-related organizational information systems-related property.	The organization being inspected/assessed upon termination of individual employment retrieves all security-related organizational information systems related property IAW organization security policy and procedures. The organization must retain an audit trail of all retrieved security-related organizational information systems-related property (AU-2).	The organization conducting the inspection/assessment obtains and examines appropriate organization security-related organizational information systems-related property documentation/logs and compares to audit trail of all retrieved security-related organizational information systems-related property (AU-2) to ensure all property has been retrieved.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(e)	CCI-001525	The organization, upon termination of individual employment, retains access to organizational information formerly controlled by terminated individual.	The organization being inspected/assessed upon termination of individual employment retains access to organizational information formerly controlled by terminated individual IAW organization security policy and procedures. Organizational information formerly controlled by terminated individuals generally refers to online work-product including email files.	The organization conducting the inspection/assessment interviews appropriate IT and security personnel to validate the organization has procedures in place which, upon termination of individual's employment, will ensure it retains access to organizational information formerly controlled by the terminated individual.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(e)	CCI-001526	The organization, upon termination of individual employment, retains access to organizational information systems formerly controlled by terminated individual.	The organization being inspected/assessed upon termination of individual employment retains access to organizational information systems formerly controlled by terminated individual IAW organization security policy and procedures. Organizational information systems formerly controlled by terminated individuals generally refers to issued hardware (e.g. laptops, BlackBerrys, PEDs, removable media, etc.)	The organization conducting the inspection/assessment interviews appropriate IT and security personnel to validate the organization has procedures in place which, upon termination of individual's employment, will ensure it retains access to organizational information systems formerly controlled by the terminated individual.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-5(a)	CCI-001527	The organization reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization.	The organization being inspected/assessed reviews and confirms ongoing operational need for logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization. The organization must maintain an audit trail of reviews.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure that the organization has confirmed the ongoing operational need for logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-5(b)	CCI-001528	The organization initiates organization-defined transfer or reassignment actions within an organization-defined time period following the formal personnel transfer action.	The organization being inspected/assessed initiates transfer or reassignment actions to ensure all system accesses no longer required are removed and actions to ensure all system accesses required due to the individual's new position are granted immediately when personnel are reassigned or transferred to other positions. DoD defines transfer or reassignment actions as actions to ensure all system accesses no longer required are removed. DoD defines the time period as immediately.	The organization conducting the inspection/assessment obtains and examines appropriate organization security-related organizational physical and logical access documentation/logs and compares to transferred personnel documentation to ensure appropriate logical and physical access have been revoked for previous positions and granted for new positions immediately. DoD defines the time period as immediately.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-5(b)	CCI-001529	The organization defines transfer or reassignment actions to initiate within an organization-defined time period following the formal personnel transfer action.	DoD defines transfer or reassignment actions as actions to ensure all system accesses no longer required are removed.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD defines transfer or reassignment actions as actions to ensure all system accesses no longer required are removed.	LOW				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-5(b)	CCI-001530	The organization defines the time period within which the organization initiates organization-defined transfer or reassignment actions, following the formal personnel transfer action.	DoD defines the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD defines the time period as immediately.	LOW				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PS-6(c)(1)	CCI-001531	The organization ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access.	The organization being inspected/assessed will ensure all individuals have appropriate access agreements in place prior to being granted access to information and information systems. DD Form 2875 is the accepted DoD methodology of requesting and granting of access to information and information systems.	The organization conducting the inspection/assessment obtains a list of organizational individuals with active accounts and validates the existence of signed DD Form 2875 (paper or electronic) associated with a sampling of individuals selected from the list.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-6(b)	CCI-001532	The organization reviews and updates the access agreements in accordance with organization-defined frequency.	The organization being inspected/assessed reviews/updates the access agreements annually of employees who have signed access agreements. The purpose of this review/update is to ensure access agreements are current and departed employees no longer have access agreements. The organization must maintain an audit trail of the review and update activity for review. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail to ensure review/update occurred annually and departed employees no longer have valid access agreements.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-6(b)	CCI-001533	The organization defines the frequency to review and update the access agreements.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-7(a)	CCI-001539	The organization establishes personnel security requirements including security roles and responsibilities for third-party providers.	DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41 meet the DoD personnel security requirements including security roles and responsibilities for third-party providers. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41.	DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41 meet the DoD personnel security requirements including security roles and responsibilities for third-party providers. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoD 8570.01-M and DoDI 3020.41.	LOW					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-7(c)	CCI-001540	The organization documents personnel security requirements for third-party providers.	The organization being inspected/assessed documents personnel security requirements for third-party providers.	The organization conducting the inspection/assessment obtains and examines the personnel security requirements to ensure the organization being inspected/assessed documents personnel security requirements for third-party providers.	LOW			X					---	CS does not need lighting, it functions perfectly well in the dark	
N/A	PS-7(e)	CCI-001541	The organization monitors third-party provider compliance with personnel security requirements.	The organization being inspected/assessed monitors third-party provider compliance with personnel security requirements. The organization must maintain an audit trail of monitoring activity.	The organization conducting the inspection/assessment obtains and examines the audit trail of monitoring activity to ensure the organization being inspected/assessed monitors third-party provider compliance with personnel security requirements.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-8(a)	CCI-001542	The organization employs a formal sanctions process for individuals failing to comply with established information security policies and procedures.	The organization being inspected/assessed will develop formal procedures within the organizational security policy to employ formal sanctions for personnel failing to comply with established information security policies and procedures.	The organization conducting the inspection/assessment obtains and examines the organizational security policy to ensure it addresses formal procedures for sanctions and interviews security personnel to validate the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-5(c)	CCI-001544	The organization manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use.	The organization being inspected/assessed documents and implements authenticator strength mechanisms sufficient for the intended use of the authenticators.	The organization conducting the inspection/assessment obtains and examines documented authenticator strength mechanisms to ensure that they are defined and that the mechanisms have sufficient strength for the intended use of the authenticators.	LOW		X	X	X				3.4 USER IDENTIFICATION AND AUTHENTICAT…		Cybersecurity design requirements are met through the use of physical security and/or contractor requirement to change all default authentication methods within the control system's capability. This is within Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	AC-1(b)(1)	CCI-001545	The organization defines a frequency for reviewing and updating the access control policy.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-1(b)(2)	CCI-001546	The organization defines a frequency for reviewing and updating the access control procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(j)	CCI-001547	The organization defines the frequency on which it will review information system accounts for compliance with account management requirements.	DoD has defined the frequency as at a minimum, annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at a minimum, annually.	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-4	CCI-001548	The organization defines the information flow control policies for controlling the flow of information within the system.	The organization being inspected/assessed defines and documents the information flow control policies for controlling the flow of information within the system. DoD has determined the information flow control policies are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information flow control policies to ensure the organization being inspected/assessed defines the information flow control policies for controlling the flow of information within the system. DoD has determined the information flow control policies are not appropriate to define at the Enterprise level.	MOD	X	X	X	X				3.2.1 Information Flow Enforcement In MOD…	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-4	CCI-001549	The organization defines the information flow control policies for controlling the flow of information between interconnected systems.	The organization being inspected/assessed defines and documents the information flow control policies for controlling the flow of information between interconnected systems. DoD has determined the information flow control policies are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information flow control policies to ensure the organization being inspected/assessed defines the information flow control policies for controlling the flow of information between interconnected systems. DoD has determined the information flow control policies are not appropriate to define at the Enterprise level.	MOD	X	X	X	X				3.2.1 Information Flow Enforcement In MOD…	FRCS has no ethernet switches	
N/A	AC-4	CCI-001550	The organization defines approved authorizations for controlling the flow of information within the system.	The organization being inspected/assessed defines and documents approved authorizations for controlling the flow of information within the system.	The organization conducting the inspection/assessment obtains and examines the documented approved authorizations to ensure the organization being inspected/assessed defines approved authorizations for controlling the flow of information within the system.	MOD	X	X	X	X				3.2.1 Information Flow Enforcement In MOD…	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-4	CCI-001551	The organization defines approved authorizations for controlling the flow of information between interconnected systems.	The organization being inspected/assessed defines and documents approved authorizations for controlling the flow of information between interconnected systems.	The organization conducting the inspection/assessment obtains and examines the documented approved authorizations to ensure the organization being inspected/assessed defines approved authorizations for controlling the flow of information between interconnected systems.	MOD	X	X	X	X				3.2.1 Information Flow Enforcement In MOD…	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-6(1)	CCI-001558	The organization defines the security functions (deployed in hardware, software, and firmware) for which access must be explicitly authorized.	DoD has defined the security functions as all functions not publicly accessible.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security functions as all functions not publicly accessible.	MOD		X		X	X			3.3.1 User Accounts 3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION" within Part 3
N/A	AC-17(3)	CCI-001561	The organization defines managed access control points for remote access to the information system.	The organization being inspected/assessed defines and documents managed access control points for remote access to the information system.	The organization conducting the inspection/assessment obtains and examines the documented managed access points to ensure the organization being inspected/assessed defines managed access control points for remote access to the information system.	MOD	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AT-1(b)(1)	CCI-001564	The organization defines the frequency of security awareness and training policy reviews and updates.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AT-1(b)(2)	CCI-001565	The organization defines the frequency of security awareness and training procedure reviews and updates.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-3(2)	CCI-001566	The organization provides organization-defined personnel or roles with initial training in the employment and operation of physical security controls.	The organization being inspected/assessed: 1. Identifies and documents physical security controls that require training. 2. Identifies the personnel defined in AT-3 (2), CCI 2051 3. Ensures designated personnel receive this training. 4. Maintains and monitors records of personnel who have received this training.	The organization conducting the inspection/assessment obtains and examines: 1. Documentation of physical security controls that require training. 2. Documented list of personnel defined in AT-3 (2), CCI 2051 3. Ensures identified personnel have received the initial training.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-3(2)	CCI-001567	The organization provides organization-defined personnel or roles with refresher training in the employment and operation of physical security controls in accordance with the organization-defined frequency.	The organization being inspected/assessed: 1. Identifies and documents physical security controls that require training. 2. Identifies personnel defined in AT-3 (2), CCI 2051 3. Ensures designated personnel receive this training annually 4. Maintains and monitors records of personnel who have received this training. DoD has defined the frequency as annual.	The organization conducting the inspection/assessment obtains and examines: 1. Documentation of physical security controls that require training. 2. Documented list of personnel defined in AT-3 (2), CCI 2051 3. Ensures identified personnel have received training annually. DoD has defined the frequency as annual.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AT-3(2)	CCI-001568	The organization defines a frequency for providing employees with refresher training in the employment and operation of physical security controls.	DoD has defined the frequency as annual.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annual.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-1(b)(1)	CCI-001569	The organization defines the frequency on which it will review and update the audit and accountability policy.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-1(b)(2)	CCI-001570	The organization defines the frequency on which it will review and update the audit and accountability procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-2(a)	CCI-001571	The organization defines the information system auditable events.	DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module load, unload, and restart.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module load, unload, and restart.	LOW		X		X	X			3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-5(a)	CCI-001572	The organization defines the personnel or roles to be alerted in the event of an audit processing failure.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the SCA and ISSO, who shall be alerted in the event of audit processing failure. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as at a minimum, the SCA and ISSO.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles who should be alerted in the event of audit processing failure to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles. DoD has defined the personnel or roles as at a minimum, the SCA and ISSO.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-12(1)	CCI-001577	The organization defines the information system components from which audit records are to be compiled into the system-wide audit trail.	The organization being inspected/assessed will define and document the information system components from which audit records are to be compiled into the system-wide audit trail. The organization will periodically update this list to ensure it is current. DoD has determined the information system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the system-wide audit trail documentation to ensure the organization being inspected/assessed maintains a current list of information system components. DoD has determined the information system components are not appropriate to define at the Enterprise level.	MOD		X	X					3.5.3.4 Audit Reduction and Report Generati...	FRCS does not have Auditing Front End Software in scope	
N/A	CA-1(b)(2)	CCI-001578	The organization defines the frequency to review and update the current security assessment and authorization procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CA-7(g)	CCI-001581	The organization defines personnel or roles to whom the security status of organization and the information system should be reported.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(b)(2)	CCI-001584	The organization defines the frequency to review and update configuration management procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-2(1)(b)	CCI-001585	The organization defines the circumstances that require reviews and updates to the baseline configuration of the information system.	DoD has defined the circumstances as baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber attacks.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the circumstances as baseline configuration changes or as events dictate such as changes due to USCYBERCOM tactical orders/ directives or cyber attacks.	MOD					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-3(g)	CCI-001586	The organization defines the configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities.	DoD has defined the configuration change control element as a configuration control board (CCB).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the configuration change control element as a configuration control board (CCB).	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-6(a)	CCI-001588	The organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for ensuring security configuration checklists reflect the most restrictive mode consistent with operational requirements. DoD Components are automatically compliant with this CCI because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for ensuring security configuration checklists reflect the most restrictive mode consistent with operational requirements. DoD Components are automatically compliant with this CCI because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	LOW		X	X	X	X			3.2.3 IP Control Networks 3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraphs "IP Control Networks" and "REQUIREMENTS FOR LEAST FUNCTIONALITY" within Part 3.
N/A	CM-7(2)	CCI-001592	The organization defines the rules authorizing the terms and conditions of software program usage on the information system.	The organization being inspected/assessed defines and documents their rules for approval of software program usage. For network capable software programs, the organization being inspected/assessed complies with DoDI 8551. DoD has determined that the rules authorizing the terms and conditions of software program usage on the information system are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the rules as well as the software list to ensure that all network capable software programs are DoDI 8551 compliant and that the rules authorizing the use of all other programs are defined. DoD has determined that the rules authorizing the terms and conditions of software program usage on the information system are not appropriate to define at the Enterprise level	MOD		X			X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-1(b)(2)	CCI-001596	The organization defines the frequency to review and update the current contingency planning procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CP-1(a)(2)	CCI-001597	The organization disseminates contingency planning procedures to organization-defined personnel or roles.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html NIST disseminates NIST SP 800-34 via http://csrc.nist.gov/publications/PubsSPs.html	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-1(b)(2)	CCI-001598	The organization reviews and updates the current contingency planning procedures in accordance with the organization-defined frequency.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	DoDI 8500.01 and NIST SP 800-34 meet the DoD requirements for contingency planning policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8500.01 and NIST SP 800-34.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-6(3)	CCI-001604	The organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.	The organization being inspected/assessed must identify and document in the contingency plan explicit mitigation actions for accessibility problems identified in CP-6 (3), CCI 509 to the alternate storage site in the event of an area-wide disruption or disaster.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure the organization has documented explicit mitigation actions for accessibility problems identified in CP-6 (3), CCI 509 to the alternate storage site in the event of an area-wide disruption or disaster.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-7(2)	CCI-001606	The organization outlines explicit mitigation actions for organization identified potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.	The organization being inspected/assessed must identify and document in the contingency plan explicit mitigation actions for accessibility problems identified in CP-7 (2), CCI 517 to the alternate processing site in the event of an area-wide disruption or disaster.	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure the organization has documented explicit mitigation actions for accessibility problems identified in CP-7 (2), CCI 517 to the alternate processing site in the event of an area-wide disruption or disaster.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-5(g)	CCI-001610	The organization defines the time period (by authenticator type) for changing/refreshing authenticators.	DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years.	LOW		X	X	X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(a)	CCI-001611	The organization defines the minimum number of special characters for password complexity enforcement.	DoD has defined the minimum number of special characters for password complexity enforcement as one special character.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of special characters for password complexity enforcement as one special character.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(a)	CCI-001612	The organization defines the minimum number of upper case characters for password complexity enforcement.	DoD has defined the minimum number of upper case characters for password complexity enforcement as one upper-case character.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of upper case characters for password complexity enforcement as one upper-case character.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(a)	CCI-001613	The organization defines the minimum number of lower case characters for password complexity enforcement.	DoD has defined the minimum number of lower case characters for password complexity enforcement as one lower-case character.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of lower case characters for password complexity enforcement as one lower-case character.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(a)	CCI-001614	The organization defines the minimum number of numeric characters for password complexity enforcement.	DoD has defined the minimum number of numeric characters for password complexity enforcement as one numeric character.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of numeric characters for password complexity enforcement as one numeric character.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(b)	CCI-001615	The organization defines the minimum number of characters that are changed when new passwords are created.	DoD has defined the minimum number of characters as 50% of the minimum password length.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum number of characters as 50% of the minimum password length.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-5(1)(d)	CCI-001616	The organization defines minimum password lifetime restrictions.	DoD has defined the minimum password lifetime restrictions as 24 hours.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the minimum password lifetime restrictions as 24 hours.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(d)	CCI-001617	The organization defines maximum password lifetime restrictions.	DoD has defined the maximum password lifetime restrictions as 60 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the maximum password lifetime restrictions as 60 days.	LOW		X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(e)	CCI-001618	The organization defines the number of generations for which password reuse is prohibited.	DoD has defined the number of generations as a minimum of 5.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the number of generations as a minimum of 5.	LOW	X	X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(1)(a)	CCI-001619	The information system enforces password complexity by the minimum number of special characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of special characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1619.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of special characters used. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1619.	LOW	X	X						3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(8)	CCI-001621	The organization implements organization-defined security safeguards to manage the risk of compromise due to individuals having accounts on multiple information systems.	The organization being inspected/assessed documents and implements policies and user training including advising users not to use the same password for any of the following: Domains of differing classification levels. More than one domain of a classification level (e.g., internal agency network and Intelink). More than one privilege level (e.g., user, administrator).	The organization conducting the inspection/assessment obtains and examines the documented policies as well as training records to ensure that the organization being inspected/assessed implements policies and training advising users not to use the same password for any of the following: Domains of differing classification levels. More than one domain of a classification level (e.g., internal agency network and Intelink). More than one privilege level (e.g., user, administrator).	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-3	CCI-001624	The organization documents the results of incident response tests.	The organization being inspected/assessed will document the results of incident response tests.	The organization conducting the inspection/assessment obtains and examines: 1. the organization's incident response plan to identify organization's testing schedule and, 2. results of previous incident response tests to ensure the organization is documenting the results IAW their incident response plan.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-4(c)	CCI-001625	The organization implements the resulting incident handling activity changes to incident response procedures, training and testing/exercise accordingly.	The organization being inspected/assessed will follow the latest incident response plan (IR-8) that has been revised (based on IR-4, CCI-000824) and disseminated.	The organization conducting the inspection/assessment obtains and examines recent changes to the incident response plan (based on IR-4, CCI 000824) to verify that they have been disseminated and reviews the most recent after action report to ensure that changes have been followed.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-1(b)(2)	CCI-001628	The organization defines a frequency to review and update the current system maintenance procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(3)(b)	CCI-001631	The organization, before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.	The organization being inspected/assessed sanitizes and inspects serviced components prior to reusing them on any information system. Alternatively, the organization being inspected/assessed complies with MA-4 (3) CCI 882.	The organization conducting the inspection/assessment obtains and examines maintenance procedures for all non-local maintenance and diagnostic services to ensure that the organization being inspected/assessed sanitizes and inspects serviced components prior to reusing them on any information system. Alternatively, the organization conducting the inspection/assessment ensures the organization being inspected/assessed complies with MA-4 (3) CCI 882.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PE-2(c)	CCI-001635	The organization removes individuals from the facility access list when access is no longer required.	The organization being inspected/assessed will remove personnel from the authorized access list who no longer have approved access and revoke their credentials, as identified in actions per PE-2, CCI 914. The organization must document each removal and revocation action as an audit trail.	The organization conducting the inspection/assessment obtains and examines the review and approval actions documentation to ensure that personnel no longer requiring access have been removed from the authorized access list and their credentials have been revoked.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PL-1(b)(1)	CCI-001636	The organization defines the frequency to review and update the current security planning policy.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PL-1(b)(1)	CCI-001637	The organization reviews and updates the current security planning policy in accordance with organization-defined frequency.	DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the frequency as every 5 years.	DoDI 8510.01 meets the requirements for a security planning policy. DoD Components are automatically compliant with this CCI because they are covered by DoD level policy, DoDI 8510.01. DoD has defined the frequency as every 5 years.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-1(b)(2)	CCI-001638	The organization defines the frequency to review and update the current security planning procedures.	DoD has defined the frequency as reviewed annually - updated as appropriate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PL-4(a)	CCI-001639	The organization makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.	The organization being inspected/assessed must disseminate to all information system users, via an information sharing capability, rules that describe information system user responsibilities and expected behavior with regard to information and information system usage, acceptable use policy (AUP). Organizations should disseminate the rules by providing to users and requiring signature of acceptance.	The organization conducting the inspection/assessment obtains and examines rules that describe information system user responsibilities via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-8	CCI-001640	The organization updates the critical infrastructure and key resources protection plan that addresses information security issues.	DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan. DoD components are automatically compliant with this CCI as they are covered by the DoD level, DoDD 3020.40.	DoDD 3020.40 meets the DoD requirement for the development of a critical infrastructure and key resource protection plan. DoD components are automatically compliant with this CCI as they are covered by the DoD level, DoDD 3020.40.	LOW					X	X	A LOW Control System doesn't deal with critical infrastructure.	---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-5(a)	CCI-001641	The organization defines the process for conducting random vulnerability scans on the information system and hosted applications.	DoD has defined the requirement for vulnerability scanning periodicity of every 30 days. If the organization being inspected/assessed has determined a requirement for random scanning they must document that process. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines random vulnerability process documentation (if applicable) to validate the organization has clearly defined and documented a process for conducting random vulnerability scans on the information system and hosted applications. If the organization being inspected/assessed has determined they have no requirement for random scanning, there is no requirement for a process.	LOW	X	X	X	X					3.11 VULNERABILITY SCANNING	FRCS has no IP devices to scan	
N/A	RA-3(b)	CCI-001642	The organization defines the organizational document in which risk assessment results are documented (e.g., security plan, risk assessment report).	DoD has defined the document as a risk assessment report.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the document as a risk assessment report.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-5(a)	CCI-001643	The organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined process for random scans.	The organization being inspected/assessed will conduct random vulnerability scans every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs). The organization will document the vulnerability scans as an audit trail for future reference. The audit trail must be maintained IAW DoD, CYBERCOM, or component policies. DoD has defined the frequency as every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs).	The organization conducting the inspection/assessment obtains and examines the vulnerability scanning results every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs) to verify compliance with the organization being inspected/assessed random vulnerability scanning process. DoD has defined the frequency as every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs).	LOW	X	X	X					3.11 VULNERABILITY SCANNING	FRCS has no IP devices to scan	
N/A	RA-5(5)	CCI-001645	The organization identifies the information system components to which privileged access is authorized for selected organization-defined vulnerability scanning activities.	DoD has defined the information system components as all information systems and infrastructure components.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system components as all information systems and infrastructure components.	MOD	X	X		X	X			2.3 DATABASE AND WEB SERVER SOFTWARE FO... 3.11 VULNERABILITY SCANNING	FRCS has no computer-based databases in scope. FRCS has no IP devices to scan	
N/A	SA-1(b)(2)	CCI-001646	The organization defines the frequency to review and update the current system and services acquisition procedures.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-18(1)	CCI-001662	The information system takes organization-defined corrective action when organization-defined unacceptable mobile code is identified.	The organization being inspected/assessed configures the information system to take corrective actions defined in SC-18 (1), CCI 2457 when unacceptable mobile code defined in SC-18 (1), CCI 2458 is identified. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1662.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to take corrective actions defined in SC-18 (1), CCI 2457 when unacceptable mobile code defined in SC-18 (1), CCI 2458 is identified. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1662.	MOD	X	X	X					3.7.3 Mobile Code In MODERATE Impact Syst...		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-20(b)	CCI-001663	The information system, when operating as part of a distributed, hierarchical namespace, provides the means to enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services).	The organization being inspected/assessed installs and utilizes software capable of validating the chain of trust (Examples of software include dig, dnsviz, dnssec-debugger, dnssec validator for Mozilla, etc.). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1663.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for authoritative name resolution services where parent and child domains exist. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that pertains to CCI 1663.	LOW				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-23(3)	CCI-001664	The information system recognizes only session identifiers that are system-generated.	The organization being inspected/assessed configures the information system to recognize only session identifiers that are system-generated. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1664.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to recognize only session identifiers that are system-generated. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1664.	MOD		X						3.2.6 Cryptographic Protection	FRCS does not contain classified information	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enriches	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-24	CCI-001665	The information system preserves organization-defined system state information in the event of a system failure.	The organization being inspected/assessed configures the information system to preserve information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes in the event of a system failure. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1665. DoD has defined system state information as information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to preserve information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes in the event of a system failure. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1665. DoD has defined system state information as information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes.	MOD		X		X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(11)	CCI-001671	The organization analyzes outbound communications traffic at selected organization-defined interior points within the system (e.g., subnetworks, subsystems) to discover anomalies.	The organization being inspected/assessed documents and implements a process to analyze outbound communications traffic at selected interior points defined in SI-4 (11), CCI 2668 within the system (e.g., subnetworks, subsystems) to discover anomalies. The organization must maintain a record of any discovered anomalies.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of any discovered anomalies to ensure the organization being inspected/assessed analyzes outbound communications traffic at selected interior points defined in SI-4 (11), CCI 2668 within the system (e.g., subnetworks, subsystems) to discover anomalies.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(14)	CCI-001673	The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.	The organization being inspected/assessed documents and implements a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.	The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified wireless intrusion detection system and the system hardware/software list to ensure the organization being inspected/assessed employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system. The organization being inspected/assessed may be required to demonstrate use of the wireless intrusion detection system.	MOD	X		X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-12	CCI-001678	The organization retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization being inspected/assessed identifies and documents federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system. The organization documents and implements a process to retain information IAW those documented federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization conducting the inspection/assessment obtains and examines the documented list of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements which apply to the information within the information system, as well as the documented process for information retention to ensure the organization being inspected/assessed retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-1(a)(2)	CCI-001680	The organization develops an organization-wide information security program plan that includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AC-2(2)	CCI-001682	The information system automatically removes or disables emergency accounts after an organization-defined time period for each type of account.	The organization being inspected/assessed configures the information system to never automatically remove or disable emergency accounts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1682. DoD has defined the time period as never.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to never automatically remove or disable emergency accounts. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1682. DoD has defined the time period as never.	MOD	X	X	X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(4)	CCI-001683	The information system notifies organization-defined personnel or roles for account creation actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account creation actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1683. DoD has defined the personnel or roles as the system administrator and ISSO.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account creation actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1683. DoD has defined the personnel or roles as the system administrator and ISSO.	MOD	X	X						3.3.1 User Accounts		CCI requirements are met within subparagraph "User Accounts" of UFGS 25 05 11.
N/A	AC-2(4)	CCI-001684	The information system notifies organization-defined personnel or roles for account modification actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account modification actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1684. DoD has defined the personnel or roles as the system administrator and ISSO.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account modification actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1684. DoD has defined the personnel or roles as the system administrator and ISSO.	MOD	X	X						3.3.1 User Accounts		CCI requirements are met within subparagraph "User Accounts" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-2(4)	CCI-001685	The information system notifies organization-defined personnel or roles for account disabling actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account disabling actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1685. DoD has defined the personnel or roles as the system administrator and ISSO.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account disabling actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1685. DoD has defined the personnel or roles as the system administrator and ISSO.	MOD	X	X						3.3.1 User Accounts		CCI requirements are met within subparagraph "User Accounts" of UFGS 25 05 11.
N/A	AC-2(4)	CCI-001686	The information system notifies organization-defined personnel or roles for account removal actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account removal actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1686. DoD has defined the personnel or roles as the system administrator and ISSO.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account removal actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1686. DoD has defined the personnel or roles as the system administrator and ISSO.	MOD	X	X						3.3.1 User Accounts		CCI requirements are met within subparagraph "User Accounts" of UFGS 25 05 11.
N/A	SC-18(2)	CCI-001687	The organization ensures the use of mobile code to be deployed in information systems meets organization-defined mobile code requirements.	The organization being inspected/assessed documents and implements a process to use mobile code IAW the requirements defined in CCI 1168.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed uses mobile code IAW the requirements defined in CCI 1168.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-18(2)	CCI-001688	The organization ensures the acquisition of mobile code to be deployed in information systems meets organization-defined mobile code requirements.	The organization being inspected/assessed documents and implements a process to acquire mobile code IAW the requirements defined in CCI 1168.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed acquire mobile code IAW the requirements defined in CCI 1168.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-18(3)	CCI-001695	The information system prevents the execution of organization-defined unacceptable mobile code.	The organization being inspected/assessed configures the information system to prevent the execution of unacceptable mobile code defined in CCI 2459. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1695.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent the execution of unacceptable mobile code defined in CCI 2459. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1695.	MOD		X	X					3.7.3 Mobile Code In MODERATE Impact Syst...		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	CM-10(a)	CCI-001726	The organization uses software in accordance with contract agreements.	The organization being inspected/assessed uses software in accordance with contract agreements.	The organization conducting the inspection/assessment obtains and examines a sampling of contract agreements and supporting evidence concerning the usage of software to ensure compliance with the contract agreements.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(a)	CCI-001727	The organization uses software documentation in accordance with contract agreements.	The organization being inspected/assessed uses software documentation in accordance with contract agreements.	The organization conducting the inspection/assessment obtains and examines a sampling of contract agreements associated with software documentation and supporting evidence concerning the usage of software documentation to ensure compliance with contract agreements.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(a)	CCI-001728	The organization uses software in accordance with copyright laws.	The organization being inspected/assessed uses software in accordance with copyright laws.	The organization conducting the inspection/assessment obtains and examines supporting evidence concerning the usage of software to ensure compliance with copyright laws.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(a)	CCI-001729	The organization uses software documentation in accordance with copyright laws.	The organization being inspected/assessed uses software documentation in accordance with copyright laws.	The organization conducting the inspection/assessment obtains and examines supporting evidence concerning the usage of software documentation to ensure compliance with copyright laws.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(b)	CCI-001730	The organization tracks the use of software protected by quantity licenses to control copying of the software.	The organization being inspected/assessed tracks the use of software protected by quantity licenses to control copying of the software. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	The organization conducting the inspection/assessment obtains and examines the tracking records to ensure the organization being inspected/assessed tracks the use of software protected by quantity licenses to control copying of the software.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(b)	CCI-001731	The organization tracks the use of software documentation protected by quantity licenses to control distribution of the software documentation.	The organization being inspected/assessed tracks the use of software documentation protected by quantity licenses to control distribution of the software documentation. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	The organization conducting the inspection/assessment obtains and examines the tracking records to ensure the organization being inspected/assessed tracks the use of software documentation protected by quantity licenses to control distribution of the software documentation.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(c)	CCI-001732	The organization controls the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	The organization being inspected/assessed reviews and authorizes in order to control the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. The organization must maintain an audit trail of peer-to-peer file sharing technology reviews and authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of peer-to-peer file sharing technology reviews and authorizations to ensure the organization being inspected/assessed controls the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	LOW	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CM-10(c)	CCI-001733	The organization documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	The organization being inspected/assessed documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	The organization conducting the inspection/assessment obtains and examines the documentation for the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	LOW	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-10(1)	CCI-001734	The organization defines the restrictions to be followed on the use of open source software.	DoD has defined the restrictions as IAW DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)" 16 Oct 2009 (http://dodcio.defense.gov/Home/Issuances/DoDCIOMemorandums.aspx).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the restrictions as IAW DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)" 16 Oct 2009 (http://dodcio.defense.gov/Home/Issuances/DoDCIOMemorandums.aspx).	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(1)	CCI-001735	The organization establishes organization-defined restrictions on the use of open source software.	DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)" 16 Oct 2009 (http://dodcio.defense.gov/Home/Issuances/DoDCIOMemorandums.aspx) meets the DoD requirement for establishing restrictions on the use of open source software. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)."	DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)" 16 Oct 2009 (http://dodcio.defense.gov/Home/Issuances/DoDCIOMemorandums.aspx) meets the DoD requirement for establishing restrictions on the use of open source software. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)."	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-2(3)	CCI-001736	The organization defines the previous versions of baseline configuration of the information system required to support rollback.	DoD has defined the previous versions as the previous approved baseline configuration of IS components for a minimum of 3 month.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the previous versions as the previous approved baseline configuration of IS components for a minimum of 3 month.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-2(7)a	CCI-001737	The organization defines the information systems, system components, or devices that are to have organization-defined configurations applied when located in areas of significant risk.	The organization being inspected/assessed defines and documents, in the configuration management policy, the information systems, system components, or devices that are to have configurations defined in CM-2 (7), CCI 1738 applied when located in areas of significant risk. DoD has determined that this value is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed defines the information systems, system components, or devices that are to have configurations defined in CM-2 (7), CCI 1738 applied when located in areas of significant risk. DoD has determined that this value is not appropriate to define at the Enterprise level.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-2(7)a	CCI-001738	The organization defines the security configurations to be implemented on information systems, system components, or devices when they are located in areas of significant risk.	The organization being inspected/assessed defines and documents, in the configuration management policy, the security configurations to be implemented on information systems, system components, or devices when they are located in areas of significant risk. DoD has determined that this value is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed defines the security configurations to be implemented on information systems, system components, or devices when they are located in areas of significant risk. DoD has determined that this value is not appropriate to define at the Enterprise level.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-2(7)a	CCI-001739	The organization issues organization-defined information systems, system components, or devices with organization-defined configurations to individuals traveling to locations the organization deems to be of significant risk.	The organization being inspected/assessed issues information systems, system components, or devices as defined in CM-2 (7) CCI 1737 with configurations as defined in CM-2 (7) CCI 1738 to individuals traveling to locations the organization deems to be of significant risk.	The organization conducting the inspection/assessment interviews organizational personnel with configuration management responsibilities to ensure that individuals traveling to locations that the organization deems to be of significant risk are issued information systems, system components, or devices as defined in CM-2 (7) CCI 1737 with configurations as defined in CM-2 (7) CCI 1738.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-3(b)	CCI-001740	The organization reviews proposed configuration controlled changes to the information system.	The organization being inspected/assessed conducts reviews of records documenting the proposed configuration controlled changes to each information system. The organization will maintain an audit trail of each proposed configuration controlled change. This action will be implemented by the CCB as defined in CM-3, CCI 1586.	The organization conducting the inspection/assessment obtains and examines the audit trail of a sampling of proposed configuration controlled changes to ensure the reviews are being conducted.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-3(c)	CCI-001741	The organization documents configuration change decisions associated with the information system.	The organization being inspected/assessed documents configuration change decisions associated with the information system. The organization must maintain an audit trail of configuration change decisions. This action will be implemented by the CCB as defined in CM-3, CCI 1586.	The organization conducting the inspection/assessment obtains and examines the audit trail documenting configuration change decisions associated with the information system to ensure the organization being inspected/assessed has documented their decisions.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-3(6)	CCI-001745	The organization defines the security safeguards that are to be provided by the cryptographic mechanisms which are employed by the organization.	DoD has defined the security safeguards as all security safeguards.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security safeguards as all security safeguards.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-3(6)	CCI-001746	The organization ensures that cryptographic mechanisms used to provide organization-defined security safeguards are under configuration management.	The organization being inspected/assessed ensures that cryptographic mechanisms used to provide all security safeguards are under configuration management. DoD has defined the security safeguards as all security safeguards.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure that cryptographic mechanisms used to provide all security safeguards are documented in the policy. DoD has defined the security safeguards as all security safeguards.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-5(5)(a)	CCI-001753	The organization limits privileges to change information system components within a production or operational environment.	The organization being inspected/assessed documents and implements a process to limit privileges to change information system components within a production or operational environment.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed limits privileges to change information system components within a production or operational environment.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-5(5)(a)	CCI-001754	The organization limits privileges to change system-related information within a production or operational environment.	The organization being inspected/assessed documents and implements a process to limit privileges to change system-related information within a production or operational environment.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed limits privileges to change system-related information within a production or operational environment.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-6(c)	CCI-001755	The organization defines the information system components for which any deviation from the established configuration settings are to be identified, documented and approved.	DoD has defined the information system components as all configurable information system components.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system components as all configurable information system components.	LOW		X	X	X	X			3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity design requires the contractor to configure and document that the control system follow any applicable STIG/SRG and/or only provide essential capabilities. This design requirement is captured in Sub-Paragraph "Requirements for Lease Functionality" within Part 3.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-6(c)	CCI-001756	The organization defines the operational requirements on which the configuration settings for the organization-defined information system components are to be based.	The organization being inspected/assessed must define and document in the system security plan, the requirements which may deviate from the approved configuration settings on the information system components defined in CM-6, CCI 1755. DoD has determined that it is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the system security plan to ensure the organization being inspected/assessed defines the requirements which may deviate from the approved configuration settings on the information system components defined in CM-6, CCI 1755. DoD has determined that it is not appropriate to define at the Enterprise level.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-7(1)(a)	CCI-001760	The organization defines the frequency of information system reviews to identify unnecessary and/or nonsecure functions, ports, protocols, and services.	DoD has defined the frequency as every 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 30 days.	LOW				X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-7(1)(b)	CCI-001761	The organization defines the functions, ports, protocols and services within the information system that are to be disabled when deemed unnecessary and/or nonsecure.	The organization being inspected/assessed must define and document in the system security plan, the functions, ports, protocols and services within the information system that are to be disabled when deemed unnecessary. DoD has determined that it is not appropriate to define unnecessary functions, ports, protocols and service at the Enterprise level. Nonsecure functions, ports, protocols and services are defined in DoDI 8551.01.	The organization conducting the inspection/assessment obtains and examines the system security plan to ensure the organization being inspected/assessed defines the functions, ports, protocols and services within the information system that are to be disabled when deemed unnecessary. DoD has determined that it is not appropriate to define unnecessary functions, ports, protocols and service at the Enterprise level. Nonsecure functions, ports, protocols and services are defined in DoDI 8551.01.	LOW		X							3.2.3 IP Control Networks 3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.
N/A	CM-7(1)(b)	CCI-001762	The organization disables organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure.	The organization being inspected/assessed must disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure as defined in CM-7 (1), CCI 1761.	The organization conducting the inspection/assessment inspects the information system to ensure the organization being inspected/assessed disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure as defined in CM-7 (1), CCI 1761.	LOW		X		X				3.2.3 IP Control Networks 3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.
N/A	CM-7(2)	CCI-001763	The organization defines the policies regarding software program usage and restrictions.	The organization being inspected/assessed defines and documents their rules for approval of software program usage. For network capable software programs, the organization being inspected/assessed complies with DoDI 8551. DoD has determined that the rules authorizing the terms and conditions of software program usage on the information system are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the rules as well as the software list to ensure that all network capable software programs are DoDI 8551 compliant and that the rules authorizing the use of all other programs are defined. DoD has determined that the rules authorizing the terms and conditions of software program usage on the information system are not appropriate to define at the Enterprise level.	MOD		X	X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-7(2)	CCI-001764	The information system prevents program execution in accordance with organization-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.	The organization being inspected/assessed configures the information system to prevent the execution of programs not authorized in accordance with CM-7 (2) CCIs 1592 and 1763.	The organization conducting the inspection/assessment examines the information systems to ensure the systems are configured to prevent the execution of programs not authorized in accordance with CM-7 (2) CCIs 1592 and 1763.	MOD		X	X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-7(5)a	CCI-001772	The organization defines the software programs authorized to execute on the information system.	The organization being inspected/assessed must define and document software programs that are authorized to execute on the information system. DoD has determined that a comprehensive list of unauthorized software programs is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented list of software programs that are authorized to execute to ensure that list is defined. DoD has determined that a comprehensive list of unauthorized software programs is not appropriate to define at the Enterprise level.	MOD		X	X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-7(5)a	CCI-001773	The organization identifies the organization-defined software programs authorized to execute on the information system.	The organization being inspected/assessed must define and document software programs that are authorized to execute on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of software programs that are authorized to execute to ensure that list is defined.	MOD		X	X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-7(5)b	CCI-001774	The organization employs an deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system.	The organization being inspected/assessed configures the information system to deny-all and only permit by exception the execution of authorized software programs on the information system.	The organization conducting the inspection/assessment examines the information system to ensure that it is configured to deny-all and only permit by exception the execution of authorized software programs on the information system.	MOD		X	X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-7(5)c	CCI-001775	The organization defines the frequency on which it will review and update the list of authorized software programs.	DoD has defined the frequency as monthly.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as monthly.	MOD			X	X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-7(5)c	CCI-001777	The organization reviews and updates the list of authorized software programs per organization-defined frequency.	The organization being inspected/assessed documents and implements a process to review and update the list of authorized software programs monthly. The organization must maintain an audit trail of the review and update activity. DoD has defined the frequency as monthly.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reviews and updates to ensure that the organization being inspected/assessed reviews and updates the list of authorized software programs monthly. DoD has defined the frequency as monthly.	MOD			X	X					---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(b)	CCI-001779	The organization defines the frequency on which the information system component inventory is to be reviewed and updated	DoD has defined the frequency as at a minimum, annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at a minimum, annually.	LOW			X	X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CM-8(b)	CCI-001780	The organization reviews and updates the information system component inventory per organization-defined frequency.	The organization being inspected/assessed documents and implements a process to review and update the information system component inventory at a minimum, annually. The organization must maintain an audit trail of review and update activity. DoD has defined the frequency as at a minimum, annually.	The organization conducting the inspection/assessment obtains and examines the documented process for reviews and updates as well as the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the information system component inventory at a minimum, annually. DoD has defined the frequency as at a minimum, annually.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-8(3)(b)	CCI-001783	The organization defines the personnel or roles to be notified when unauthorized hardware, software, and firmware components are detected within the information system.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO or ISSM, to be notified when unauthorized hardware, software, and firmware components are detected within the information system. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles to be notified when unauthorized hardware, software, and firmware components are detected within the information system to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	MOD					X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-8(3)(b)	CCI-001784	When unauthorized hardware, software, and firmware components are detected within the information system, the organization takes action to disable network access by such components, isolates the components, and/or notifies organization-defined personnel or roles.	The organization being inspected/assessed documents and implements a process to take action to disable network access by unauthorized software, hardware, and firmware components, isolate the components, and/or notify the ISSO and ISSM and others as the local organization deems appropriate. The organization must maintain an audit trail of actions taken upon detection of unauthorized software, hardware, and firmware components. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the documented process and audit trail for taking action upon detection of unauthorized components to ensure the organization being inspected/assessed takes action to disable network access by unauthorized software, hardware, and firmware components, isolate the components, and/or notify the ISSO and ISSM and others as the local organization deems appropriate. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	MOD			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-9(b)	CCI-001790	The organization develops and documents a configuration management plan for the information system that establishes a process for identifying configuration items throughout the system development life cycle.	The organization being inspected/assessed will develop and document a configuration management plan for the information system that establishes a process for identifying configuration items throughout the system development life cycle.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to verify it establishes and documents a process for identifying configuration items throughout the system development life cycle.	MOD			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-9(b)	CCI-001792	The organization implements a configuration management plan for the information system that establishes a process for identifying configuration items throughout the system development life cycle.	The organization being inspected/assessed will implement a configuration management plan for the information system that establishes a process for identifying configuration items throughout the system development life cycle.	The organization conducting the inspection/assessment obtains and examines the configuration management plan as well as evidence of implementation (e.g., completed change requests, meeting minutes, and other relevant documents) to ensure the organization being inspected/assessed implements a configuration management plan for the information system that establishes a process for identifying configuration items throughout the system development life cycle. Checks should include verification that items being processed for CM are the items identified and that identified configuration items have not been changed without going through the documented process.	MOD			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-9(b)	CCI-001793	The organization develops and documents a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items.	The organization being inspected/assessed will develop and document a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure it establishes and documents a process for managing the configuration of the configuration items.	MOD			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-9(b)	CCI-001795	The organization implements a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items.	The organization being inspected/assessed will implement a configuration management plan that has a process for controlling changes to configuration items.	The organization conducting the inspection/assessment obtains and examines the configuration management plan as well as evidence of implementation (e.g., completed change requests, meeting minutes, and other relevant documents) to ensure the organization being inspected/assessed implements a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items.	MOD			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-9(c)	CCI-001796	The organization develops and documents a configuration management plan for the information system that places the configuration items under configuration management.	The organization being inspected/assessed will develop and document a configuration management plan for the information system that places the configuration items under configuration management.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure the organization being inspected/assessed documents that configuration items are placed under configuration management.	MOD			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-9(c)	CCI-001798	The organization implements a configuration management plan for the information system that places the configuration items under configuration management.	The organization being inspected/assessed will implement a configuration management plan for the information system that places the configuration items under configuration management.	The organization conducting the inspection/assessment obtains and examines the configuration management plan as well as evidence of implementation (e.g., completed change requests, meeting minutes, and other relevant documents) to ensure the organization being inspected/assessed implements a configuration management plan for the information system and that configuration items identified are under configuration management.	MOD			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-9(d)	CCI-001799	The organization develops a configuration management plan for the information system that protects the configuration management plan from unauthorized disclosure and modification.	The organization being inspected/assessed must develop and document a plan to protect the configuration management plan from unauthorized disclosure and modification. Measures must include marking, labeling, and handling to prevent improper disclosure. The organization being inspected/assessed must ensure that all changes to the CM plan are approved.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to verify that it identifies the protection measures.	MOD			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-9(d)	CCI-001801	The organization implements a configuration management plan for the information system that protects the configuration management plan from unauthorized disclosure and modification.	The organization being inspected/assessed must implement a plan to protect the configuration management plan from unauthorized disclosure and modification. Measures must include marking, labeling, and handling to prevent improper disclosure. The organization being inspected/assessed must ensure that all changes to the CM plan are approved.	The organization conducting the inspection/assessment obtains and examines the configuration management plan to verify that the identified protection measures are implemented.	MOD			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-10(b)	CCI-001802	The organization tracks the use of software documentation protected by quantity licenses to control copying of the software documentation.	The organization being inspected/assessed tracks the use of software documentation protected by quantity licenses to control copying of the software documentation. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	The organization conducting the inspection/assessment obtains and examines the tracking records to ensure the organization being inspected/assessed tracks the use of software documentation protected by quantity licenses to control copying of the software documentation.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-10(b)	CCI-001803	The organization tracks the use of software protected by quantity licenses to control distribution of the software.	The organization being inspected/assessed tracks the use of software protected by quantity licenses to control distribution of the software. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	The organization conducting the inspection/assessment obtains and examines the tracking records to ensure the organization being inspected/assessed tracks the use of software protected by quantity licenses to control distribution of the software.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-11(a)	CCI-001804	The organization defines the policies for governing the installation of software by users.	The organization being inspected/assessed must define policies governing the installation of software by users. DoD has determined the policies are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines policies governing the installation of software by users (e.g., user agreements, CM plan, etc.) to ensure the organization being inspected/assessed defines the policies for governing the installation of software by users. DoD has determined the policies are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-11(a)	CCI-001805	The organization establishes organization-defined policies governing the installation of software by users.	The organization being inspected/assessed documents their policies governing the installation of software by users (e.g., user agreements, CM plan, etc.).	The organization conducting the inspection/assessment obtains and examines documented policies governing the installation of software by users (e.g., user agreements, CM plan, etc.) to ensure the organization being inspected/assessed establishes policies governing the installation of software by users.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-11(b)	CCI-001806	The organization defines methods to be employed to enforce the software installation policies.	The organization being inspected/assessed must define and document the methods employed to enforce the software installation policies. DoD has determined the policies are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines documentation of the methods employed to ensure the organization being inspected/assessed defines methods to be employed to enforce the software installation policies. DoD has determined the policies are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-11(b)	CCI-001807	The organization enforces software installation policies through organization-defined methods.	The organization being inspected/assessed must enforce software installation policies as defined in CM-11, CCI 1804 through methods defined in CM-11, CCI 1806.	The organization conducting the inspection/assessment obtains and examines software installation policies defined in CM-11, CCI 1804 and inspects the methods defined in CM-11, CCI 1806 to verify they are properly implemented.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-11(c)	CCI-001808	The organization defines the frequency on which it will monitor software installation policy compliance.	DoD has defined the frequency as at least monthly.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least monthly.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-11(c)	CCI-001809	The organization monitors software installation policy compliance per organization-defined frequency.	The organization being inspected/assessed must monitor software installation policy compliance at least monthly. The organization must maintain audit trails of monitoring activity. DoD has defined the frequency as at least monthly.	The organization conducting the inspection/assessment obtains and examines the audit trails of monitoring activities to ensure the organization being inspected/assessed monitors software installation policy compliance at least monthly. DoD has defined the frequency as at least monthly.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-11(2)	CCI-001812	The information system prohibits user installation of software without explicit privileged status.	The organization being inspected/assessed must configure the information system to prevent the installation of software by non-privileged users. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1812.	The organization conducting the inspection/assessment obtains and examines the configuration of the information system components to ensure that installation of software without explicit privileged status is prohibited. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1812.	MOD		X	X					3.3.1 User Accounts		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts" within Part 3
N/A	CM-5(1)	CCI-001813	The information system enforces access restrictions.	The organization being inspected/assessed documents and implements a process to enforce access restrictions provided by the information system.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the configuration of the information system to ensure access restrictions are implemented.	MOD		X	X					3.3.1 User Accounts		CCI requirements are met within subparagraph "User Accounts" of UFGS 25 05 11.
N/A	CM-5(1)	CCI-001814	The Information system supports auditing of the enforcement actions.	The organization being inspected/assessed leverages only information systems which support auditing of enforcement actions.	The organization conducting the inspection/assessment reviews vendor documentation to ensure the information system supports auditing of the enforcement actions. If vendor documentation is not available, the organization conducting the inspection/assessment tests the information system for the capability.	MOD		X	X					3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	CM-2(7)b	CCI-001815	The organization defines the security safeguards to be applied to devices when they return from areas of significant risk.	The organization being inspected/assessed defines and documents, in the configuration management policy, the security safeguards to be applied to devices when they return from areas of significant risk. DoD has determined that this value is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being inspected/assessed defines the security safeguards to be applied to devices when they return from areas of significant risk. DoD has determined that this value is not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-2(7)b	CCI-001816	The organization applies organization-defined security safeguards to devices when individuals return from areas of significant risk.	The organization being inspected/assessed applies security safeguards as defined in CM-2 (7) CCI 1815 to devices when individuals return from areas of significant risk.	The organization conducting the inspection/assessment interviews organizational personnel with configuration management responsibilities to ensure that when individuals return from areas of significant risk, security safeguards as defined in CM-2 (7) CCI 1815 are applied to devices as defined in CM-2 (7) CCI 1737.	MOD								---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CM-4(1)	CCI-001817	The organization, when analyzing changes to the information system, looks for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	The organization being inspected/assessed documents within their process for analyzing changes to the information system, methods for identifying security impacts due to flaws, weaknesses, incompatibility, or intentional malice. The organization implements the documented process and must maintain a record of analysis.	The organization conducting the inspection/assessment obtains and examines the documented process and record of analysis to ensure the organization being inspected/assessed, when analyzing changes to the information system, looks for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-4(1)	CCI-001818	The organization analyzes changes to the information system in a separate test environment before installation in an operational environment.	The organization being inspected/assessed documents and employs a policy to analyze changes to the information system in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. The organization must maintain records of analysis of changes to the information system.	The organization conducting the inspection/assessment obtains and examines the documented policy for analyzing changes as well as records of analysis to ensure the organization being inspected/assessed analyzes changes to the information system in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	MOD			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-3(d)	CCI-001819	The organization implements approved configuration-controlled changes to the information system.	The organization being inspected/assessed implements approved configuration-controlled changes to the information system. The organization must maintain an audit trail of the implementation of approved configuration-controlled changes.	The organization conducting the inspection/assessment obtains and examines the audit trail documenting the implementation of approved configuration-controlled changes to the information system to ensure the organization being inspected/assessed has implemented the approved changes.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(a)	CCI-001821	The organization defines the organizational personnel or roles to whom the configuration management policy is to be disseminated.	DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(a)(1)	CCI-001822	The organization disseminates the configuration management policy to organization defined personnel or roles.	The organization being inspected/assessed disseminates a configuration management policy via an information sharing capability (e.g. portal, intranet, email, etc.) to all stakeholders in the configuration management process. DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	The organization conducting the inspection/assessment obtains and examines the configuration management policy via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-1(a)	CCI-001824	The organization defines the organizational personnel or roles to whom the configuration management procedures are to be disseminated.	DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	LOW			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-1(a)(2)	CCI-001825	The organization disseminates to organization defined personnel or roles the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization being inspected/assessed disseminates the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls via an information sharing capability (e.g. portal, intranet, email, etc.) to all stakeholders in the configuration management process. DoD has defined the organizational personnel or roles as all stakeholders in the configuration management process.	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the configuration management policy and associated configuration management controls via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-5(2)	CCI-001826	The organization defines the circumstances when the organization reviews the information system changes to determine whether unauthorized changes have occurred.	DoD has defined the circumstances as when there is an incident or when planned changes have been performed.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the circumstances as when there is an incident or when planned changes have been performed.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-5(5)(b)	CCI-001827	The organization defines frequency to review information system privileges.	DoD has defined the frequency as every 90 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 90 days.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-5(5)(b)	CCI-001828	The organization defines frequency to reevaluate information system privileges.	DoD has defined the frequency as every 90 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 90 days.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	CM-5(5)(b)	CCI-001829	The organization reviews information system privileges per organization defined frequency.	The organization being inspected/assessed reviews information system privileges every 90 days. The organization must maintain the reviews as an audit trail. DoD has defined the frequency as every 90 days.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organization being inspected/assessed reviews information system privileges every 90 days . DoD has defined the frequency as every 90 days.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-5(5)(b)	CCI-001830	The organization reevaluates information system privileges per organization defined frequency.	The organization being inspected/assessed reevaluates information system privileges every 90 days . The organization must maintain the reevaluations as an audit trail. DoD has defined the frequency as every 90 days.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organization being inspected/assessed reevaluates information system privileges every 90 days. DoD has defined the frequency as every 90 days.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-1(a)(1)	CCI-001832	The organization disseminates the audit and accountability policy to organization-defined personnel or roles.	The organization being inspected/assessed disseminates, via an information sharing capibility, to the ISSO and ISSM and others as the local organization deems appropriate an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the audit and accountability procedures via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-1(a)(2)	CCI-001834	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The organization being inspected/assessed disseminates, via an information sharing capibility, to the ISSO and ISSM and others as the local organization deems appropriate audit and accountability procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the audit and accountability procedures via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below Enclave		Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-4	CCI-001848	The organization defines the audit record storage requirements.	The organization being inspected/assessed defines and documents the required audit record storage capacity. DoD has determined the audit record storage requirements are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented audit record storage requirements to ensure the organization being inspected/assessed has defined those requirements. DoD has determined the audit record storage requirements are not appropriate to define at the Enterprise level.	LOW		X	X					3.5.4 Audit Storage Capacity and Audit Up...		CCI requirements are met within subparagraph "Audit Storage Capacity and Audit Upload" of UFGS 25 05 11.
N/A	AU-4	CCI-001849	The organization allocates audit record storage capacity in accordance with organization-defined audit record storage requirements.	The organization being inspected/assessed allocates, and configures the information system to allocate audit record storage capacity as defined in AU-4, CCI 1848. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1849.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to allocate audit record storage capacity as defined in AU-4, CCI 1848. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1849.	LOW		X	X					3.5.4 Audit Storage Capacity and Audit Up...		CCI requirements are met within subparagraph "Audit Storage Capacity and Audit Upload" of UFGS 25 05 11.
N/A	AU-4(1)	CCI-001850	The organization defines the frequency on which the information system off-loads audit records onto a different system or media than the system being audited.	DoD has defined the frequency as at a minimum, real-time for interconnected systems and weekly for stand-alone systems.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at a minimum, real-time for interconnected systems and weekly for stand-alone systems.	LOW			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AU-4(1)	CCI-001851	The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.	The organization being inspected/assessed configures the information system to off-load audit records at a minimum, in real-time for interconnected systems and weekly for stand-alone systems onto a different system or media than the system being audited. DoD has defined the frequency as at a minimum, real-time for interconnected systems and weekly for stand-alone systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1851.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to off-load audit records at a minimum, in real-time for interconnected systems and weekly for stand-alone systems onto a different system or media than the system being audited. DoD has defined the frequency as at a minimum, real-time for interconnected systems and weekly for stand-alone systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1851.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AU-5(1)	CCI-001852	The organization defines the personnel, roles and/or locations to receive a warning when allocated audit record storage volume reaches a defined percentage of maximum audit records storage capacity.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO/PMO and ISSM, who shall receive a warning when allocated audit record storage volume reaches a defined percentage of maximum audit records storage capacity. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as at a minimum, the ISSO/PMO and ISSM.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles who should receive a warning when allocated audit record storage volume reaches a defined percentage of maximum audit records storage capacity to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles beyond the ISSO/PMO and ISSM. DoD has defined the personnel or roles as at a minimum, the ISSO/PMO and ISSM.	MOD		X	X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-5(1)	CCI-001853	The organization defines the time period within which organization-defined personnel, roles and/or location are to receive warnings when allocated audit record storage volume reaches a organization-defined percentage of maximum audit records storage capacity.	DoD has defined the time period as immediate.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediate.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-5(1)	CCI-001854	The organization defines the percentage of maximum audit record storage capacity that is to be reached at which time the information system will provide a warning to organization-defined personnel, roles and/or locations.	DoD has defined the percentage as 75 percent.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the percentage as 75 percent.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-5(1)	CCI-001855	The information system provides a warning to organization-defined personnel, roles, and/or locations within organization-defined time period when allocated audit record storage volume reaches organization-defined percentage of repository maximum audit record storage capacity.	The organization being inspected/assessed configures the information system to immediately provide a warning to personnel, roles, and/or locations defined in AU-5 (1), CCI 1852 when allocated audit record storage volume reaches 75 percent of repository maximum audit record storage capacity. DoD has defined the time period as immediate. DoD has defined the percentage as 75 percent. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1855.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to immediately provide a warning to personnel, roles, and/or locations defined in AU-5 (1), CCI 1852 when allocated audit record storage volume reaches 75 percent of repository maximum audit record storage capacity. DoD has defined the time period as immediate. DoD has defined the percentage as 75 percent. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1855.	MOD		X						3.5.4.1 Audit Log Storage Notification In M...		CCI requirements are met within subparagraph "Audit Log Storage Notification In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	AU-6(a)	CCI-001862	The organization defines the types of inappropriate or unusual activity to be reviewed and analyzed in the audit records.	The organization being inspected/assessed defines and documents the types of inappropriate or unusual activity to be reviewed and analyzed in the audit records. DoD has determined that the types of inappropriate or unusual activity are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented types of inappropriate or unusual activity to ensure they have been defined. DoD has determined that the types of inappropriate or unusual activity are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-6(b)	CCI-001863	The organization defines the personnel or roles to receive the reports of organization-defined inappropriate or unusual activity.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO and ISSM, who shall receive the reports of inappropriate or unusual activity defined in AU-6, CCI 1862. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles who should receive the reports of inappropriate or unusual activity defined in AU-6, CCI 1862 to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-6(1)	CCI-001864	The organization employs automated mechanisms to integrate audit review and analysis to support organizational processes for investigation of response to suspicious activities.	The organization being inspected/assessed identifies and implements automated mechanisms to integrate audit review and analysis. The goal is to support organizational investigation of and response to suspicious activities.	The organization conducting the inspection/assessment obtains and examines documentation identifying automated mechanisms to integrate audit review and analysis to ensure such mechanisms have been identified. The organization conducting the inspection/assessment examines the identified automated mechanisms to ensure they have been implemented.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-6(1)	CCI-001865	The organization employs automated mechanisms to integrate reporting processes to support organizational investigation of and response to suspicious activities.	The organization being inspected/assessed identifies and implements automated mechanisms to integrate reporting processes (e.g., centralized log analysis tools). The goal is to support organizational investigation of and response to suspicious activities.	The organization conducting the inspection/assessment obtains and examines documentation identifying automated mechanisms to integrate reporting processes to ensure such mechanisms have been identified. The organization conducting the inspection/assessment examines the identified automated mechanisms to ensure they have been implemented.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-6(10)	CCI-001872	The organization adjusts the level of audit review and analysis within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	The organization being inspected/assessed documents and implements a process for adjusting the level of audit review within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information (e.g., INFOCON).	The organization conducting the inspection/assessment obtains and examines the documented process and supporting records to ensure the organization being inspected/assessed adjusts the level of audit review within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-6(10)	CCI-001874	The organization adjusts the level of audit reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	The organization being inspected/assessed documents and implements a process for adjusting the level of audit reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information (e.g., INFOCON).	The organization conducting the inspection/assessment obtains and examines the documented process and supporting records to ensure the organization being inspected/assessed adjusts the level of audit reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-7(a)	CCI-001875	The information system provides an audit reduction capability that supports on-demand audit review and analysis.	The organization being inspected/assessed must employ information systems that provide an audit reduction capability that support on-demand audit review and analysis (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1875.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed employs information systems that provide an audit reduction capability that support on-demand audit review and analysis (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1875.	MOD	X	X		X				3.5.3.4 Audit Reduction and Report Generati...	FRCS does not have Auditing Front End Software in scope	
N/A	AU-7(a)	CCI-001876	The information system provides an audit reduction capability that supports on-demand reporting requirements.	The organization being inspected/assessed must employ information systems that provide an audit reduction capability that support on-demand reporting requirements (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1876.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed employs information systems that provide an audit reduction capability that supports on-demand reporting requirements (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1876.	MOD	X	X		X				3.5.3.4 Audit Reduction and Report Generati...	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-7(a)	CCI-001877	The information system provides an audit reduction capability that supports after-the-fact investigations of security incidents.	The organization being inspected/assessed must employ information systems that provide an audit reduction capability that support after-the-fact investigations of security incidents (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1877.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed employs information systems that provide an audit reduction capability that supports after-the-fact investigations of security incidents (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1877.	MOD	X	X		X				3.5.3.4 Audit Reduction and Report Generati...	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-7(a)	CCI-001878	The information system provides a report generation capability that supports on-demand audit review and analysis.	The organization being inspected/assessed must employ information systems that provide a report generation capability that support on-demand audit review and analysis (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1878.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed employs information systems that provide a report generation capability that supports on-demand audit review and analysis (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1878.	MOD	X	X		X				3.5.3.4 Audit Reduction and Report Generati...	FRCS does not have Auditing Front End Software in scope	
N/A	AU-7(a)	CCI-001879	The information system provides a report generation capability that supports on-demand reporting requirements.	The organization being inspected/assessed must employ information systems that provide a report generation capability that support on-demand reporting requirements (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1879.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed employs information systems that provide a report generation capability that supports on-demand reporting requirements (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1879.	MOD	X	X		X				3.5.3.4 Audit Reduction and Report Generati...	FRCS does not have Auditing Front End Software in scope	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-7(a)	CCI-001880	The information system provides a report generation capability that supports after-the-fact investigations of security incidents.	The organization being inspected/assessed must employ information systems that provide a report generation capability that support after-the-fact investigations of security incidents (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1880.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed employs information systems that provide a report generation capability that supports after-the-fact investigations of security incidents (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1880.	MOD	X	X		X				3.5.3.4 Audit Reduction and Report Generati...	FRCS does not have Auditing Front End Software in scope	
N/A	AU-7(b)	CCI-001881	The information system provides an audit reduction capability that does not alter original content or time ordering of audit records.	The organization being inspected/assessed must ensure that the audit reduction capability does not alter the original audit records. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1881.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed employs an audit reduction capability that does not alter original audit records. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1881.	MOD	X	X		X				3.5.3.4 Audit Reduction and Report Generati...	FRCS does not have Auditing Front End Software in scope	
N/A	AU-7(b)	CCI-001882	The information system provides a report generation capability that does not alter original content or time ordering of audit records.	The organization being inspected/assessed must ensure that the report generation capability does not alter the original audit records. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1882.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed employs a report generation capability that does not alter original audit records. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1882.	MOD	X	X		X				3.5.3.4 Audit Reduction and Report Generati...	FRCS does not have Auditing Front End Software in scope	
N/A	AU-7(1)	CCI-001883	The organization defines the audit fields within audit records to be processed for events of interest by the information system.	The organization being inspected/assessed must define and document the audit fields within audit records to be processed for events of interest by the information system. DoD has determined that the audit fields are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented audit fields to ensure the organization being inspected/assessed defines the audit fields within audit records to be processed for events of interest by the information system. DoD has determined that the audit fields are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-8(b)	CCI-001888	The organization defines the granularity of time measurement for time stamps generated for audit records.	DoD has defined the granularity of time measurement as one second.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the granularity of time measurement as one second.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AU-8(b)	CCI-001889	The information system records time stamps for audit records that meets organization-defined granularity of time measurement.	The organization being inspected/assessed configures the information system to generate time in the time stamps for audit records that meets one second granularity of time measurement. DoD has defined the granularity of time measurement as one second. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1889.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate time in the time stamps for audit records that meets one second granularity of time measurement. DoD has defined the granularity of time measurement as one second. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1889.	LOW		X						3.5.2 Audit Time Stamps		CCI requirements are met within subparagraph "Audit Time Stamps" of UFGS 25 05 11.
N/A	AU-8(b)	CCI-001890	The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	The organization being inspected/assessed configures the information system to generate time stamps for audit records that contain time zones or time offsets that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1890.	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to generate time stamps for audit records that contain time zones or time offsets that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1890.	LOW		X						3.5.2 Audit Time Stamps		CCI requirements are met within subparagraph "Audit Time Stamps" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-8(1)	CCI-001891	The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.	The organization being inspected/assessed configures the information system to synchronize internal information system clocks every 24 hours for networked systems with an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS) when the time difference is greater than the difference defined in AU-8 (1), CCI 1892. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1891. DoD has defined the frequency as every 24 hours for networked systems. DoD has defined the authoritative time source as an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS)	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed has configured the information system to synchronize internal information system clocks every 24 hours for networked systems with an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS) when the time difference is greater than the difference defined in AU-8 (1), CCI 1892. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1891. DoD has defined the frequency as every 24 hours for networked systems. DoD has defined the authoritative time source as an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS)	MOD		X						3.5.2 Audit Time Stamps		CCI requirements are met within subparagraph "Audit Time Stamps" of UFGS 25 05 11.
N/A	AU-8(1)	CCI-001892	The organization defines the time difference which, when exceeded, will require the information system to synchronize the internal information system clocks to the organization-defined authoritative time source.	The organization being inspected/assessed defines and documents the time difference, which, when exceeded, will require the information system to synchronize the internal information system clocks. DoD has determined the time difference is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented time difference to ensure the organization being inspected/assessed defines the time difference which, when exceeded, will require the information system to synchronize the internal information system clocks. DoD has determined the time difference is not appropriate to define at the Enterprise level.	MOD		X	X					3.5.2 Audit Time Stamps		CCI requirements are met within subparagraph "Audit Time Stamps" of UFGS 25 05 11.
N/A	AU-9(4)	CCI-001894	The organization defines the subset of privileged users who will be authorized access to the management of audit functionality.	The organization being inspected/assessed defines and documents the subset of privileged users to be authorized access to the management of audit functionality. DoD has determined the subset of privileged users is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented subset of privileged users to be authorized access to the management of audit functionality, to ensure the organization being inspected/assessed defines and documents the subset of privileged users to be authorized access to the management of audit functionality. DoD has determined the subset of privileged users is not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-10	CCI-001899	The organization defines the action to be covered by non-repudiation.	DoD has defined the actions to be covered by non-repudiation as actions defined by DoDI 8520.02 and DoDI 8520.03.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the actions to be covered by non-repudiation as actions defined by DoDI 8520.02 and DoDI 8520.03.	MOD		X	X		X			3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-12(b)	CCI-001910	The organization defines the personnel or roles allowed select which auditable events are to be audited by specific components of the information system.	DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	LOW		X		X	X			3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-12(3)	CCI-001911	The organization defines the selectable event criteria to be used as the basis for changes to the auditing to be performed on organization-defined information system components, by organization-defined individuals or roles, within organization-defined time thresholds.	The organization being inspected/assessed defines and documents the selectable event criteria for which changed auditing is to be performed. DoD has determined the selectable event criteria is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented selectable event criteria to ensure the organization being inspected/assessed defines the selectable event criteria for which changed auditing is to be performed. DoD has determined the selectable event criteria is not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-12(3)	CCI-001912	The organization defines the time thresholds for organizational-defined individuals or roles to change the auditing to be performed based on organization-defined selectable event criteria.	The organization being inspected/assessed defines and documents the time thresholds for individuals or roles to change the auditing to be performed on information system components based on selectable event criteria defined in AU-12 (3), CCI 1911 occurs. DoD has determined the time thresholds are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented time thresholds to ensure the organization being inspected/assessed defines the time thresholds for individuals or roles to change the auditing to be performed on information system components based on selectable event criteria defined in AU-12 (3), CCI 1911 occurs. DoD has determined the time thresholds are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-12(3)	CCI-001913	The organization defines the individuals or roles that are to be provided the capability to change the auditing to be performed based on organization-defined selectable event criteria, within organization-defined time thresholds.	The organization being inspected/assessed defines and documents the individuals or roles that are to be provided the capability to change the auditing to be performed based on the selectable event criteria defined in AU-12 (3), CCI 1911, within the time thresholds defined in AU-12 (3), CCI 1912. DoD has determined that the individuals or roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented individuals or roles to ensure the organization being inspected/assessed defines the individuals or roles that are to be provided the capability to change the auditing to be performed based on the selectable event criteria defined in AU-12 (3), CCI 1911, within the time thresholds defined in AU-12 (3), CCI 1912. DoD has determined that the individuals or roles are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-12(3)	CCI-001914	The information system provides the capability for organization-defined individuals or roles to change the auditing to be performed on organization-defined information system components based on organization-defined selectable event criteria within organization-defined time thresholds.	The organization being inspected/assessed configures the information system to provide the capability for individuals or roles defined in AU-12 (3), CCI 1913 to change the auditing to be performed on information system components defined in AU-12 (3), CCI 2047 based on selectable event criteria defined in AU-12 (3), CCI 1911 within time thresholds defined in AU-12 (3), CCI 1912. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1914.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for individuals or roles defined in AU-12 (3), CCI 1913 to change the auditing to be performed on information system components defined in AU-12 (3), CCI 2047 based on selectable event criteria defined in AU-12 (3), CCI 1911 within time thresholds defined in AU-12 (3), CCI 1912. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1914.	MOD		X						3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AU-14(b)	CCI-001919	The information system provides the capability for authorized users to select a user session to capture/record or view/hear.	The organization being inspected/assessed configures the information system to provide the capability for authorized users to select a user session to capture/record or view/hear. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1919.	The organization conducting the inspection/assessments examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for authorized users to select a user session to capture/record or view/hear. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1919.	MOD		X	X					3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	AU-1(a)	CCI-001930	The organization defines the organizational personnel or roles to whom the audit and accountability policy is to be disseminated.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO or ISSM, to whom the audit and accountability policy is to be disseminated. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles to whom the audit and accountability policy is to be disseminated to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AU-1(a)	CCI-001931	The organization defines the organizational personnel or roles to whom the audit and accountability procedures are to be disseminated.	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO or ISSM, to whom the audit and accountability procedures are to be disseminated. If there are no additional personnel or roles, the organization must also document that. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles to whom the audit and accountability procedures are to be disseminated to ensure the organization being inspected/assessed has either defined additional personnel or roles, or identified that there are no additional personnel or roles. DoD has defined the personnel or roles as the ISSO and ISSM and others as the local organization deems appropriate.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IA-1(a)(1)	CCI-001932	The organization documents an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoD documents within DoDI 8520.02 and DoDI 8520.03 an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies. DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-1(a)	CCI-001933	The organization defines the personnel or roles to be recipients of the identification and authentication policy and the procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	DoD has defined the roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate. DoDI 8520.02 and DoDI 8520.03 meet the DoD requirement for Identification and Authentication policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies. DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8520.02 and DoDI 8520.03. DoD has defined the roles to be recipients of the identification and authentication policy and the procedures as the ISSO and ISSM and others as the local organization deems appropriate.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-1(a)	CCI-001934	The organization documents procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	DoD documents within DoDI 8520.02 and DoDI 8520.03 procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies. DoDI 8520.02 and DoDI 8520.03.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 8520.02 and DoDI 8520.03.	LOW	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-2(8)	CCI-001941	The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.	The organization being inspected/assessed configures the information system to implement replay-resistant authentication mechanisms for network access to privileged accounts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1941.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement replay-resistant authentication mechanisms for network access to privileged accounts. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1941.	MOD								---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-2(9)	CCI-001942	The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.	The organization being inspected/assessed configures the information system to implement replay-resistant authentication mechanisms for network access to non-privileged accounts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1942.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement replay-resistant authentication mechanisms for network access to non-privileged accounts. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1942.	MOD		X		X				3.2.6 Cryptographic Protection	FRCS does not contain classified information	
N/A	IA-2(11)	CCI-001947	The organization defines the strength of mechanism requirements for the device that is separate from the system gaining access and is to provide one factor of a multifactor authentication for remote access to privileged accounts.	For the strength of mechanism requirements DoD has defined requirements as DoD PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. For the strength of mechanism requirements DoD has defined requirements as DoD PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H.3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-2(11)	CCI-001948	The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.	The organization being inspected/assessed configures the information system to implement multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1948.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1948.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-2(11)	CCI-001949	The device used in the information system implementation of multifactor authentication for remote access to privileged accounts meets organization-defined strength of mechanism requirements.	The organization being inspected/assessed will use DoD PKI or a technology approved by their Authorizing Official that meet Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1949.	The organization conducting the inspection/assessment obtains and examines the device used to ensure that the device implemented for multifactor authentication for remote access to privileged accounts meets Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1949.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-2(11)	CCI-001950	The organization defines the strength of mechanism requirements for the device that is separate from the system gaining access and is to provide one factor of a multifactor authentication for remote access to non-privileged accounts.	For the strength of mechanism requirements DoD has defined requirements as DoD PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. For the strength of mechanism requirements DoD has defined requirements as DoD PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-2(11)	CCI-001951	The information system implements multifactor authentication for remote access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.	The organization being inspected/assessed configures the information system to implement multifactor authentication for remote access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1951.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement multifactor authentication for remote access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1951.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-2(11)	CCI-001952	The device used in the information system implementation of multifactor authentication for remote access to non-privileged accounts meets organization-defined strength of mechanism requirements.	The organization being inspected/assessed will use DoD PKI or a technology approved by their Authorizing Official that meet Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1952.	The organization conducting the inspection/assessment obtains and examines the device used to ensure that the device implemented for multifactor authentication for remote access to non-privileged accounts meets Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1952.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-2(12)	CCI-001953	The information system accepts Personal Identity Verification (PIV) credentials.	The organization being inspected/assessed configures the information system to accept PIV/CAC authentication. This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1953	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to accept PIV/CAC authentication. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1953.	LOW	X	X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT…		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-2(12)	CCI-001954	The information system electronically verifies Personal Identity Verification (PIV) credentials.	The organization being inspected/assessed configures the information system to verify PIV/CAC authentication. This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1954.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to verify PIV/CAC authentication. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1954.	LOW	X	X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT…		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enriches	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-3	CCI-001958	The information system authenticates an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.	The organization being inspected/assessed configures the network infrastructure to authenticate all mobiles devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1958. DoD has defined the value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	The organization conducting the inspection/assessment examine a sampling of the network infrastructure device configurations to ensure devices connecting to the infrastructure are uniquely authenticated. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1958.	LOW	X	X		X				1.9.4 Control System Inventory Report 3.2.7 Device Identification and Authentic...		Cybersecurity requirement is met by requiring the contractor to identify and document all components within the control system through the Control System Inventory Report. This CCI is further enforced through requiring the contractor to provide 802.1x capable switches when design requires switches. This design requirement is captured in Sub-Paragraph "Control System Inventory Report" within Part 1 and Device Identification and Authentication within Part 3
N/A	IA-3(1)	CCI-001959	The organization defines the specific devices and/or type of devices the information system is to authenticate before establishing a connection.	DoD has defined the value as all network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the value as all network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	MOD		X		X	X			3.2.6 Cryptographic Protection	FRCS does not contain classified information	
N/A	IA-3(4)	CCI-001965	The organization defines the configuration management process that is to handle the device authentication procedures.	The organization being inspected/assessed defines and documents the configuration management process that is to handle the device authentication procedures. DoD has determined the configuration management process is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented configuration management process to ensure the organization being inspected/assessed defines the configuration management process that is to handle the device authentication procedures. DoD has determined the configuration management process is not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-3(4)	CCI-001966	The organization ensures that device identification based on attestation is handled by the organization-defined configuration management process.	The organization being inspected/assessed ensures that device identification based on attestation is handled by the configuration management process defined in IA-3 (4), CCI 1968.	The organization conducting the inspection/assessment obtains and examines the documented configuration management process to ensure the organization being inspected/assessed has device identification based on attestation handled via the configuration management process.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-3(1)	CCI-001967	The information system authenticates organization-defined devices and/or types of devices before establishing a local, remote and/or network connection using bidirectional authentication that is cryptographically based.	The organization being inspected/assessed configures the information system to use cryptographically based bidirectional authentication. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1967.	The organization conducting the inspection/assessment examine a sampling of the network infrastructure device configurations to ensure devices connecting to the infrastructure use cryptographically based bidirectional authentication. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1967.	MOD		X		X				3.2.6 Cryptographic Protection	FRCS does not contain classified information	
N/A	IA-3(4)	CCI-001968	The organization defines the configuration management process that is to handle the device identification procedures.	The organization being inspected/assessed defines and documents the configuration management process that is to handle the device identification procedures. DoD has determined the configuration management process is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented configuration management process to ensure the organization being inspected/assessed defines the configuration management process that is to handle the device identification procedures. DoD has determined the configuration management process is not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-3(4)	CCI-001969	The organization ensures that device authentication based on attestation is handled by the organization-defined configuration management process.	The organization being inspected/assessed ensures that device authentication based on attestation is handled by the configuration management process defined in IA-3 (4), CCI 1965.	The organization conducting the inspection/assessment obtains and examines the documented configuration management process to ensure the organization being inspected/assessed has device authentication based on attestation handled via the configuration management process.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-4(a)	CCI-001970	The organization defines the personnel or roles that authorize the assignment of individual, group, role, and device identifiers.	DoD has defined the personnel or roles as the ISSM or ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSM or ISSO.	LOW	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IA-4(a)	CCI-001971	The organization manages information system identifiers by receiving authorization from organization-defined personnel or roles to assign an individual, group, role or device identifier.	The organization being inspected/assessed implements a process to manage information system identifiers by receiving authorization from the ISSM or ISSO to assign an individual, group, role or device identifier. DoD has defined the personnel or roles as the ISSM or ISSO.	The organization conducting the inspection/assessment obtains and examines documentation and system configuration information to ensure the organization being inspected/assessed manages information system identifiers by receiving authorization from the ISSM or ISSO to assign an individual, group, role or device identifier. DoD has defined the personnel or roles as the ISSM or ISSO.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-4(b)	CCI-001972	The organization manages information system identifiers by selecting an identifier that identifies an individual, group, role, or device.	The organization being inspected/assessed implements a process to manage information system identifiers by selecting an identifier that identifies an individual, group, role, or device.	The organization conducting the inspection/assessment obtains and examines documentation or system configuration information to ensure the organization being inspected/assessed manages information system identifiers by selecting an identifier that identifies an individual, group, role, or device.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-4(c)	CCI-001973	The organization manages information system identifiers by assigning the identifier to the intended individual, group, role, or device.	The organization being inspected/assessed implements a process to manage information system identifiers by assigning the identifier to the intended individual, group, role, or device.	The organization conducting the inspection/assessment obtains and examines documentation or system configuration information to ensure the organization being inspected/assessed manages information system identifiers by assigning the identifier to the intended individual, group, role, or device.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-4(d)	CCI-001974	The organization defines the time period for which the reuse of identifiers is prohibited.	DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier).	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-4(d)	CCI-001975	The organization manages information system identifiers by preventing reuse of identifiers for an organization-defined time period.	The organization being inspected/assessed implements a process for information system identifiers to prevent reuse of identifiers for 1 year for user identifiers (DoD is not going to specify value for device identifier). DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier).	The organization conducting the inspection/assessment obtains and examines documentation or system configuration information to ensure the organization being inspected/assessed prevents the reuse of identifiers for 1 year for user identifiers (DoD is not going to specify value for device identifier). DoD has defined the time period as 1 year for user identifiers (DoD is not going to specify value for device identifier).	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-5(a)	CCI-001980	The organization manages information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.	The organization being inspected/assessed defines and documents procedures for the secure distribution of authenticators. The process shall include verification of the identify of the individual, group, role, or device receiving the authenticator.	The organization conducting the inspection/assessment obtains and examines the documented procedures for the secure distribution of authenticators to ensure they have been defined and that they include a method to verify the identify of the individual, group, role, or device receiving the authenticator.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(d)	CCI-001981	The organization manages information system authenticators by establishing administrative procedures for initial authenticator distribution.	The organization being inspected/assessed defines and documents procedures for the secure distribution of authenticators.	The organization conducting the inspection/assessment obtains and examines the documented procedures for the secure distribution of authenticators to ensure they have been defined.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(d)	CCI-001982	The organization manages information system authenticators by establishing administrative procedures for lost/compromised authenticators.	The organization being inspected/assessed defines and documents procedures for lost/compromised authenticators.	The organization conducting the inspection/assessment obtains and examines the documented procedures for lost/compromised authenticators to ensure they have been defined.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(d)	CCI-001983	The organization manages information system authenticators by establishing administrative procedures for damaged authenticators.	The organization being inspected/assessed defines and documents procedures for the secure disposal of damaged authenticators.	The organization conducting the inspection/assessment obtains and examines the documented procedures for the secure disposal of damaged authenticators to ensure they have been defined.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(d)	CCI-001984	The organization manages information system authenticators by establishing administrative procedures for revoking authenticators.	The organization being inspected/assessed defines and documents procedures for revoking authenticators.	The organization conducting the inspection/assessment obtains and examines the documented procedures for revoking authenticators to ensure the procedures are defined.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(d)	CCI-001985	The organization manages information system authenticators by implementing administrative procedures for initial authenticator distribution.	The organization being inspected/assessed implements administrative procedures for initial authenticator distribution as documented in IA-5, CCIs 1980 & 1981.	The organization conducting the inspection/assessment obtains and examines records of initial authenticator distribution and interviews individuals responsible for authenticator distribution to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCIs 1980 & 1981.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(d)	CCI-001986	The organization manages information system authenticators by implementing administrative procedures for lost/compromised authenticators.	The organization being inspected/assessed implements administrative procedures for the response to lost/compromised authenticators as documented in IA-5, CCI 1982.	The organization conducting the inspection/assessment obtains and examines documented procedures for the response to lost/compromised authenticators to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCI 1982.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(d)	CCI-001987	The organization manages information system authenticators by implementing administrative procedures for damaged authenticators.	The organization being inspected/assessed implements administrative procedures for the response to damaged authenticators as documented in IA-5, CCI 1983.	The organization conducting the inspection/assessment obtains and examines documented procedures for the response to damaged authenticators to ensure that the organization being inspected/assessed implements the process as defined in IA-5, CCI 1983.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5	CCI-001988	The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.	The organization being inspected/assessed documents and enforces a requirement for developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.	The organization conducting the inspection/assessment obtains and examines the documented requirements placed upon developers/installers of information system components to ensure that there is a documented requirement to provide unique authenticators or change default authenticators prior to delivery/installation.	LOW				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(e)	CCI-001989	The organization manages information system authenticators by changing default content of authenticators prior to information system installation.	The organization being inspected/assessed documents and implements a procedures to change default authenticators prior to information system installation.	The organization conducting the inspection/assessment obtains and examines the documented procedures to change default authenticators to ensure the procedures are defined. The organization conducting the inspection/assessment obtains and examines a sampling of authenticator age data for default accounts to ensure that default authenticators are changed prior to installation.	LOW		X						3.4 USER IDENTIFICATION AND AUTHENTICAT...		Cybersecurity design requirements are met through the use of physical security and/or contractor requirement to change all default authentication methods within the control system's capability. This is within Sub-Paragraph "User Identification and Authentication" and further enforced in "Passwords for Devices Minimally Supporting Accounts" within Part 3
N/A	IA-5(j)	CCI-001990	The organization manages information system authenticators by changing authenticators for group/role accounts when membership to those accounts changes.	The organization being inspected/assessed documents and implements procedures for changing authenticators for group/role accounts when membership to those accounts changes.	The organization conducting the inspection/assessment obtains and examines the documented procedures for group/role authenticator change to ensure the procedures are defined and applied when membership to those accounts changes. The organization conducting the inspection/assessment obtains and examines a sampling of authenticator age data and documentation of personnel role changes to ensure that group/role authenticators are changed when membership changes.	LOW	X		X					---	CS is not publically accessible	
N/A	IA-5(2)(d)	CCI-001991	The information system, for PKI-based authentication, implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	The information system must be configured to locally cache revocation data to support path discovery and validation in case of inability to access revocation information via the network. The information system may meet this requirement by locally caching certificate revocation lists (CRLs), Online Certificate Status Protocol (OCSP) responses, or a combination thereof. Cached revocation data must include revocation information from all PKIs serving known or anticipated users of the information system. Cached data must be refreshed with a frequency shorter than the life of the data (e.g. if a CRL is valid for 7 days, a new CRL must be retrieved and cached more frequently than every 7 days) to ensure that cached data is valid and not expired. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1991.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to locally cache revocation data (CRLs and/or OCSP responses) to support path discovery and validation in case of inability to access revocation information via the network. The organization conducting the inspection/assessment examines the information system to ensure that revocation data is cached for all PKIs serving known or anticipated users of the information system. The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured a process for the information system to refresh cached revocation data prior to the data's expiration. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1991.	MOD	X	X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-5(3)	CCI-001992	The organization defines the personnel or roles responsible for authorizing the organization's registration authority accountable for the authenticator registration process.	The DoD PKI Registration Authority (RA) – Local Registration Authority (LRA) Certification Practice Statement (CPS) defines the nomination process for DoD PKI RAs. The NSS PKI DoD Registration Practice Statement (RPS) defines the nomination process for NSS PKI RAs for DoD. DoD Components are automatically compliant with this CCI because they are covered by the DoD PKI RA-LRA CPS and NSS PKI DoD RPS.	The DoD PKI RA–LRA CPS defines the nomination process for DoD PKI RAs. The NSS PKI DoD RPS defines the nomination process for NSS PKI RAs for DoD. DoD Components are automatically compliant with this CCI because they are covered by the DoD PKI RA-LRA CPS and NSS PKI DoD RPS.	MOD	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-5(3)	CCI-001993	The organization defines the registration authority accountable for the authenticator registration process.	The DoD PKI Certificate Policy (CP) defines the role and responsibilities of a DoD PKI Registration Authority (RA). The NSS PKI CP defines the role and responsibilities of an NSS PKI RA. DoD Components are automatically compliant with this CCI because they are covered by the DoD PKI CP and NSS PKI CP.	The DoD PKI CP defines the role and responsibilities of a DoD PKI Registration Authority (RA). The NSS PKI CP defines the role and responsibilities of an NSS PKI RA. DoD Components are automatically compliant with this CCI because they are covered by the DoD PKI CP and NSS PKI CP.	MOD	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-5(3)	CCI-001994	The organization defines the types of and/or specific authenticators that are subject to the authenticator registration process.	The DoD PKI Certificate Policy (CP) defines DoD PKI subscribers (entities identified as the subject of PKI certificates) and the authentication requirements for issuance of credentials to subscribers. The NSS PKI CP defines NSS PKI subscribers and the authentication requirements for issuance of credentials to subscribers. DoD Components are automatically compliant with this CCI because they are covered by the DoD PKI CP and NSS PKI CP.	The DoD PKI CP defines DoD PKI subscribers and the authentication requirements for issuance of credentials to subscribers. The NSS PKI CP defines NSS PKI subscribers and the authentication requirements for issuance of credentials to subscribers. DoD Components are automatically compliant with this CCI because they are covered by the DoD PKI CP and NSS PKI CP.	MOD	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-5(3)	CCI-001995	The organization requires that the registration process, to receive organization-defined types of and/or specific authenticators, be conducted in person, or by a trusted third-party, before organization-defined registration authority with authorization by organization-defined personnel or roles.	The DoD PKI Certificate Policy (CP) requires in-person authentication of DoD PKI applicants in accordance with each Certificate Management Authority's (CMA's) Certification Practice Statement (CPS) prior to issuance of credentials. The NSS PKI CP requires in-person authentication of NSS PKI applicants by a Registration Authority (RA) or Trusted Agent (TA) prior to issuance of credentials. DoD Components are automatically compliant with this CCI because they are covered by the DoD PKI CP and NSS PKI CP.	The DoD PKI CP requires in-person authentication of DoD PKI applicants in accordance with each CMA's CPS prior to issuance of credentials. The NSS PKI CP requires in-person authentication of NSS PKI applicants by an RA or TA prior to issuance of credentials. DoD Components are automatically compliant with this CCI because they are covered by the DoD PKI CP and NSS PKI CP.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(4)	CCI-001996	The organization defines the requirements required by the automated tools to determine if password authenticators are sufficiently strong.	DoD has defined the requirements as the complexity as identified in IA-5 (1) Part A.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements as the complexity as identified in IA-5 (1) Part A.	MOD		X	X		X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-5(4)	CCI-001997	The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy organization-defined requirements.	The organization being inspected/assessed implements automated tools to check passwords strength per the complexity requirements defined in IA-5 (1) Part A.	The organization conducting the inspection/assessment examines the automated tools and inspects the configuration of the automated tools to ensure that they are implemented to check password strength per the complexity requirements defined in IA-5 (1) Part A.	MOD		X	X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-5(11)	CCI-002002	The organization defines the token quality requirements to be employed by the information system mechanisms for token-based authentication.	DoDI 8520.03 defines types of authentication credentials that are acceptable for authentication to different systems based on the systems' information sensitivity levels and the users' access environments. The definitions for credential strengths D, E and H found in DoDI 8520.03 Enclosure 3, Section 3 specifically deal with acceptable types of hardware PKI credentials. DoD Components are automatically compliant with this CCI because they are covered by the DoD-level policy, DoDI 8520.03.	DoDI 8520.03 defines types of authentication credentials that are acceptable for authentication to different systems based on the systems' information sensitivity levels and the users' access environments. The definitions for credential strengths D, E and H found in DoDI 8520.03 Enclosure 3, Section 3 specifically deal with acceptable types of hardware PKI credentials. DoD Components are automatically compliant with this CCI because they are covered by the DoD-level policy, DoDI 8520.03.	LOW	X	X		X	X			3.4 USER IDENTIFICATION AND AUTHENTICAT…		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(11)	CCI-002003	The information system, for token-based authentication, employs mechanisms that satisfy organization-defined token quality requirements.	The information system performing hardware token-based authentication must be configured to accept only DoD-approved PKI credentials in accordance with DoDI 8520.02 and DoDI 8520.03. For unclassified systems, DoD-approved PKI credentials include DoD PKI credentials, External Certification Authority (ECA) PKI credentials, and DoD-approved external PKI credentials. For SIPRNet, DoD-approved PKI credentials include DoD PKI credentials and NSS PKI credentials. If the information system accepts DoD-approved external PKI credentials, the information system must be configured to accept only certificates at approved assurance levels, as represented by the Certificate Policy Object Identifiers (OIDs) asserted in the certificate. The current list of DoD-approved external PKIs and acceptable Object Identifiers (OIDs) for each approved external PKI is available at http://iase.disa.mil/pki-pke/interoperability.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept only DoD-approved PKI credentials in accordance with (IAW) DoDI 8520.02 and DoDI 8520.03. If the information system accepts DoD-approved external PKI credentials, the organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept only DoD-approved external PKI credentials that assert an approved Certificate Policy OID and reject credentials issued off of DoD-approved external PKIs that do not assert an approved OID.	LOW	X	X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT…		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3
N/A	IA-5(13)	CCI-002006	The organization defines the time period after which the use of cached authenticators are prohibited.	The organization being inspected/assessed defines and documents the time period after which the use of cached authenticators are prohibited. DoD has determined the time period is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented time period to ensure it has been defined. DoD has determined the time period is not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-5(13)	CCI-002007	The information system prohibits the use of cached authenticators after an organization defined time period.	The organization being inspected/assessed configures the information system to prohibit the use of cached authenticators after an organization defined time period. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2007.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prohibit the use of cached authenticators after an organization defined time period. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2007.	MOD		X	X					3.4 USER IDENTIFICATION AND AUTHENTICAT…		CCI requirements are addressed within subparagraph "USER IDENTIFICATION AND AUTHENTICATION" of UFGS 25 05 11.
N/A	IA-5(14)	CCI-002008	The organization, for PKI-based authentication, employs a deliberate organization-wide methodology for managing the content of PKI trust stores installed across all platforms including networks, operating systems, browsers, and applications.	DoD trust store management requirements are defined in information system components' applicable STIGs and SRGs. All information systems are required to undergo a STIG compliance review as part of their certification and accreditation process prior to being granted an authority to operate. DoD Components are automatically compliant with this CCI because they are covered by the DoD-level STIGs and SRGs.	DoD trust store management requirements are defined in information system components' applicable STIGs and SRGs. All information systems are required to undergo a STIG compliance review as part of their certification and accreditation process prior to being granted an authority to operate. DoD Components are automatically compliant with this CCI because they are covered by the DoD-level STIGs and SRGs.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-8(1)	CCI-002009	The information system accepts Personal Identity Verification (PIV) credentials from other federal agencies.	The information system performing hardware token-based authentication must be configured to accept DoD-approved external PKI PIV credentials to authenticate federal agency users in accordance with DoDI 8520.02 and DoDI 8520.03. The information system must be configured to accept only certificates at approved assurance levels, as represented by the Certificate Policy Object Identifiers (OIDs) asserted in the certificate. The current list of DoD-approved external PKIs and acceptable Object Identifiers (OIDs) for each approved external PKI is available at http://iase.disa.mil/pki-pke/interoperability. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2009.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept DoD-approved external PKI PIV credentials in accordance with DoDI 8520.02 and DoDI 8520.03. The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to accept only DoD-approved external PKI PIV credentials that assert an approved Certificate Policy OID and reject credentials issued off of DoD-approved external PKIs that do not assert an approved OID. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2009.	LOW	X			X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-8(1)	CCI-002010	The information system electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.	The information system performing hardware token-based authentication must be configured to validate DoD-approved external PKI PIV credentials to authenticate federal agency users in accordance with RFC 5280. The information system must be configured to perform a revocation check as part of the certificate validation process. Revocation checking may be performed using certificate revocation lists (CRLs) published by the issuing PKI or Online Certificate Status Protocol (OCSP) services. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2010.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to validate DoD-approved external PKI PIV credentials in accordance with RFC 5280. The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed has configured the information system to perform a revocation check as part of the certificate validation process. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2010.	LOW	X			X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-8(2)	CCI-002011	The information system accepts FICAM-approved third-party credentials.	The organization being inspected/assessed configures the information system to accept Federal Identity, Credential, and Access Management (FICAM)-approved third-party credentials. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2011. FICAM Guidance is available at http://www.idmanagement.gov.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to accept FICAM-approved third-party credentials For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2011.	LOW	X			X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-8(3)	CCI-002012	The organization defines the information systems which will employ only FICAM-approved information system components.	The organization being inspected/assessed defines and documents the information systems which will employ only Federal Identity, Credential, and Access Management (FICAM)-approved information system components. DoD has determined the information systems are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information systems to ensure they have been defined. DoD has determined the information systems are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IA-8(3)	CCI-002013	The organization employs only FICAM-approved information system components in organization-defined information systems to accept third-party credentials.	The organization being inspected/assessed employs only Federal Identity, Credential, and Access Management (FICAM)-approved information system components to accept third-party credentials in information systems defined in IA-8 (3), CCI 2012. FICAM Guidance is available at http://www.idmanagement.gov.	The organization conducting the inspection/assessment obtains and examines the list of information system components in use to ensure the organization being inspected/assessed uses only FICAM-approved components in information systems defined in IA-8 (3), CCI 2012.	LOW	X			X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	IA-8(4)	CCI-002014	The information system conforms to FICAM-issued profiles.	The organization being inspected/assessed configures the information system to conform to Federal Identity, Credential, and Access Management (FICAM)-issued profiles. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2014. FICAM Guidance is available at http://www.idmanagement.gov.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to conform to FICAM-issued profiles. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2014.	LOW	X			X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(1)(f)	CCI-002041	The information system allows the use of a temporary password for system logons with an immediate change to a permanent password.	The organization being inspected/assessed configures the information system to allow the use of a temporary password for system logons with an immediate change to a permanent password. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2041.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to allow the use of a temporary password for system logons with an immediate change to a permanent password. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2041.	LOW	X	X		X				3.4 USER IDENTIFICATION AND AUTHENTICAT…		Cybersecurity design requirements are met through Sub-Paragraph "User Identification and Authentication" within Part 3

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IA-5(h)	CCI-002042	The organization manages information system authenticators by protecting authenticator content from unauthorized modification.	The organization being inspected/assessed configures the information system to manage information system authenticators by protecting authenticator content from unauthorized modification. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2042.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to manage information system authenticators by protecting authenticator content from unauthorized modification. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2042.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-11(1)	CCI-002044	The organization defines measures to be employed to ensure that long-term audit records generated by the information system can be retrieved.	The organization being inspected/assessed defines and documents measures to be employed to ensure that long-term audit records generated by the information system can be retrieved. DoD has determined that the measures are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented measures to ensure the organization being inspected/assessed defines measures to be employed to ensure that long-term audit records generated by the information system can be retrieved. DoD has determined that the measures are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-11(1)	CCI-002045	The organization employs organization-defined measures to ensure that long-term audit records generated by the information system can be retrieved.	The organization being inspected/assessed employs the measures defined in AU-11 (1), CCI 2044 to ensure that long-term audit records generated by the information system can be retrieved.	The organization conducting the inspection/assessment obtains and examines the documented measures to ensure the organization being inspected/assessed employs the measures defined in AU-11 (1), CCI 2044 to ensure that long-term audit records generated by the information system can be retrieved.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AU-8(1)	CCI-002046	The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.	The organization being inspected/assessed configures the information system to synchronize the internal system clocks to the authoritative time source when the time difference is greater than the time period defined in AU-8 (1), CCI 1892. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2046.	The organization conducting the inspection/assessment examines the information system to ensure the system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the time period defined in AU-8 (1), CCI 1892. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2046.	MOD		X						3.5.2 Audit Time Stamps		CCI requirements are met within subparagraph "Audit Time Stamps" of UFGS 25 05 11.
N/A	AU-12(3)	CCI-002047	The organization defines the information system components on which the auditing that is to be performed can be changed by organization-defined individuals or roles.	The organization being inspected/assessed defines and documents the information system components on which the auditing that is to be performed can be changed by individuals or roles defined in AU-12 (3), CCI 1913. DoD has determined the information system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed has defined the information system components on which the auditing that is to be performed can be changed by the individuals or roles defined in AU-12 (3), CCI 1913. DoD has determined the information system components are not appropriate to define at the Enterprise level.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AT-1(a)	CCI-002048	The organization defines the personnel or roles to whom the security awareness and training policy is disseminated.	DoD has defined the roles as organizational personnel with security awareness and training responsibilities. DoD disseminates DoDD 8570.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/dir.html	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with security awareness and training responsibilities.	LOW			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AT-1(a)	CCI-002049	The organization defines the personnel or roles to whom the security awareness and training procedures are disseminated.	DoD has defined the roles as organizational personnel with security awareness and training responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with security awareness and training responsibilities.	LOW			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AT-3(2)	CCI-002051	The organization defines the personnel or roles to whom initial and refresher training in the employment and operation of physical security controls is to be provided.	The organization being inspected/assessed defines and documents the personnel or roles to whom initial and refresher training in the employment and operation of physical security controls is to be provided. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles to whom initial and refresher training in the employment and operation of physical security controls is to be provided. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AT-3(4)	CCI-002053	The organization provides training to its personnel on organization-defined indicators of malicious code to recognize suspicious communications and anomalous behavior in organizational information systems.	The organization being inspected/assessed provides training to its personnel on indicators of malicious code defined in AT-3 (4), CCI 2054 to recognize suspicious communications and anomalous behavior in organizational information systems.	The organization conducting the inspection/assessment obtains and examines the training materials and indicators of malicious code defined in AT-3 (4), CCI 2054 to ensure the organization being inspected/assessed provides users with the means to recognize suspicious communications and anomalous behavior in organizational information systems.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AT-3(4)	CCI-002054	The organization defines indicators of malicious code to recognize suspicious communications and anomalous behavior in organizational information systems.	The organization being inspected/assessed defines and documents indicators of malicious code to recognize suspicious communications and anomalous behavior in organizational information systems. DoD has determined the indicators are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented indicators to ensure the organization being inspected/assessed defines indicators of malicious code to recognize suspicious communications and anomalous behavior in organizational information systems. DoD has determined the indicators are not appropriate to define at the Enterprise level.	MOD		X	X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AT-2(2)	CCI-002055	The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.	The IA Awareness CBT, "Cyber Awareness Challenge," and Virtual Training Environment (VTE) Courses: "Introduction to Insider Threat" and "Monitoring for Insider Threat" available on the IASE website meet the DoD requirement to include security awareness training on recognizing and reporting potential indicators of insider threat. DoD Components are automatically compliant with this CCI because they are covered by the DoD level training available on the IASE website.	The IA Awareness CBT, "Cyber Awareness Challenge," and Virtual Training Environment (VTE) Courses: "Introduction to Insider Threat" and "Monitoring for Insider Threat" available on the IASE website meet the DoD requirement to include security awareness training on recognizing and reporting potential indicators of insider threat. DoD Components are automatically compliant with this CCI because they are covered by the DoD level training available on the IASE website.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CM-3(e)	CCI-002056	The organization defines the time period the record of configuration-controlled changes are to be retained.	DoD has defined the time period as a time period defined by the organization's CCB.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as a time period defined by the organization's CCB.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CM-6(1)	CCI-002059	The organization defines the information system components for which the organization will employ automated mechanisms to centrally manage, apply, and verify configuration settings.	The organization being inspected/assessed defines and documents the information system components for which the organization will employ automated mechanisms to centrally manage, apply, and verify configuration settings. DoD has determined the information system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examine the documented information system components to ensure the organization being inspected/assessed defines the information system components for which the organization will employ automated mechanisms to centrally manage, apply, and verify configuration settings. DoD has determined the information system components are not appropriate to define at the Enterprise level.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-1(a)	CCI-002061	The organization defines the personnel or roles to whom security assessment and authorization policy is to be disseminated.	DoD has defined the personnel or roles as all personnel. DoD disseminates DoDI 8510.01 organization-wide via the DoD Issuances website. http://www.dtic.mil/whs/directives/corres/ins1.html	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.	LOW			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CA-1(a)	CCI-002062	The organization defines the personnel or roles to whom the security assessment and authorization procedures are to be disseminated.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.	LOW			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	CA-2(1)	CCI-002063	The organization defines the level of independence for assessors or assessment teams to conduct security control assessments of organizational information systems.	The organization being inspected/assessed defines and documents the level of independence for assessors or assessment teams to conduct security control assessments of organizational information systems. DoD has determined the level of independence is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented level of independence to ensure the organization being inspected/assessed defines the level of independence for assessors or assessment teams to conduct security control assessments of organizational information systems. DoD has determined the level of independence is not appropriate to define at the Enterprise level.	MOD			X					---	CS does not use VoIP	
N/A	CA-2(a)(3)	CCI-002070	The organization's security assessment plan describes assessment team, assessment roles and responsibilities.	The organization being inspected/assessed lists their assessment team members and their associated assessment roles and responsibilities in the security assessment plan.	The organization conducting the inspection/assessment obtains and examines the security assessment plan to ensure the organization being inspected/assessed lists their assessment team members and their associated assessment roles and responsibilities in the security assessment plan.	LOW			X					---	CS does not use VoIP	
N/A	CA-2(d)	CCI-002071	The organization defines the individuals or roles to whom the results of the security control assessment is to be provided.	DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM.	LOW					X			---	CS does not use VoIP	
N/A	CA-3(5)	CCI-002080	The organization employs either an allow-all, deny-by exception or deny-all, permit by exception policy for allowing organization-defined information systems to connect to external information systems.	The organization being inspected/assessed configures the information system to employ a deny-all, permit by exception policy for allowing any systems requiring external connectivity to connect to external information systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2080. DoD has defined the information systems as any systems requiring external connectivity.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to employ a deny-all, permit by exception policy for allowing any systems requiring external connectivity to connect to external information systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2080. DoD has defined the information systems as any systems requiring external connectivity.	MOD	X							---	CS does not use VoIP	
N/A	CA-3(5)	CCI-002081	The organization defines the information systems that employ either allow-all, deny-by-exception or deny-all, permit by exception policy for allowing connection to external information systems.	DoD has defined the information systems as any systems requiring external connectivity.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information systems as any systems requiring external connectivity.	MOD	X							---	CS does not use VoIP	
N/A	CA-3(5)	CCI-002082	The organization selects either allow-all, deny-by exception or deny-all, permit by exception policy for allowing organization-defined information systems to connect to external information systems.	The organization being inspected/assessed selects deny-all, permit by exception policy for allowing any systems requiring external connectivity to connect to external information systems. DoD has defined the information systems as any systems requiring external connectivity.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed selects deny-all, permit by exception policy for allowing any systems requiring external connectivity to connect to external information systems. DoD has defined the information systems as any systems requiring external connectivity.	MOD	X							---	CS does not act as external DNS server	
N/A	CA-3(c)	CCI-002083	The organization reviews and updates Interconnection Security Agreements on an organization-defined frequency.	The organization being inspected/assessed reviews and updates Interconnection Security Agreements at least annually. The organization must maintain an audit trail of reviews and updates. DoD has defined the frequency as at least annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates Interconnection Security Agreements at least annually. DoD has defined the frequency as at least annually.	LOW			X					---	CS does not act as external DNS server	
N/A	CA-3(c)	CCI-002084	The organization defines the frequency that reviews and updates to the Interconnection Security Agreements must be conducted.	DoD has defined the frequency as at least annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at least annually.	LOW					X			---	CS does not act as external DNS server	
N/A	CA-7(1)	CCI-002085	The organization defines the level of independence the assessors or assessment teams must have to monitor the security controls in the information system on an ongoing basis.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	MOD			X					---	CS does not act as external DNS server	
N/A	CA-7(a)	CCI-002087	The organization establishes and defines the metrics to be monitored for the continuous monitoring program.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CA-7(b)	CCI-002088	The organization establishes and defines the frequencies for continuous monitoring.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	CA-7(b)	CCI-002089	The organization establishes and defines the frequencies for assessments supporting continuous monitoring.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CA-7(d)	CCI-002090	The organization implements a continuous monitoring program that includes ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CA-7(e)	CCI-002091	The organization implements a continuous monitoring program that includes correlation and analysis of security-related information generated by assessments and monitoring.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	CS does not act as external DNS server	
N/A	CA-7(f)	CCI-002092	The organization implements a continuous monitoring program that includes response actions to address results of the analysis of security-related information.	Future DoD-wide CM guidance to be published	Future DoD-wide CM guidance to be published	LOW			X					---	CS does not act as external DNS server	
N/A	CA-9(a)	CCI-002101	The organization authorizes internal connections of organization-defined information system components or classes of components to the information system.	The organization being inspected/assessed authorizes internal connections of information system components defined in CA-9, CCI 2102 or classes of components to the information system. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes internal connections of information system components defined in CA-9, CCI 2102 or classes of components to the information system.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CA-9(a)	CCI-002102	The organization defines the information system components or classes of components that that are authorized internal connections to the information system.	The organization being inspected/assessed defines and documents the information system components or classes of components that that are authorized internal connections to the information system. DoD has determined the information system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components or classes of components that that are authorized internal connections to the information system. DoD has determined the information system components are not appropriate to define at the Enterprise level.	LOW		X						1.9.3 Network Communication Report		Cybersecurity requirements will be documented by the contractor and required for submission of the Network Communication Report. This is documented within Sub-Paragraph "Network Communication Report" withing Part 1
N/A	CA-9(b)	CCI-002103	The organization documents, for each internal connection, the interface characteristics.	The organization being inspected/assessed documents, for each internal connection, the interface characteristics.	The organization conducting the inspection/assessment obtains and examines the documented interface characteristics as well as the network topology to ensure the organization being inspected/assessed documents, for each internal connection, the interface characteristics.	LOW		X						1.9.3 Network Communication Report		Cybersecurity requirements will be documented by the contractor and required for submission of the Network Communication Report. This is documented within Sub-Paragraph "Network Communication Report" withing Part 1
N/A	CA-9(b)	CCI-002104	The organization documents, for each internal connection, the security requirements.	The organization being inspected/assessed documents, for each internal connection, the security requirements.	The organization conducting the inspection/assessment obtains and examines the documented security requirements as well as the network topology to ensure the organization being inspected/assessed documents, for each internal connection, the security requirements.	LOW		X						1.9.3 Network Communication Report		Cybersecurity requirements will be documented by the contractor and required for submission of the Network Communication Report. This is documented within Sub-Paragraph "Network Communication Report" withing Part 1
N/A	CA-9(b)	CCI-002105	The organization documents, for each internal connection, the nature of the information communicated.	The organization being inspected/assessed documents, for each internal connection, the nature of the information communicated.	The organization conducting the inspection/assessment obtains and examines the documented nature of information communication as well as the network topology to ensure the organization being inspected/assessed documents, for each internal connection, the nature of the information communicated.	LOW		X						1.9.3 Network Communication Report		Cybersecurity requirements will be documented by the contractor and required for submission of the Network Communication Report. This is documented within Sub-Paragraph "Network Communication Report" withing Part 1
N/A	AC-1(a)	CCI-002107	The organization defines the personnel or roles to be recipients of the access control policy necessary to facilitate the implementation of the access control policy and associated access controls.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.	LOW			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AC-1(a)	CCI-002108	The organization defines the personnel or roles to be recipients of the procedures necessary to facilitate the implementation of the access control policy and associated access controls.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.	LOW			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(a)	CCI-002110	The organization defines the information system account types that support the organizational missions/business functions.	The organization being inspected/assessed defines and documents the information system account types that support the organizational missions/business functions. DoD has determined the information system account types are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system account types to ensure the organization being inspected/assessed defines the information system account types that support the organizational missions/business functions. DoD has determined the information system account types are not appropriate to define at the Enterprise level.	LOW		X						3.3.1 User Accounts		Cybersecurity requirements are met for user accounts (including device capabilities) within Sub-Paragraph "User Accounts" within Part 3
N/A	AC-2(a)	CCI-002111	The organization identifies and selects the organization-defined information system account types of information system accounts which support organizational missions/business functions.	The account types are defined per AC-2, CCI 2110.	The account types are defined per AC-2, CCI 2110.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(b)	CCI-002112	The organization assigns account managers for information system accounts.	The organization being inspected/assessed documents personnel responsible for the management of system accounts.	The organization conducting the inspection/assessment obtains and examines the documented appointment of management personnel to ensure that the organization being inspected/assessed has documented personnel responsible for the management of system accounts.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(c)	CCI-002113	The organization establishes conditions for role membership.	The organization being inspected/assessed documents conditions for adding accounts as members of roles.	The organization conducting the inspection/assessment obtains and examines the documented conditions for adding accounts as members of roles to ensure that the conditions are established.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(d)	CCI-002115	The organization specifies authorized users of the information system.	The organization being inspected/assessed documents authorized users of the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of authorized users for a sampling of information system accounts to ensure that the authorized users are specified.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(d)	CCI-002116	The organization specifies authorized group membership on the information system.	The organization being inspected/assessed documents authorized group membership on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of authorized groups for a sampling of information system accounts to ensure that the authorized groups are specified.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(d)	CCI-002117	The organization specifies authorized role membership on the information system.	The organization being inspected/assessed documents authorized role membership on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of authorized roles for a sampling of information system accounts to ensure that the authorized roles are specified	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(d)	CCI-002118	The organization specifies access authorizations (i.e., privileges) for each account on the information system.	The organization being inspected/assessed documents access authorizations (i.e., privileges) for each account on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of access authorizations for a sampling of information system accounts to ensure that the access authorizations are specified.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-2(d)	CCI-002119	The organization specifies other attributes for each account on the information system.	The organization being inspected/assessed documents other attributes for each account on the information system.	The organization conducting the inspection/assessment obtains and examines the documented list of other attributes for a sampling of information system accounts to ensure that other attributes are specified.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(e)	CCI-002120	The organization defines the personnel or roles authorized to approve the creation of information system accounts.	DoD has defined the personnel or roles as the ISSM or ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSM or ISSO.	LOW			X	X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(f)	CCI-002121	The organization defines the procedures or conditions to be employed when creating, enabling, modifying, disabling, and removing information system accounts.	The organization being inspected/assessed defines and documents the procedures or conditions to be employed when creating, enabling, modifying, disabling, and removing information system accounts. DoD has determined the procedures or conditions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented procedures or conditions to ensure the organization being inspected/assessed defines the procedures or conditions to be employed when creating, enabling, modifying, disabling, and removing information system accounts. DoD has determined the procedures or conditions are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(g)	CCI-002122	The organization monitors the use of information system accounts.	The organization being inspected/assessed implements a process to monitor the use of information system accounts.	The organization conducting the inspection/assessment obtains and examines the audit trail to ensure that the organization being inspected/assessed implements a process to monitor the use of information system accounts.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(h)(1)	CCI-002123	The organization notifies account managers when accounts are no longer required.	The organization being inspected/assessed implements a process to notify account managers when accounts are no longer required. The organization being inspected/assessed maintains an audit trail of notifications.	The organization conducting the inspection/assessment obtains and examines the audit trail of notifications to ensure the organization being inspected/assessed implements a process to notify account managers when accounts are no longer required.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(h)(2)	CCI-002124	The organization notifies account managers when users are terminated or transferred.	The organization being inspected/assessed implements a process to notify account managers when users are terminated or transferred. The organization being inspected/assessed maintains an audit trail of notifications.	The organization conducting the inspection/assessment obtains and examines the audit trail of notifications to ensure the organization being inspected/assessed implements a process to notify account managers when users are terminated or transferred.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(h)(3)	CCI-002125	The organization notifies account managers when individual information system usage or need-to-know changes.	The organization being inspected/assessed implements a process to notify account managers when individual information system usage or need-to-know changes. The organization being inspected/assessed maintains an audit trail of notifications.	The organization conducting the inspection/assessment obtains and examines the audit trail of notifications to ensure the organization being inspected/assessed implements a process to notify account managers when individual information system usage or need-to-know changes.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(i)(1)	CCI-002126	The organization authorizes access to the information system based on a valid access authorization.	The organization being inspected/assessed authorizes access to the information system based on the access authorization process. The organization being inspected/assessed maintains an audit trail of approved access.	The organization conducting the inspection/assessment obtains and examines the audit trail of approved access to ensure the organization being inspected/assessed authorizes access to the information system based on the access authorization process.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(i)(2)	CCI-002127	The organization authorizes access to the information system based on intended system usage.	The organization being inspected/assessed authorizes access to the information system based on intended system usage. The organization being inspected/assessed maintains an audit trail of approved access.	The organization conducting the inspection/assessment obtains and examines the audit trail of approved access to ensure the organization being inspected/assessed authorizes access to the information system based on intended system usage.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(i)(3)	CCI-002128	The organization authorizes access to the information system based on other attributes as required by the organization or associated missions/business functions.	The organization being inspected/assessed authorizes access to the information system based on other attributes as required by the organization or associated missions/business functions. The organization being inspected/assessed maintains an audit trail of approved access.	The organization conducting the inspection/assessment obtains and examines the audit trail of approved access to ensure the organization being inspected/assessed authorizes access to the information system based on other attributes as required by the organization or associated missions/business functions.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(k)	CCI-002129	The organization establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	The organization being inspected/assessed includes in the account management procedures a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	The organization conducting the inspection/assessment obtains and examines the account management procedures to ensure the organization being inspected/assessed includes in the account management procedures a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(4)	CCI-002130	The information system automatically audits account enabling actions.	The organization being inspected/assessed configures the information system to automatically audit account enabling actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2130.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically audit account enabling actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2130.	MOD	X	X		X				3.3.1 User Accounts		CCI requirements are met within subparagraph "User Accounts" of UFGS 25 05 11.
N/A	AC-2(4)	CCI-002131	The organization defines the personnel or roles to be notified on account creation, modification, enabling, disabling, and removal actions.	DoD has defined the personnel or roles as the system administrator and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the system administrator and ISSO.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AC-2(4)	CCI-002132	The information system notifies organization-defined personnel or roles for account enabling actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account enabling actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2132. DoD has defined the personnel or roles as the system administrator and ISSO.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account enabling actions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2132. DoD has defined the personnel or roles as the system administrator and ISSO.	MOD	X	X						3.3.1 User Accounts		CCI requirements are met within subparagraph "User Accounts" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-2(5)	CCI-002133	The organization defines other conditions when users are required to log out.	The organization being inspected/assessed defines and documents the other conditions when users are required to log out. DoD has determined the conditions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure they have been defined. DoD has determined the conditions are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(7)(c)	CCI-002136	The organization defines the actions to be taken when privileged role assignments are no longer appropriate	DoD has defined the actions as disables (or revokes) privileged user account.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the actions as disables (or revokes) privileged user account.	MOD			X		X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(7)(c)	CCI-002137	The organization takes organization-defined actions when privileged role assignments are no longer appropriate.	The organization being inspected/assessed documents and implements a process to disable (or revoke) the privileged user account when privileged role assignments are no longer appropriate. The organization must maintain an audit trail of the actions taken. DoD has defined the actions as disables (or revokes) privileged user account.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of actions taken to ensure the organization being inspected/assessed disables (or revokes) the privileged user account when privileged role assignments are no longer appropriate. DoD has defined the actions as disables (or revokes) privileged user account.	MOD			X		X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(9)	CCI-002140	The organization defines the conditions for establishing shared/group accounts.	The organization being inspected/assessed defines and documents the conditions for establishing shared/group accounts. DoD has determined the conditions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure they have been defined. DoD has determined the conditions are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(9)	CCI-002141	The organization only permits the use of shared/group accounts that meet organization-defined conditions for establishing shared/group accounts.	The organization being inspected/assessed only permits the use of shared/group accounts that meet the conditions for establishing shared/group accounts defined in AC-2 (9), CCI 2140.	The organization conducting the inspection/assessment examines the shared/group accounts to ensure the organization being inspected/assessed only permits the use of shared/group accounts that meet the conditions for establishing shared/group accounts defined in AC-2 (9), CCI 2140.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(10)	CCI-002142	The information system terminates shared/group account credentials when members leave the group.	The organization being inspected/assessed configures the information system to terminate shared/group account credentials when members leave the group. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2142.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to terminate shared/group account credentials when members leave the group. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2142.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-2(12)(a)	CCI-002146	The organization defines atypical usage for which the information system accounts are to be monitored.	The organization being inspected/assessed defines and documents atypical usage for which the information system accounts are to be monitored. DoD has determined atypical usage is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented atypical usage to ensure it has been defined. DoD has determined atypical usage is not appropriate to define at the Enterprise level.	MOD		X	X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(12)(a)	CCI-002147	The organization monitors information system accounts for organization-defined atypical use.	The organization being inspected/assessed monitors information system accounts for atypical use defined in AC-2 (12), CCI 2146. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the audit trail of monitoring to ensure the organization being inspected/assessed monitors information system accounts for atypical use defined in AC-2 (12), CCI 2146.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(12)(b)	CCI-002148	The organization defines the personnel or roles to whom atypical usage of information system accounts are to be reported.	DoD has defined the personnel or roles as at a minimum, the ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO.	MOD			X		X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(12)(b)	CCI-002149	The organization reports atypical usage of information system accounts to organization-defined personnel or roles.	The organization being inspected/assessed documents and implements a process to report atypical usage defined in AC-2 (12), CCI 2146 of information system accounts to at a minium, the ISSO. The organization must maintain an audit trail of reporting. DoD has defined the personnel or roles as at a minium, the ISSO.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reporting to ensure the organization being inspected/assessed reports atypical usage defined in AC-2 (12), CCI 2146 of information system accounts to at a minimum, the ISSO. DoD has defined the personnel or roles as at a minimum, the ISSO.	MOD			X		X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-2(13)	CCI-002150	The organization defines the time period within which the accounts of users posing a significant risk are to be disabled after discovery of the risk.	DoD has defined the time period as 30 minutes unless otherwise defined in formal organizational policy.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 30 minutes unless otherwise defined in formal organizational policy.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AC-2(13)	CCI-002151	The organization disables accounts of users posing a significant risk within organization-defined time period of discovery of the risk.	The organization being inspected/assessed documents and implements a process to disable accounts of users posing a significant risk within 30 minutes unless otherwise defined in formal organizational policy. DoD has defined the time period as 30 minutes unless otherwise defined in formal organizational policy.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed disables accounts of users posing a significant risk within 30 minutes unless otherwise defined in formal organizational policy. DoD has defined the time period as 30 minutes unless otherwise defined in formal organizational policy.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-3(4)	CCI-002163	The organization defines the discretionary access control policies the information system is to enforce over subjects and objects.	The organization being inspected/assessed defines and documents the discretionary access control policies the information system is to enforce over subjects and objects. DoD has determined that the discretionary access control policies are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented access control policies to ensure they have been defined. DoD has determined that the discretionary access control policies are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-3(4)	CCI-002164	The organization specifies in the discretionary access control policies that a subject which has been granted access to information can do one or more of the following: pass the information to any other subjects or objects; grant its privileges to other subjects; change security attributes on subjects, objects, the information system, or the information system's components; choose the security attributes to be associated with newly created or revised objects; and/or change the rules governing access control.	The organization being inspected/assessed documents the discretionary access control policies that a subject which has been granted access to information can do one or more of the following: pass the information to any other subjects or objects; grant its privileges to other subjects; change security attributes on subjects, objects, the information system, or the information system's components; choose the security attributes to be associated with newly created or revised objects; and/or change the rules governing access control.	The organization conducting the inspection/assessment obtains and examines the documented discretionary access control policies to ensure the organization being inspected/assessed specifies that a subject which has been granted access to information can do one or more of the following: pass the information to any other subjects or objects; grant its privileges to other subjects; change security attributes on subjects, objects, the information system, or the information system's components; choose the security attributes to be associated with newly created or revised objects; and/or change the rules governing access control.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-3(4)	CCI-002165	The information system enforces organization-defined discretionary access control policies over defined subjects and objects.	The organization being inspected/assessed configures the information system to enforce the discretionary access control policies defined in AC-3 (4), CCI 2163 over defined subjects and objects. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2165.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enforce the discretionary access control policies defined in AC-3 (4), CCI 2163 over defined subjects and objects. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2165.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-5(a)	CCI-002219	The organization defines the duties of individuals that are to be separated.	The organization being inspected/assessed defines and documents the duties of individuals that are to be separated. DoD has determined the duties are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented duties to ensure the organization being inspected/assessed defines the duties of individuals that are to be separated. DoD has determined the duties are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-5(c)	CCI-002220	The organization defines information system access authorizations to support separation of duties.	The organization being inspected/assessed defines and documents the information system access authorizations to support separation of duties.	The organization conducting the inspection/assessment obtains and examines the documented information system access authorizations to ensure the organization being inspected/assessed defines information system access authorizations to support separation of duties.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-6(1)	CCI-002221	The organization defines the security-relevant information for which access must be explicitly authorized.	DoD has defined the security-relevant information as all security-relevant information not publicly available.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security-relevant information as all security-relevant information not publicly available.	MOD		X		X	X			3.3.1 User Accounts 3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI requirements are addressed within subparagraph "User Accounts" "USER IDENTIFICATION AND AUTHENTICATION" of UFGS 25 05 11.
N/A	AC-6(1)	CCI-002222	The organization explicitly authorizes access to organization-defined security functions.	The organization being inspected/assessed documents and implements a process to explicitly authorize access to all functions not publicly accessible. Explicit authorization can be in the form of an acceptable use policy signed by the user at the time of access being granted. DoD has defined the security functions as all functions not publicly accessible.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed explicitly authorizes access to all functions not publicly accessible. DoD has defined the security functions as all functions not publicly accessible.	MOD		X		X	X			3.3.1 User Accounts 3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI requirements are addressed within subparagraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION" of UFGS 25 05 11.
N/A	AC-6(1)	CCI-002223	The organization explicitly authorizes access to organization-defined security-relevant information.	The organization being inspected/assessed documents and implements a process to explicitly authorize access to all security-relevant information not publicly available. Explicit authorization can be in the form of an acceptable use policy signed by the user at the time of access being granted. DoD has defined the security-relevant information as all security-relevant information not publicly available.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed explicitly authorizes access to all security-relevant information not publicly available. DoD has defined the security-relevant information as all security-relevant information not publicly available.	MOD		X		X	X			3.3.1 User Accounts 3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI requirements are addressed within subparagraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION" of UFGS 25 05 11.
N/A	AC-6(5)	CCI-002226	The organization defines the personnel or roles to whom privileged accounts are to be restricted on the information system.	The organization being inspected/assessed defines and documents the personnel or roles to whom privileged accounts are to be restricted on the information system. DoD has determined the personnel and roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles to whom privileged accounts are to be restricted on the information system. DoD has determined the personnel and roles are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-6(5)	CCI-002227	The organization restricts privileged accounts on the information system to organization-defined personnel or roles.	The organization being inspected/assessed implements a process to only provide privileged accounts on the information system to personnel or roles defined in AC-6 (5), CCI 2226.	The organization conducting the inspection/assessment obtains and examines a sampling of information system access authorizations to ensure the organization being inspected/assessed implements a process to only provide privileged accounts on the information system to personnel or roles defined in AC-6 (5), CCI 2226.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-6(7)(a)	CCI-002228	The organization defines the frequency on which it conducts reviews of the privileges assigned to organization-defined roles or classes of users.	DoD has defined the frequency as at a minimum, annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at a minimum, annually.	MOD			X		X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-6(7)(a)	CCI-002229	The organization defines the roles or classes of users that are to have their privileges reviewed on an organization-defined frequency.	DoD has defined the roles or classes of users as all users.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles or classes of users as all users.	MOD			X		X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H.3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-6(7)(a)	CCI-002230	The organization reviews the privileges assigned to organization-defined roles or classes of users on an organization-defined frequency to validate the need for such privileges.	The organization being inspected/assessed documents and implements a process to review the privileges assigned to all users at a minimum, annually to validate the need for such privileges. The organization must maintain an audit trail of reviews. DoD has defined the roles or classes of users as all users. DoD has defined the frequency as at a minimum, annually.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reviews to ensure the organization being inspected/assessed reviews the privileges assigned to all users at a minimum, annually. to validate the need for such privileges. DoD has defined the roles or classes of users as all users. DoD has defined the frequency as at a minimum, annually.	MOD			X		X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AC-6(7)(b)	CCI-002231	The organization reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.	The organization being inspected/assessed documents and implements a process to reassign or remove privileges, if necessary, to correctly reflect organizational mission/business needs.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.	MOD	X		X						---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-6(8)	CCI-002232	The organization defines software that is restricted from executing at a higher privilege than users executing the software.	DoD has defined the software as any software except software explicitly documented.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the software as any software except software explicitly documented.	MOD			X		X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-6(8)	CCI-002233	The information system prevents organization-defined software from executing at higher privilege levels than users executing the software.	The organization being inspected/assessed configures the information system to any software except software explicitly documented from executing at higher privilege levels than users executing the software. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2233. DoD has defined the software as any software except software explicitly documented.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent any software except software explicitly documented from executing at higher privilege levels than users executing the software. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2233. DoD has defined the software as any software except software explicitly documented.	MOD			X		X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-6(9)	CCI-002234	The information system audits the execution of privileged functions.	The organization being inspected/assessed configures the information system to audit the execution of privileged functions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2234.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to audit the execution of privileged functions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2234.	MOD		X		X				3.3.1 User Accounts 3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI requirements are addressed within subparagraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION" of UFGS 25 05 11.
N/A	AC-6(10)	CCI-002235	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	The organization being inspected/assessed configures the information system to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2235.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2235.	MOD		X		X				3.3.1 User Accounts 3.4 USER IDENTIFICATION AND AUTHENTICAT...		CCI requirements are addressed within subparagraph "User Accounts" and "USER IDENTIFICATION AND AUTHENTICATION" of UFGS 25 05 11.
N/A	AC-7(b)	CCI-002236	The organization defines the time period the information system will automatically lock the account or node when the maximum number of unsuccessful attempts is exceeded.	DoD has defined the time period as until released by an administrator.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as until released by an administrator.	LOW		X		X	X			3.3.2 Unsuccessful Logon Attempts		Cybersecurity requirements are met for log in attempts within Sub-Paragraph "Unsuccessful Logon Attempts" within Part 3
N/A	AC-7(b)	CCI-002237	The organization defines the delay algorithm to be employed by the information system to delay the next login prompt when the maximum number of unsuccessful attempts is exceeded.	DoD has defined the delay algorithm as a minimum of 5 seconds.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the delay algorithm as a minimum of 5 seconds.	LOW		X		X	X			3.3.2 Unsuccessful Logon Attempts		Cybersecurity requirements are met for log in attempts within Sub-Paragraph "Unsuccessful Logon Attempts" within Part 3
N/A	AC-7(b)	CCI-002238	The information system automatically locks the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next login prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.	The organization being inspected/assessed configures the information system to automatically lock the account or node until the locked account is released by an administrator and delays the next login prompt for a minimum of 5 seconds when the maximum number of unsuccessful attempts is exceeded. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2238. DoD has defined the delay algorithm as a minimum of 5 seconds. DoD has defined the time period as until released by an administrator.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically lock the account or node until the locked account is released by an administrator and delays the next login prompt for a minimum of 5 seconds when the maximum number of unsuccessful attempts is exceeded. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2238. DoD has defined the delay algorithm as a minimum of 5 seconds. DoD has defined the time period as until released by an administrator.	LOW		X		X				3.3.2 Unsuccessful Logon Attempts		Cybersecurity requirements are met for log in attempts within Sub-Paragraph "Unsuccessful Logon Attempts" within Part 3

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-8(a)(1)	CCI-002243	The organization-defined information system use notification message or banner is to state that users are accessing a U.S. Government information system.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	LOW	X	X		X	X			3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-8(a)(2)	CCI-002244	The organization-defined information system use notification message or banner is to state that information system usage may be monitored, recorded, and subject to audit.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	LOW	X	X		X	X			3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-8(a)(3)	CCI-002245	The organization-defined information system use notification message or banner is to state that unauthorized use of the information system is prohibited and subject to criminal and civil penalties.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	LOW	X	X		X	X			3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-8(a)(4)	CCI-002246	The organization-defined information system use notification message or banner is to state that use of the information system indicates consent to monitoring and recording.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	LOW	X	X		X	X			3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-8(a)	CCI-002247	The organization defines the use notification message or banner the information system displays to users before granting access to the system.	DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	LOW	X	X		X	X			3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-8(c)(1)	CCI-002248	The organization defines the conditions of use which are to be displayed to users of the information system before granting further access.	DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	LOW	X	X		X	X			3.3.3 System Use Notification		Cybersecurity requirements are met for System Use Notifications within Sub-Paragraph "System Use Notification" within Part 3
N/A	AC-10	CCI-002252	The organization defines the accounts for which the information system will limit the number of concurrent sessions.	DoD has defined the account types and/or accounts as all account types and/or accounts.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the account types and/or accounts as all account types and/or accounts.	MOD		X	X		X			3.3.4 Session Lock and Session Terminatio...		CCI requirements are addressed within subparagraph "Session Lock and Session Termination Requirements In MODERATE Impact Systems:" of UFGS 25 05 11.
N/A	AC-16(a)	CCI-002256	The organization defines security attributes having organization-defined types of security attribute values which are associated with information in storage.	The organization being inspected/assessed defines and documents the security attributes having organization-defined types of security attribute values which are associated with information in storage. DoD has determined the security attributes are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization being inspected/assessed defines security attributes having organization-defined types of security attribute values which are associated with information in storage. DoD has determined the security attributes are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-16(a)	CCI-002257	The organization defines security attributes having organization-defined types of security attribute values which are associated with information in process.	The organization being inspected/assessed defines and documents the security attributes having organization-defined types of security attribute values which are associated with information in process. DoD has determined the security attributes are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization being inspected/assessed defines security attributes having organization-defined types of security attribute values process. DoD has determined the security attributes are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-16(a)	CCI-002258	The organization defines security attributes, having organization-defined types of security attribute values, which are associated with information in transmission.	The organization being inspected/assessed defines and documents the security attributes having organization-defined types of security attribute values which are associated with information in transmission. DoD has determined the security attributes are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization being inspected/assessed defines security attributes having organization-defined types of security attribute values which are associated with information in transmission. DoD has determined the security attributes are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-16(a)	CCI-002259	The organization defines security attribute values associated with organization-defined types of security attributes for information in storage.	The organization being inspected/assessed defines and documents the security attributes values associated with organization-defined types of security attributes for information in storage. DoD has determined the security attribute values are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security attribute values to ensure the organization being inspected/assessed defines security attribute values associated with organization-defined types of security attributes for information in storage. DoD has determined the security attribute values are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-16(a)	CCI-002260	The organization defines security attribute values associated with organization-defined types of security attributes for information in process.	The organization being inspected/assessed defines and documents the security attributes values associated with organization-defined types of security attributes for information in process. DoD has determined the security attribute values are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security attribute values to ensure the organization being inspected/assessed defines security attribute values associated with organization-defined types of security attributes for information in process. DoD has determined the security attribute values are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below Enclave	Enclave Designer	Non-Designer Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-16(a)	CCI-002261	The organization defines security attribute values associated with organization-defined types of security attributes for information in transmission.	The organization being inspected/assessed defines and documents the security attributes values associated with organization-defined types of security attributes for information in transmission. DoD has determined the security attribute values are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security attribute values to ensure the organization being inspected/assessed defines security attribute values associated with organization-defined types of security attributes for information in transmission. DoD has determined the security attribute values are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-16(a)	CCI-002262	The organization provides the means to associate organization-defined types of security attributes having organization-defined security attribute values with information in storage.	The organization being inspected/assessed configures the information system to provide the means to associate types of security attributes in defined in AC-16, CCI 2256 having security attribute values defined in AC-16, CCI 2259 with information in storage. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2262.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the means to associate types of security attributes in defined in AC-16, CCI 2256 having security attribute values defined in AC-16, CCI 2259 with information in storage. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2262.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-16(a)	CCI-002263	The organization provides the means to associate organization-defined types of security attributes having organization-defined security attribute values with information in process.	The organization being inspected/assessed configures the information system to provide the means to associate types of security attributes in defined in AC-16, CCI 2257 having security attribute values defined in AC-16, CCI 2260 with information in process. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2263.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the means to associate types of security attributes in defined in AC-16, CCI 2257 having security attribute values defined in AC-16, CCI 2260 with information in process. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2263.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-16(a)	CCI-002264	The organization provides the means to associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.	The organization being inspected/assessed configures the information system to provide the means to associate types of security attributes in defined in AC-16, CCI 2258 having security attribute values defined in AC-16, CCI 2261 with information in transmission. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2264.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the means to associate types of security attributes in defined in AC-16, CCI 2258 having security attribute values defined in AC-16, CCI 2261 with information in transmission. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2264.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-16(b)	CCI-002265	The organization ensures that the security attribute associations are made with the information.	The organization being inspected/assessed documents and implements a process to ensure that the security attribute associations are made with the information.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures that the security attribute associations are made with the information.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-16(b)	CCI-002266	The organization ensures that the security attribute associations are retained with the information.	The organization being inspected/assessed documents and implements a process to ensure that the security attribute associations are retained with the information.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures that the security attribute associations are retained with the information.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-16(c)	CCI-002267	The organization defines the security attributes that are permitted for organization-defined information systems.	DoD has defined the security attributes as the security attributes defined in AC-16, CCIs 2256-2258.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security attributes as the security attributes defined in AC-16, CCIs 2256-2258.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AC-16(c)	CCI-002268	The organization defines the information systems for which permitted organization-defined attributes are to be established.	DoD has defined the information systems as all information systems.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information systems as all information systems.	MOD			X		X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-16(c)	CCI-002269	The organization establishes the permitted organization-defined security attributes for organization-defined information systems.	The organization being inspected/assessed establishes and documents the permitted security attributes for all information systems as a subset of the security attributes defined in AC-16, CCI 2267. DoD has defined the information systems as all information systems.	The organization conducting the inspection/assessment obtains and examines the documented list of permitted security attributes to ensure the organization being inspected/assessed has established the list of permitted security attributes for all information systems as a subset of the security attributes defined in AC-16, CCI 2267. DoD has defined the information systems as all information systems.	MOD			X		X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-16(d)	CCI-002270	The organization defines the values or ranges permitted for each of the established security attributes.	DoD has defined the values or ranges as the values defined in AC-16, CCIs 2259-2261.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the values or ranges as the values defined in AC-16, CCIs 2259-2261.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	AC-16(d)	CCI-002271	The organization determines the permitted organization-defined values or ranges for each of the established security attributes.	The organization being inspected/assessed establishes and documents the permitted values or ranges for each of the established security attributes as a subset of the values or ranges defined in AC-16, CCI 2270.	The organization conducting the inspection/assessment obtains and examines the documented permitted values or ranges to ensure the organization being inspected/assessed has established the permitted values or ranges for each of the established security attributes as a subset of the values or ranges defined in AC-16, CCI 2270.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-16(6)	CCI-002291	The organization defines the security policies to be followed by personnel when associating organization-defined security attributes with organization-defined subjects and objects.	The organization being inspected/assessed defines and documents the security policies to be followed by personnel when associating organization-defined security attributes with organization-defined subjects and objects. DoD has determined the security policies are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security policies to ensure the organization being inspected/assessed defines the security policies to be followed by personnel when associating organization-defined security attributes with organization-defined subjects and objects. DoD has determined the security policies are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-16(6)	CCI-002292	The organization defines the security attributes which are to be associated with organization-defined subjects and objects.	The organization being inspected/assessed defines and documents the security attributes which are to be associated with organization-defined subjects and objects. DoD has determined the security attributes are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization being inspected/assessed defines the security attributes which are to be associated with organization-defined subjects and objects. DoD has determined the security attributes are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-16(6)	CCI-002293	The organization defines the subjects to be associated, and that association maintained, with organization-defined security attributes in accordance with organization-defined security policies.	The organization being inspected/assessed defines and documents the subjects to be associated, and that association maintained, with organization-defined security attributes in accordance with organization-defined security policies. DoD has determined the subjects are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented subjects to ensure the organization being inspected/assessed defines the subjects to be associated, and that association maintained, with organization-defined security attributes in accordance with organization-defined security policies. DoD has determined the subjects are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-16(6)	CCI-002294	The organization defines the objects to be associated, and that association maintained, with organization-defined security attributes in accordance with organization-defined security policies.	The organization being inspected/assessed defines and documents the objects to be associated, and that association maintained, with organization-defined security attributes in accordance with organization-defined security policies. DoD has determined the objects are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented objects to ensure the organization being inspected/assessed defines the objects to be associated, and that association maintained, with organization-defined security attributes in accordance with organization-defined security policies. DoD has determined the objects are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-16(6)	CCI-002295	The organization allows personnel to associate organization-defined security attributes with organization-defined subjects in accordance with organization-defined security policies.	The organization being inspected/assessed documents and implements a process requiring personnel to associate security attributes defined in AC-16 (6), CCI 2292 with subjects defined in AC-16 (6), CCI 2293 in accordance with security policies defined in AC-16 (6), CCI 2291.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires personnel to associate security attributes defined in AC-16 (6), CCI 2292 with subjects defined in AC-16 (6), CCI 2293 in accordance with security policies defined in AC-16 (6), CCI 2291.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-16(6)	CCI-002296	The organization allows personnel to associate organization-defined security attributes with organization-defined objects in accordance with organization-defined security policies.	The organization being inspected/assessed documents and implements a process requiring personnel to associate security attributes defined in AC-16 (6), CCI 2292 with objects defined in AC-16 (6), CCI 2294 in accordance with security policies defined in AC-16 (6), CCI 2291.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires personnel to associate security attributes defined in AC-16 (6), CCI 2292 with objects defined in AC-16 (6), CCI 2294 in accordance with security policies defined in AC-16 (6), CCI 2291.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-16(6)	CCI-002297	The organization allows personnel to maintain the association of organization-defined security attributes with organization-defined subjects in accordance with organization-defined security policies.	The organization being inspected/assessed documents and implements a process requiring personnel to maintain the association of security attributes defined in AC-16 (6), CCI 2292 with subjects defined in AC-16 (6), CCI 2293 in accordance with security policies defined in AC-16 (6), CCI 2291.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires personnel to maintain the association of security attributes defined in AC-16 (6), CCI 2292 with subjects defined in AC-16 (6), CCI 2293 in accordance with security policies defined in AC-16 (6), CCI 2291.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-16(6)	CCI-002298	The organization allows personnel to maintain the association of organization-defined security attributes with organization-defined objects in accordance with organization-defined security policies.	The organization being inspected/assessed documents and implements a process requiring personnel to maintain the association of security attributes defined in AC-16 (6), CCI 2292 with objects defined in AC-16 (6), CCI 2294 in accordance with security policies defined in AC-16 (6), CCI 2291.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires personnel to maintain the association of security attributes defined in AC-16 (6), CCI 2292 with objects defined in AC-16 (6), CCI 2294 in accordance with security policies defined in AC-16 (6), CCI 2291.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(a)	CCI-002310	The organization establishes and documents usage restrictions for each type of remote access allowed.	The organization being inspected/assessed establishes and documents usage restrictions for each type of remote access allowed.	The organization conducting the inspection/assessment obtains and examines the documented usage restrictions to ensure the organization being inspected/assessed establishes and documents usage restrictions for each type of remote access allowed.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(a)	CCI-002311	The organization establishes and documents configuration/connection requirements for each type of remote access allowed.	The organization being inspected/assessed establishes and documents configuration/connection requirements for each type of remote access allowed.	The organization conducting the inspection/assessment obtains and examines the documented requirements to ensure the organization being inspected/assessed establishes and documents configuration/connection requirements for each type of remote access allowed.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(a)	CCI-002312	The organization establishes and documents implementation guidance for each type of remote access allowed.	The organization being inspected/assessed establishes and documents implementation guidance for each type of remote access allowed.	The organization conducting the inspection/assessment obtains and examines the documented implementation guidance to ensure the organization being inspected/assessed establishes and documents implementation guidance for each type of remote access allowed.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-17(1)	CCI-002314	The information system controls remote access methods.	The organization being inspected/assessed configures the information system to control remote access methods. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2314.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to control remote access methods. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2314.	MOD	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(3)	CCI-002315	The organization defines the number of managed network access control points through which the information system routes all remote access.	The organization being inspected/assessed defines and documents the number of managed network access control points through which the information system routes all remote access. DoD has determined the number is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented number to ensure the organization being inspected/assessed defines the number of managed network access control points through which the information system routes all remote access. DoD has determined the number is not appropriate to define at the Enterprise level.	MOD	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(4)(a)	CCI-002316	The organization authorizes the access to security relevant information via remote access only for organization-defined needs.	The organization being inspected/assessed authorizes the access to security-relevant information via remote access only for needs defined in AC-17 (4), CCI 2318. The organization being inspected/assessed maintains an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes the access to security-relevant information via remote access only for needs defined in AC-17 (4), CCI 2318.	MOD	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-17(4)(a)	CCI-002317	The organization defines the operational needs when the execution of privileged commands via remote access is to be authorized.	The organization being inspected/assessed defines and documents the operational needs when the execution of privileged commands via remote access is to be authorized. DoD has determined the operational needs are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented operational needs to ensure the organization being inspected/assessed defines the operational needs when the execution of privileged commands via remote access is to be authorized. DoD has determined the operational needs are not appropriate to define at the Enterprise level.	MOD	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(4)(a)	CCI-002318	The organization defines the operational needs when access to security-relevant information via remote access is to be authorized.	The organization being inspected/assessed defines and documents the operational needs when access to security-relevant information via remote access is to be authorized. DoD has determined the operational needs are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented operational needs to ensure the organization being inspected/assessed defines the operational needs when access to security-relevant information via remote access is to be authorized. DoD has determined the operational needs are not appropriate to define at the Enterprise level.	MOD	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(4)(b)	CCI-002319	The organization documents in the security plan for the information system the rationale for authorization of the execution of privilege commands via remote access.	The organization being inspected/assessed documents in the security plan for the information system the rationale for authorization of the execution of privilege commands via remote access.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed documents in the security plan for the information system the rationale for authorization of the execution of privilege commands via remote access.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-17(4)(b)	CCI-002320	The organization documents in the security plan for the information system the rationale for authorization of access to security-relevant information via remote access.	The organization being inspected/assessed documents in the security plan for the information system the rationale for authorization of access to security-relevant information via remote access.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed documents in the security plan for the information system the rationale for authorization of access to security-relevant information via remote access.	MOD	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(9)	CCI-002321	The organization defines the time period within which it disconnects or disables remote access to the information system.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.	MOD	X		X		X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-17(9)	CCI-002322	The organization provides the capability to expeditiously disconnect or disable remote access to the information system within the organization-defined time period.	The organization being inspected/assessed configures the information system to provide the capability to expeditiously disconnect or disable remote access to the information system immediately. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2322. DoD has defined the time period as immediately.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability to expeditiously disconnect or disable remote access to the information system immediately. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2322. DoD has defined the time period as immediately.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-18(a)	CCI-002323	The organization establishes configuration/connection requirements for wireless access.	The organization being inspected/assessed establishes and documents configuration/connection requirements for wireless access.	The organization conducting the inspection/assessment obtains and examines the documented configuration/connection requirements to ensure the organization being inspected/assessed establishes configuration/connection requirements for wireless access.	LOW		X	X					3.2.3 Wireless and Wired Broadcast Commun…	Specification is for Fire Protection systems only, therefore this CCI is not included	
N/A	AC-18(4)	CCI-002324	The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.	The organization being inspected/assessed identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities. The organization must maintain an audit trail of authorizations.	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.	MOD			X					---	While control systems may have outbound email for alarm, event and audit reporting, control systems don't use inbound email.	
N/A	AC-19(a)	CCI-002325	The organization establishes configuration requirements for organization controlled mobile devices.	DoD is automatically compliant with this CCI because existing STIGs establish configuration requirements for approved mobile devices.	DoD is automatically compliant with this CCI because existing STIGs establish configuration requirements for approved mobile devices.	LOW	X				X			---	While control systems may have outbound email for alarm, event and audit reporting, control systems don't use inbound email.	
N/A	AC-19(a)	CCI-002326	The organization establishes connection requirements for organization controlled mobile devices.	The organization being inspected/assessed establishes and documents connection requirements for organization controlled mobile devices.	The organization conducting the inspection/assessment obtains and examines the documented connection requirements to ensure the organization being inspected/assessed establishes connection requirements for organization controlled mobile devices.	LOW	X		X					---	While control systems may have outbound email for alarm, event and audit reporting, control systems don't use inbound email.	
N/A	AC-19(5)	CCI-002329	The organization defines the mobile devices that are to employ full-device or container encryption to protect the confidentiality and integrity of the information on device.	The organization being inspected/assessed defines and documents the mobile devices that are to employ full-device or container encryption to protect the confidentiality and integrity of the information on device. DoD has determined the mobile devices are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented mobile devices to ensure the organization being inspected/assessed defines the mobile devices that are to employ full-device or container encryption to protect the confidentiality and integrity of the information on device. DoD has determined the mobile devices are not appropriate to define at the Enterprise level.	MOD	X		X					---	While control systems may have outbound email for alarm, event and audit reporting, control systems don't use inbound email.	
N/A	AC-19(5)	CCI-002330	The organization employs full-device encryption or container encryption to protect the confidentiality of information on organization-defined mobile devices.	The organization being inspected/assessed documents and implements a process for full-device encryption or container encryption to protect the confidentiality of information on mobile devices defined in AC-19 (5), CCI 2329.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs full-device encryption or container encryption to protect the confidentiality of information on mobile devices defined in AC-19 (5), CCI 2329.	MOD	X		X					---	While control systems may have outbound email for alarm, event and audit reporting, control systems don't use inbound email.	
N/A	AC-19(5)	CCI-002331	The organization employs full-device encryption or container encryption to protect the integrity of information on organization-defined mobile devices.	The organization being inspected/assessed documents and implements a process for full-device encryption or container encryption to protect the integrity of information on mobile devices defined in AC-19 (5), CCI 2329.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed employs full-device encryption or container encryption to protect the integrity of information on mobile devices defined in AC-19 (5), CCI 2329.	MOD				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	AC-10(b)	CCI-002332	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store or transmit organization-controlled information using the external information systems.	The organization being inspected/assessed establishes and documents the terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store or transmit organization-controlled information using the external information systems.	The organization conducting the inspection/assessment obtains and examines the documented terms and conditions to ensure the organization being inspected/assessed establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store or transmit organization-controlled information using the external information systems.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	AC-20(1)(a)	CCI-002333	The organization permits authorized individuals to use an external information system to access the information system only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.	The organization being inspected/assessed documents and implements a process to permit authorized individuals to use an external information system to access the information system only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed permits authorized individuals to use an external information system to access the information system only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-20(1)(a)	CCI-002334	The organization permits authorized individuals to use an external information system to process organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.	The organization being inspected/assessed documents and implements a process to permit authorized individuals to use an external information system to process organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed permits authorized individuals to use an external information system to process organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-20(1)(a)	CCI-002335	The organization permits authorized individuals to use an external information system to store organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.	The organization being inspected/assessed documents and implements a process to permit authorized individuals to use an external information system to store organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed permits authorized individuals to use an external information system to store organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.	MOD	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-20(1)(a)	CCI-002336	The organization permits authorized individuals to use an external information system to transmit organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.	The organization being inspected/assessed documents and implements a process to permit authorized individuals to use an external information system to transmit organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed permits authorized individuals to use an external information system to transmit organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.	MOD	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	AC-20(1)(b)	CCI-002337	The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization retains approved information system connection or processing agreements with the organizational entity hosting the external information system.	The organization being inspected/assessed documents and implements a process to permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization retains approved information system connection or processing agreements with the organizational entity hosting the external information system.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization retains approved information system connection or processing agreements with the organizational entity hosting the external information system.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-20(3)	CCI-002338	The organization restricts or prohibits the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.	The organization being inspected/assessed documents and implements a process to restrict or prohibit the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed restricts or prohibits the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	AC-12	CCI-002360	The organization defines the conditions or trigger events requiring session disconnect to be employed by the information system when automatically terminating a user session.	The organization being inspected/assessed defines and documents the conditions or trigger events requiring session disconnect to be employed by the information system when automatically terminating a user session. DoD has determined the conditions or trigger events are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented conditions or trigger events to ensure the organization being inspected/assessed defines the conditions or trigger events requiring session disconnect to be employed by the information system when automatically terminating a user session. DoD has determined the conditions or trigger events are not appropriate to define at the Enterprise level.	MOD	X	X		X				3.3.4 Session Lock and Session Terminatio…		CCI requirements are addressed within subparagraph "Session Lock and Session Termination Requirements In MODERATE Impact Systems:" of UFGS 25 05 11.
N/A	AC-12	CCI-002361	The information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect.	The organization being inspected/assessed configures the information system to automatically terminate a user session after conditions or trigger events requiring session disconnect, as defined in AC-12, CCI 2360. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2361.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to automatically terminate a user session after conditions or trigger events requiring session disconnect, as defined in AC-12, CCI 2360. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2361.	MOD	X	X		X				3.3.4 Session Lock and Session Terminatio…		CCI requirements are addressed within subparagraph "Session Lock and Session Termination Requirements In MODERATE Impact Systems:" of UFGS 25 05 11.
N/A	IA-5(i)	CCI-002365	The organization manages information system authenticators by requiring individuals to take specific security safeguards to protect authenticators.	The organization being inspected/assessed documents within user agreements that individuals shall safeguard authenticators.	The organization conducting the inspection/assessment obtains and examines the user agreements of the organization being inspected/assessed to ensure that there are requirements for individuals to safeguard authenticators.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IA-5(i)	CCI-002366	The organization manages information system authenticators by having devices implement specific security safeguards to protect authenticators.	The organization being inspected/assessed configures the information system to manage information system authenticators by having devices implement, specific security safeguards to protect authenticators. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2366.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to manage information system authenticators by having devices implement, specific security safeguards to protect authenticators. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2366.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-1(a)	CCI-002368	The organization defines the personnel or roles to whom the risk assessment policy is disseminated.	DoD has defined the roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-1(a)	CCI-002369	The organization defines the personnel or roles to whom the risk assessment procedures are disseminated.	DoD has defined the roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	RA-3(d)	CCI-002370	The organization disseminates risk assessment results to organization-defined personnel or roles.	The organization being inspected/assessed documents and implements a process to disseminates risk assessment results to the ISSM, ISSO, AO, and PM. DoD has defined the personnel or roles as the ISSM, ISSO, AO, and PM.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed disseminates the risk assessment results to the ISSM, ISSO, AO, and PM. DoD has defined the personnel or roles as the ISSM, ISSO, AO, and PM.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	RA-3(d)	CCI-002371	The organization defines the personnel or roles whom the risk assessment results will be disseminated.	DoD has defined the personnel or roles as the ISSM, ISSO, AO, and PM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSM, ISSO, AO, and PM.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-5(e)	CCI-002376	The organization defines the personnel or roles whom the information obtained from the vulnerability scanning process and security control assessments will be shared.	DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(a)	CCI-002378	The organization defines the personnel or roles to be recipients of the system and communications protection policy.	The organization being inspected/assessed defines and documents personnel or roles to be recipients of the system and communications protection policy. The personnel or roles must include at a minimum, the ISSM/ISSO. DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles to be recipients of the system and communications protection policy. The personnel or roles must include at a minimum, the ISSM/ISSO. DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-1(a)	CCI-002380	The organization defines the personnel or roles to be recipients of the procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	The organization being inspected/assessed defines and documents personnel or roles to be recipients of the procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. The personnel or roles must include at a minimum, the ISSM/ISSO. DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles to be recipients of the procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. The personnel or roles must include at a minimum, the ISSM/ISSO. DoD has defined the personnel or roles as at a minimum, the ISSO/ISSM.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-5	CCI-002385	The information system protects against or limits the effects of organization-defined types of denial of service attacks by employing organization-defined security safeguards.	The organization being inspected/assessed configures the information system to protect against or limits the effects of types of denial of service attacks defined in SC-5, CCI 1093 by employing security safeguards defined in SC-5, CCI 2386. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2385.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect against or limits the effects of types of denial of service attacks defined in SC-5, CCI 1093 by employing security safeguards defined in SC-5, CCI 2386. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2385.	LOW	X	X						3.7.2 Denial of Service Protection<TAI OP...		CCI requirements are addressed within subparagraph "Denial of Service Protection" of UFGS 25 05 11.
N/A	SC-5	CCI-002386	The organization defines the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks.	The organization being inspected/assessed defines and documents the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	LOW	X	X	X					3.7.2 Denial of Service Protection<TAI OP...		CCI requirements are addressed within subparagraph "Denial of Service Protection" of UFGS 25 05 11.
N/A	SC-5(1)	CCI-002387	The organization defines the denial of service attacks against other information systems the information system is to restrict the ability of individuals to launch.	The organization being inspected/assessed defines and documents the denial of service attacks against other information systems the information system is to restrict the ability of individuals to launch. DoD has determined the denial of service attacks as not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented denial of service attacks to ensure the organization being inspected/assessed defines the denial of service attacks against other information systems the information system is to restrict the ability of individuals to launch. DoD has determined the denial of service attacks as not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-5(3)(a)	CCI-002388	The organization defines a list of monitoring tools to be employed to detect indicators of denial of service attacks against the information system.	The organization being inspected/assessed defines and documents a list of monitoring tools to be employed to detect indicators of denial of service attacks against the information system. DoD has determined the monitoring tools are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented monitoring tools to ensure the organization being inspected/assessed defines a list of monitoring tools to be employed to detect indicators of denial of service attacks against the information system. DoD has determined the monitoring tools are not appropriate to define at the Enterprise level.	MOD		X	X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-5(3)(a)	CCI-002389	The organization employs organization-defined list of monitoring tools to detect indicators of denial of service attacks against the information system.	The organization being inspected/assessed implements the monitoring tools defined in SC-5 (3), CCI 2388 to detect indicators of denial of service attacks against the information system.	The organization conducting the inspection/assessment obtains and examines the list of monitoring tools as defined in SC-5 (3), CCI 2388 and a sampling of monitoring results to ensure the organization being inspected/assessed employs organization-defined list of monitoring tools to detect indicators of denial of service attacks against the information system.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-5(3)(b)	CCI-002390	The organization defines the information system resources to be monitored to determine if sufficient resources exist to prevent effective denial of service attacks.	The organization being inspected/assessed defines and documents the information system resources to be monitored to determine if sufficient resources exist to prevent effective denial of service attacks. DoD has determined the information system resources are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system resources to ensure the organization being inspected/assessed defines the information system resources to be monitored to determine if sufficient resources exist to prevent effective denial of service attacks. DoD has determined the information system resources are not appropriate to define at the Enterprise level.	MOD		X	X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-5(3)(b)	CCI-002391	The organization monitors organization-defined information system resources to determine if sufficient resources exist to prevent effective denial of service attacks.	The organization being inspected/assessed monitors information system resources defined in SC-5 (3), CCI 2390 to determine if sufficient resources exist to prevent effective denial of service attacks.	The organization conducting the inspection/assessment obtains and examines the documented monitoring procedures and any available artifacts from the monitoring process to ensure the organization being inspected/assessed monitors information system resources defined in SC-5 (3), CCI 2390 to determine if sufficient resources exist to prevent effective denial of service attacks.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-7(b)	CCI-002395	The information system implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks.	The organization being inspected/assessed designs the information system to leverage subnetworks so that publicly accessible system components are physically and/or logically separated from internal organizational networks.	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component partitioning to ensure the organization being inspected/assessed implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks.	LOW								---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-7(4)(c)	CCI-002396	The organization protects the confidentiality and integrity of the information being transmitted across each interface for each external telecommunication service.	The organization being inspected/assessed documents and implements mechanisms to protect the confidentiality and integrity of the information being transmitted across each interface for each external telecommunication service.	The organization conducting the inspection/assessment obtains and examines the documented mechanisms to ensure the organization being inspected/assessed protects the confidentiality and integrity of the information being transmitted across each interface for each external telecommunication service.	MOD	X							3.7.5 Process Isolation and Boundary Prot...		CCI requirements are addressed within subparagraph "Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems" of UFGS 25 05 11.
N/A	SC-7(7)	CCI-002397	The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.	The organization being inspected/assessed configures the information system to prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2397.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2397.	MOD	X							3.7.5 Process Isolation and Boundary Prot...		CCI requirements are addressed within subparagraph "Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems" of UFGS 25 05 11.
N/A	SC-7(9)(a)	CCI-002398	The information system detects outgoing communications traffic posing a threat to external information systems.	The organization being inspected/assessed configures the information system to detect outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2398.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to detect outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2398.	MOD	X	X	X					1.9.2 Cybersecurity Interconnection Sched... 3.7.5 Process Isolation and Boundary Prot...		CCI requirements are addressed within subparagraph "Cybersecurity Interconnection Schedule" and "Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems" of UFGS 25 05 11.
N/A	SC-7(9)(a)	CCI-002399	The information system denies outgoing communications traffic posing a threat to external information systems.	The organization being inspected/assessed configures the information system to deny outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2399.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to deny outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2399.	MOD	X	X	X					1.9.2 Cybersecurity Interconnection Sched... 3.7.5 Process Isolation and Boundary Prot...		CCI requirements are addressed within subparagraph "Cybersecurity Interconnection Schedule" and "Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems" of UFGS 25 05 11.
N/A	SC-7(9)(b)	CCI-002400	The information system audits the identity of internal users associated with denied outgoing communications traffic posing a threat to external information systems.	The organization being inspected/assessed configures the information system to audit the identity of internal users associated with denied outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2400.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to audit the identity of internal users associated with denied outgoing communications traffic posing a threat to external information systems. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2400.	MOD		X		X				3.5.1 Audit Events, Content of Audit Reco...		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	SC-7(11)	CCI-002401	The organization defines the authorized sources from which the information system will allow incoming communications.	The organization being inspected/assessed defines and documents the authorized sources from which the information system will allow incoming communications. DoD has determined the authorized sources are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented authorized sources to ensure the organization being inspected/assessed defines the authorized sources from which the information system will allow incoming communications. DoD has determined the authorized sources are not appropriate to define at the Enterprise level.	MOD	X	X	X					1.9.2 Cybersecurity Interconnection Sched...		Default Requirement in UFGS 25 05 11 listed in "Cybersecurity Interconnection Schedule"
N/A	SC-7(11)	CCI-002402	The organization defines the authorized destinations for routing inbound communications.	The organization being inspected/assessed defines and documents the authorized destinations for routing inbound communications. DoD has determined the authorized destinations are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented authorized destinations to ensure the organization being inspected/assessed defines the authorized destinations for routing inbound communications. DoD has determined the authorized destinations are not appropriate to define at the Enterprise level.	MOD	X	X	X					1.9.2 Cybersecurity Interconnection Sched...		Default Requirement in UFGS 25 05 11 listed in "Cybersecurity Interconnection Schedule"
N/A	SC-7(11)	CCI-002403	The information system only allows incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.	The organization being inspected/assessed configures the information system to allow incoming communications from authorized sources defined in SC-7 (11), CCI 2401 routed to authorized destinations defined in SC-7 (11), CCI 2402. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2403.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to allow incoming communications from authorized sources defined in SC-7 (11), CCI 2401 routed to authorized destinations defined in SC-7 (11), CCI 2402. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2403.	MOD	X	X	X					1.9.2 Cybersecurity Interconnection Sched... 3.7.5 Process Isolation and Boundary Prot...		CCI requirements are addressed within subparagraph "Cybersecurity Interconnection Schedule" and "Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems" of UFGS 25 05 11.
N/A	SC-7(12)	CCI-002404	The organization defines the host-based boundary protection mechanisms that are to be implemented at organization-defined information system components.	DoD has defined the information system components as McAfee Host Intrusion Prevention (HIPS).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system components as McAfee Host Intrusion Prevention (HIPS).	MOD	X	X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-7(12)	CCI-002405	The organization defines the information system components at which organization-defined host-based boundary protection mechanisms will be implemented.	DoD has defined the information system components as all information system components.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system components as all information system components.	MOD	X	X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-7(12)	CCI-002406	The organization implements organization-defined host-based boundary protection mechanisms at organization-defined information system components.	The organization being inspected/assessed implements McAfee Host Intrusion Prevention (HIPS) on all information system components. DoD has defined the host-based boundary protection mechanisms as McAfee Host Intrusion Prevention (HIPS). DoD has defined the information system components as all information system components.	The organization conducting the inspection/assessment examines a sampling of information system components to ensure the organization being inspected/assessed implements McAfee Host Intrusion Prevention (HIPS) on all information system components. DoD has defined the host-based boundary protection mechanisms as McAfee Host Intrusion Prevention (HIPS). DoD has defined the information system components as all information system components.	MOD	X	X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-7(14)	CCI-002407	The organization defines the managed interfaces at which the organization protects against unauthorized physical connections.	DoD has defined the managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the managed interfaces as internet access points, enclave LAN to WAN, cross domain solutions, and any DoD Approved Alternate Gateways.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-8	CCI-002418	The information system protects the confidentiality and/or integrity of transmitted information.	The organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of transmitted information. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2418.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of transmitted information. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2418.	MOD		X						3.2.6 Cryptographic Protection 3.3.6 Pysical Security in MODERATE Impact...		CCI requirements are addressed within subparagraph "Physical Security in MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-8(1)	CCI-002419	The organization defines the alternative physical safeguards to be employed when cryptographic mechanisms are not implemented to protect information during transmission.	DoD has defined the alternative physical safeguards as Protected Distribution System (PDS).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the alternative physical safeguards as Protected Distribution System (PDS).	MOD		X			X			3.3.6 Pysical Security in MODERATE Impact...		CCI requirements are addressed within subparagraph "Physical Security in MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-8(2)	CCI-002420	The information system maintains the confidentiality and/or integrity of information during preparation for transmission.	The organization being inspected/assessed configures the information system to maintain the confidentiality and integrity of information during preparation for transmission. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2420. DoD has defined the selection as both confidentiality and integrity.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to maintain the confidentiality and integrity of information during preparation for transmission. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2420.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-8(1)	CCI-002421	The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by organization-defined alternative physical safeguards.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by Protected Distribution System (PDS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2421. DoD has defined the selection as both prevention of unauthorized disclosure and detection of changes to information. DoD has defined the alternative physical safeguards as Protected Distribution System (PDS).	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by Protected Distribution System (PDS). For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2421. DoD has defined the alternative physical safeguards as Protected Distribution System (PDS).	MOD		X						3.3.6 Pysical Security in MODERATE Impact...		CCI requirements are addressed within subparagraph "Physical Security in MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-8(2)	CCI-002422	The information system maintains the confidentiality and/or integrity of information during reception.	The organization being inspected/assessed configures the information system to maintain the confidentiality and integrity of information during reception. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2422. DoD has defined the selection as both confidentiality and integrity.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to maintain the confidentiality and integrity of information during reception. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2422.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002428	The organization defines the requirements for cryptographic key generation to be employed within the information system.	DoD has defined the requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW	X			X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002429	The organization defines the requirements for cryptographic key distribution to be employed within the information system.	DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW	X			X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-12	CCI-002430	The organization defines the requirements for cryptographic key storage to be employed within the information system.	DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW	X			X	X			3.7.2 Denial of Service Protection<TAI OP...		CCI requirements are addressed within subparagraph "Denial of Service Protection" of UFGS 25 05 11.
N/A	SC-12	CCI-002431	The organization defines the requirements for cryptographic key access to be employed within the information system.	DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW	X			X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002432	The organization defines the requirements for cryptographic key destruction to be employed within the information system.	DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW	X			X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002433	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key generation.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key generation as requirements for key generation defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002434	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key distribution.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002435	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key storage.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002436	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key access.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002437	The organization establishes cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key destruction.	The organization being inspected/assessed documents and implements a process to establish cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed establishes cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-12	CCI-002438	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key generation.	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key generation as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key generation as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002439	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key distribution.	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key distribution as requirements for key distribution defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002440	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key storage.	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key storage as requirements for key storage defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002441	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key access.	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key access as requirements for key access defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-12	CCI-002442	The organization manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key destruction.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	The organization being inspected/assessed documents and implements a process to manage cryptographic keys for required cryptography employed within the information system in accordance with requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." DoD has defined the requirements for key destruction as requirements for key destruction defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems."	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-13	CCI-002449	The organization defines the cryptographic uses, and type of cryptography required for each use, to be implemented by the information system.	DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography.	LOW	X	X		X	X	X	A LOW CS doesn't have any classified information	3.2.6 Cryptographic Protection	FRCS does not contain classified information	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-13	CCI-002450	The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	The organization being inspected/assessed configures the information system to implement, for, protection of classified information: NSA-approved cryptography; for provision of digital signatures and hashing: FIPS-validated cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2450. DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement, for, protection of classified information: NSA-approved cryptography; for provision of digital signatures and hashing: FIPS-validated cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2450. DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography.	LOW	X	X		X		X	A LOW CS doesn't have any classified information	3.2.6 Cryptographic Protection	FRCS does not contain classified information	
N/A	SC-17	CCI-002456	The organization defines the certificate policy employed to issue public key certificates.	DoD has defined the certificate policy as DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling."	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the certificate policy as DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-18(1)	CCI-002457	The organization defines the corrective actions to be taken when organization-defined unacceptable mobile code is identified.	DoD has defined the corrective actions to be taken when organization-defined unacceptable mobile code is identified as the corrective actions defined in the Protection Profile for Web Browsers and Application SRG.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the corrective actions to be taken when organization-defined unacceptable mobile code is identified as the corrective actions defined in the Protection Profile for Web Browsers and Application SRG.	MOD	X	X	X					3.7.3 Mobile Code In MODERATE Impact Syst…		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-18(1)	CCI-002458	The organization defines what constitutes unacceptable mobile code for its information systems.	The organization being inspected/assessed defines and documents unacceptable mobile code IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must define IAW the STIG/SRG guidance that pertains to CCI 2458. DoD has determined the unnacceptable mobile code is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessmenet obtains and examines the documented acceptable and unacceptable mobile code and mobile code technologies to ensure the organization being inspected/assessed defines unacceptable mobile code IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has defined unacceptable mobile code IAW the applicable STIGs and SRGs pertaining to CCI 2458. DoD has determined the unnacceptable mobile code is not appropriate to define at the Enterprise level.	MOD	X	X	X					3.7.3 Mobile Code In MODERATE Impact Syst…		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-18(3)	CCI-002459	The organization defines the unacceptable mobile code of which the information system is to prevent download and execution.	The organization being inspected/assessed defines and documents unacceptable mobile code of which the information system is to prevent download and execution IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must define IAW the STIG/SRG guidance that pertains to CCI 2459. DoD has determined the unnaceptable mobile code is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessmenet obtains and examines the documented unacceptable mobile code to ensure the organization being inspected/assessed defines unacceptable mobile code of which the information system is to prevent download and execution IAW the Protection Profile for Web Browsers and Application SRG. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has defined unacceptable mobile code IAW the applicable STIGs and SRGs pertaining to CCI 2459. DoD has determined the unnaceptable mobile code is not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-18(4)	CCI-002460	The information system enforces organization-defined actions prior to executing the code.	The organization being inspected/assessed configures the information system to prompt the user prior to executing the code. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2460. DoD has defined the actions as the user be prompted.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to prompt the user prior to executing the code. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2460. DoD has defined the actions as the user be prompted.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-20(a)	CCI-002462	The information system provides additional integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.	The organization being inspected/assessed configures the authoritative name server software for external queries to enable DNSSEC and creates resource records with digital signatures (RRSig) for each A record. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2462.	The organization conducting the inspection/assessment: 1. inspects the configuration files for the presence of DNSSEC records for each A record hosted in a zone; 2. utilizes DNSSEC diagnostic tools, such as dig; and 3. performs queries which will exercise the data flow path for authoritative name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2462.	LOW				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-21	CCI-002465	The information system requests data origin authentication verification on the name/address resolution responses the system receives from authoritative sources.	The organization being inspected/assessed configures the: 1. recursive/caching name server software to enable DNSSEC; 2. software to enable DNSSEC validation; and 3. software to establish a secure entry point trust anchor by installing key signing keys in the software configuration of trusted keys. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2465.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2465.	LOW	X			X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-21	CCI-002466	The information system requests data integrity verification on the name/address resolution responses the system receives from authoritative sources.	The organization being inspected/assessed configures the: 1. recursive/caching name server software to enable DNSSEC; 2. software to enable DNSSEC validation; and 3. software to establish a secure entry point trust anchor by installing key signing keys in the software configuration of trusted keys. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2466.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2466.	LOW	X			X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-21	CCI-002467	The information system performs data integrity verification on the name/address resolution responses the system receives from authoritative sources.	The organization being inspected/assessed configures the: 1. recursive/caching name server software to enable DNSSEC; 2. software to enable DNSSEC validation; and 3. software to establish a secure entry point trust anchor by installing key signing keys in the software configuration of trusted keys. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2467.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2467.	LOW	X			X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-21	CCI-002468	The information system performs data origin verification authentication on the name/address resolution responses the system receives from authoritative sources.	The organization being inspected/assessed configures the: 1. recursive/caching name server software to enable DNSSEC; 2. software to enable DNSSEC validation; and 3. software to establish a secure entry point trust anchor by installing key signing keys in the software configuration of trusted keys. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that determines the name server software configuration files and pertains to CCI 2468.	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the data flow path for recursive name resolution services. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs that determine the name server software configuration files and pertain to CCI 2468.	LOW	X			X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-23(5)	CCI-002469	The organization defines the certificate authorities the information system will allow to be used on the information system.	DoD has defined the certificate authorities as DoD PKI established certificate authorities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the certificate authorities as DoD PKI established certificate authorities.	MOD			X		X			3.7.3 Mobile Code In MODERATE Impact Syst...		CCI requirements are addressed within subparagraph "Mobile Code In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SC-23(5)	CCI-002470	The information system only allows the use of organization-defined certificate authorities for verification of the establishment of protected sessions.	The organization being inspected/assessed configures the information system to allow the use of DoD PKI established certificate authorities for verification of the establishment of protected sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2470. DoD has defined the certificate authorities as DoD PKI established certificate authorities.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to allow the use of DoD PKI established certificate authorities for verification of the establishment of protected sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2470. DoD has defined the certificate authorities as DoD PKI established certificate authorities.	MOD		X						3.2.7 Device Identification and Authentic...		CCI requirements are addressed within subparagraph "Device Identification and Authentication" of UFGS 25 05 11.
N/A	SC-28	CCI-002472	The organization defines the information at rest that is to be protected by the information system.	The organization being inspected/assessed defines and documents the information at rest that is to be protected by the information system which must include, at a minimum, PII and classified information. DoD has determined the information at rest is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information at rest to ensure the organization being inspected/assessed defines and documents the information at rest that is to be protected by the information system which must include, at a minimum, PII and classified information. DoD has determined the information at rest is not appropriate to define at the Enterprise level.	MOD		X	X	X				3.7.4 Protection of Information at Rest I...	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SC-28(1)	CCI-002473	The organization defines the information at rest for which cryptographic mechanisms will be implemented.	The organization being inspected/assessed defines and documents the information at rest that is to be protected by the information system which must include, at a minimum, PII and classified information. DoD has determined the information at rest is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information at rest to ensure the organization being inspected/assessed defines and documents the information at rest that is to be protected by the information system which must include, at a minimum, PII and classified information. DoD has determined the information at rest is not appropriate to define at the Enterprise level.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below Enclave	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SC-28(1)	CCI-002474	The organization defines the information system components which require the implementation of cryptographic mechanisms to prevent unauthorized disclosure and modification of organization-defined information at rest.	DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473.	MOD			X		X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SC-28(1)	CCI-002475	The information system implements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent unauthorized modification of information at rest defined in SC-28 (1), CCI 2473 on any information system components storing data defined in SC-28 (1), 2473. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2475. DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent unauthorized modification of information at rest defined in SC-28 (1), CCI 2473 on any information system components storing data defined in SC-28 (1), 2473. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2475. DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473.	MOD		X		X	X			3.7.4 Protection of Information at Rest I...	FRCS does not contain PII, CUI, or classified information	
N/A	SC-28(1)	CCI-002476	The information system implements cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent unauthorized disclosure of information at rest defined in SC-28 (1), CCI 2473 on any information system components storing data defined in SC-28 (1), 2473. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2476. DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent unauthorized disclosure of information at rest defined in SC-28 (1), CCI 2473 on any information system components storing data defined in SC-28 (1), 2473. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2476. DoD has defined the information system components as any information system components storing data defined in SC-28 (1), 2473.	MOD		X		X	X			3.7.4 Protection of Information at Rest I...	FRCS does not contain PII, CUI, or classified information	
N/A	SC-38	CCI-002528	The organization defines the operations security safeguards to be employed to protect key organizational information throughout the system development life cycle.	The organization being inspected/assessed defines and documents the operations security safeguards to be employed to protect key organizational information throughout the system development life cycle. DoD has determined the operations security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented operations security safeguards to ensure the organization being inspected/assessed defines the operations security safeguards to be employed to protect key organizational information throughout the system development life cycle. DoD has determined the operations security safeguards are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-38	CCI-002529	The organization employs organization-defined operations security safeguards to protect key organizational information throughout the system development life cycle.	The organization being inspected/assessed implements operations security safeguards defined in SC-38, CCI 2528 to protect key organizational information throughout the system development life cycle. The organization must maintain an audit trail of security safeguard implementation.	The organization conducting the inspection/assessment obtains and examines the audit trail of security safeguard implementation to ensure the organization being inspected/assessed employs operations security safeguards defined in SC-38, CCI 2528 to protect key organizational information throughout the system development life cycle.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SC-39	CCI-002530	The information system maintains a separate execution domain for each executing process.	The organization being inspected/assessed configures the information system to maintain a separate execution domain for each executing process. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2530.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to maintain a separate execution domain for each executing process. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2530.	LOW		X		X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SC-41	CCI-002544	The organization defines the information systems or information system components on which organization-defined connection ports or input/output devices are to be physically disabled or removed.	The organization being inspected/assessed defines and documents the information systems or information system components on which organization-defined connection ports or input/output devices are to be physically disabled or removed. DoD has determined the information systems or information system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information systems or information system components to ensure the organization being inspected/assessed defines the information systems or information system components on which organization-defined connection ports or input/output devices are to be physically disabled or removed. DoD has determined the information systems or information system components are not appropriate to define at the Enterprise level.	LOW	X	X	X					3.2.3 IP Control Networks 3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.
N/A	SC-41	CCI-002545	The organization defines the connection ports or input/output devices that are to be physically disabled or removed from organization-defined information systems or information system components.	The organization being inspected/assessed defines and documents the connection ports or input/output devices that are to be physically disabled or removed from organization-defined information systems or information system components. DoD has determined the connection ports or input/output devices are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented connection ports or input/output devices to ensure the organization being inspected/assessed defines the connection ports or input/output devices that are to be physically disabled or removed from organization-defined information systems or information system components. DoD has determined the connection ports or input/output devices are not appropriate to define at the Enterprise level.	LOW	X	X	X					3.2.3 IP Control Networks 3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.
N/A	SC-41	CCI-002546	The organization physically disables or removes organization-defined connection ports or input/output devices on organization-defined information systems or information system components.	The organization being inspected/assessed physically disables or removes connection ports or input/output devices defined in SC-41, CCI 2545 on information systems or information system components defined in SC-41, CCI 2544.	The organization conducting the inspection/assessment examines a sampling of devices to ensure the organization being inspected/assessed physically disables or removes connection ports or input/output devices defined in SC-41, CCI 2545 on information systems or information system components defined in SC-41, CCI 2544.	LOW		X		X				3.2.3 IP Control Networks 3.6 REQUIREMENTS FOR LEAST FUNCTIONALIT...		Cybersecurity design requires the contractor to configure and document that the control system only provides essential capabilities. This design requirement is captured in Sub-Paragraph "REQUIREMENTS FOR LEAST FUNCTIONALITY" and "IP Control Networks" within Part 3.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures		Applies at or Below Enclave	Enclave Designer	Non-Designer Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	MP-1(a)(1)	CCI-002566	The organization defines personnel or roles to whom a documented media protection policy and procedures will be disseminated.	DoD has defined the personnel or roles as all users.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all users.	LOW	X		X	X	X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-6(a)	CCI-002578	The organization defines information system media to sanitize prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies.	DoD has defined the information system media as all media.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system media as all media.	LOW	X				X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-6(a)	CCI-002579	The organization defines the sanitization techniques and procedures in accordance with applicable federal and organization standards and policies to be used to sanitize organization-defined information system media prior to disposal, release out of organizational control, or release for reuse.	DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88.	LOW	X				X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MP-6(b)	CCI-002580	The organization employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	The organization being inspected/assessed implements sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. The organization must maintain an audit trail of sanitization actions.	The organization conducting the inspection/assessment obtains and examines the audit trail of sanitization actions to ensure the organization being inspected/assessed implements sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MP-7	CCI-002581	The organization defines the types of information system media to restrict or prohibit on organization-defined information systems or system components using organization-defined security safeguards.	The organization being inspected/assessed defines and documents the types of information system media to restrict or prohibit on organization-defined information systems or system components using organization-defined security safeguards. DoD has determined the types of information system media are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented type of information system media to ensure the organization being inspected/assessed defines the types of information system media to restrict or prohibit on organization-defined information systems or system components using organization-defined security safeguards. DoD has determined the types of information system media are not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MP-7	CCI-002582	The organization defines the information systems or system components to restrict or prohibit the use of organization-defined types of information system media using organization-defined security safeguards.	The organization being inspected/assessed defines and documents the information systems or system components to restrict or prohibit the use of organization-defined types of information system media using organization-defined security safeguards. DoD has determined the information systems or system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information systems or system components to ensure the organization being inspected/assessed defines the information systems or system components to restrict or prohibit the use of organization-defined types of information system media using organization-defined security safeguards. DoD has determined the information systems or system components are not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MP-7	CCI-002583	The organization defines the security safeguards to use for restricting or prohibiting the use of organization-defined types of information system media on organization-defined information systems or system components.	The organization being inspected/assessed defines and documents the security safeguards to use for restricting or prohibiting the use of organization-defined types of information system media on organization-defined information systems or system components. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to use for restricting or prohibiting the use of organization-defined types of information system media on organization-defined information systems or system components. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MP-7	CCI-002584	The organization restricts or prohibits the use of organization-defined types of information system media on organization-defined information systems or system components using organization-defined security safeguards.	The organization being inspected/assessed documents and enforces controls for the use of media defined in MP-7, CCI 2581 on systems defined in MP-7, CCI 2582 using security safeguards defined in MP-7, CCI 2583.	The organization conducting the inspection/assessment obtains and examines the documented controls and examines information system procedures associated with the use of media to ensure the organization being inspected/assessed documents and enforces controls for the use of media defined in MP-7, CCI 2581 on systems defined in MP-7, CCI 2582 using security safeguards defined in MP-7, CCI 2583.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MP-7(1)	CCI-002585	The organization prohibits the use of portable storage devices in organization information systems when such devices have no identifiable owner.	The organization being inspected/assessed does not use portable storage devices in organization information systems when such devices have no identifiable owner.	The organization conducting the inspection/assessment examines a sampling of portable storage devices used in the information system to ensure that the devices have an identifiable owner.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-1(a)	CCI-002601	The organization defines the personnel or roles to whom the system and information integrity policy and procedures are to be disseminated.	DoD has defined the personnel or roles as all appointed information assurance personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all appointed information assurance personnel.	LOW					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-2(b)	CCI-002602	The organization tests firmware updates related to flaw remediation for effectiveness before installation.	The organization being inspected/assessed documents and implements a process to test firmware updates related to flaw remediation for effectiveness before installation. If the firmware update is being provided by a vendor who has documented the effectiveness of the update in fixing the affected IAVM/CVE, further testing by the organization may not be required.	The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests firmware updates related to flaw remediation for effectiveness before installation.	LOW	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-2(b)	CCI-002603	The organization tests firmware updates related to flaw remediation for potential side effects before installation.	The organization being inspected/assessed documents and implements a process for regression testing IAW CM-4 to identify any potential side effects before installation of software updates.	The organization conducting the inspection/assessment obtains and examines the documented process and test results to ensure the organization being inspected/assessed tests firmware updates related to flaw remediation for potential side effects before installation.	LOW	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-2(c)	CCI-002604	The organization defines the time period within the release of updates that security-related software updates are to be installed.	DoD has defined the time period as 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 30 days	LOW				X	X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-2(c)	CCI-002605	The organization installs security-relevant software updates within organization-defined time period of the release of the updates	The organization being inspected/assessed configures the information system to install security-relevant software updates within 30 days of the release of the updates For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2605. DoD has defined the time period as 30 days.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to install security-relevant software updates within 30 days of the release of the updates. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2605. DoD has defined the time period as 30 days.	LOW			X					1.10 SOFTWARE LICENSING		CCI requirements are addressed within subparagraph "Software Licensing" of UFGS 25 05 11.
N/A	SI-2(c)	CCI-002606	The organization defines the time period within the release of updates that security-related firmware updates are to be installed.	DoD has defined the time period as 30 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 30 days	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-2(c)	CCI-002607	The organization installs security-relevant firmware updates within organization-defined time period of the release of the updates	The organization being inspected/assessed configures the information system to install security-relevant firmware updates within 30 days of the release of the updates. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2607. DoD has defined the time period as 30 days.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to install security-relevant firmware updates within 30 days of the release of the updates. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2607. DoD has defined the time period as 30 days.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-2(6)	CCI-002615	The organization defines the software components to be removed (e.g., previous versions) after updated versions have been installed.	DoD has defined the software components as all upgraded/replaced software components that are no longer required for operation.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the software components as all upgraded/replaced software components that are no longer required for operation.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-2(6)	CCI-002616	The organization defines the firmware components to be removed (e.g., previous versions) after updated versions have been installed.	DoD has defined the firmware components as all upgraded/replaced firmware components that are no longer required for operation.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the firmware components as all upgraded/replaced firmware components that are no longer required for operation.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-2(6)	CCI-002617	The organization removes organization-defined software components (e.g., previous versions) after updated versions have been installed.	The organization being inspected/assessed configures the information system to remove all upgraded/replaced software components that are no longer required for operation (e.g., previous versions) after updated versions have been installed. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2617. DoD has defined the software components as all upgraded/replaced software components that are no longer required for operation.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to remove all upgraded/replaced software components that are no longer required for operation (e.g., previous versions) after updated versions have been installed. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2617. DoD has defined the software components as all upgraded/replaced software components that are no longer required for operation.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-2(6)	CCI-002618	The organization removes organization-defined firmware components (e.g., previous versions) after updated versions have been installed.	The organization being inspected/assessed configures the information system to remove all upgraded/replaced firmware components that are no longer required for operation e.g., previous versions) after updated versions have been installed. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2618. DoD has defined the firmware components as all upgraded/replaced firmware components that are no longer required for operation.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to remove all upgraded/replaced firmware components that are no longer required for operation (e.g., previous versions) after updated versions have been installed. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2618. DoD has defined the firmware components as all upgraded/replaced firmware components that are no longer required for operation.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-3(a)	CCI-002619	The organization employs malicious code protection mechanisms at information system entry points to detect malicious code.	The organization being inspected/assessed identifies and documents the information system entry points and implements malicious code protection mechanisms at those entry points to detect malicious code. Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies.	The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system entry points and verifies that malicious code protection mechanisms are implemented.	LOW	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-3(a)	CCI-002620	The organization employs malicious code protection mechanisms at information system exit points to detect malicious code.	The organization being inspected/assessed identifies and documents the information system exit points and implements malicious code protection mechanisms at those exit points to detect malicious code. Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies.	The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system exit points and verifies that malicious code protection mechanisms are implemented.	LOW	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-3(a)	CCI-002621	The organization employs malicious code protection mechanisms at information system entry points to eradicate malicious code.	The organization being inspected/assessed configures the malicious code protection mechanisms identified in SI-3, CCI 2619 to eradicate malicious code.	The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system entry points and verifies that malicious code protection mechanisms are implemented to eradicate malicious code.	LOW	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-3(a)	CCI-002622	The organization employs malicious code protection mechanisms at information system exit points to eradicate malicious code.	The organization being inspected/assessed configures the malicious code protection mechanisms identified in SI-3, CCI 2620 to eradicate malicious code.	The organization conducting the inspection/assessment examines the information system architecture as well as the organization's documentation of information system exit points and verifies that malicious code protection mechanisms are implemented to eradicate malicious code.	LOW	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-3(c)(1)	CCI-002623	The organization defines the frequency for performing periodic scans of the information system for malicious code.	DoD has defined the frequency as every 7 days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 7 days.	LOW		X		X	X			3.13.1 Malicious Code Protection	FRCS has no computers	
N/A	SI-3(c)(1)	CCI-002624	The organization configures malicious code protection mechanisms to perform real-time scans of files from external sources at network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy.	The organization being inspected/assessed configures the malicious code protection mechanisms to perform real-time scans of files from external sources at network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2624.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures malicious code protection mechanisms to perform real-time scans of files from external sources at network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2624.	LOW	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-3(10)(a)	CCI-002634	The organization defines the tools to be employed to analyze the characteristics and behavior of malicious code.	The organization being inspected/assessed defines and documents the tools to be employed to analyze the characteristics and behavior of malicious code. DoD has determined the tools are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented tools to ensure the organization being inspected/assessed defines the tools to be employed to analyze the characteristics and behavior of malicious code. DoD has determined the tools are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-3(10)(a)	CCI-002635	The organization defines the techniques to be employed to analyze the characteristics and behavior of malicious code.	The organization being inspected/assessed defines and documents the techniques to be employed to analyze the characteristics and behavior of malicious code. DoD has determined the techniques are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being inspected/assessed defines the techniques to be employed to analyze the characteristics and behavior of malicious code. DoD has determined the techniques are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-3(10)(a)	CCI-002636	The organization employs organization-defined tools to analyze the characteristics and behavior of malicious code.	The organization being inspected/assessed documents and implements tools defined in SI-3 (10), CCI 2634 to analyze the characteristics and behavior of malicious code.	The organization conducting the inspection/assessment obtains and examines the documented tools to ensure the organization being inspected/assessed employs tools defined in SI-3 (10), CCI 2634 to analyze the characteristics and behavior of malicious code.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-3(10)(a)	CCI-002638	The organization employs organization-defined techniques to analyze the characteristics and behavior of malicious code.	The organization being inspected/assessed documents and implements techniques defined in SI-3 (10), CCI 2635 to analyze the characteristics and behavior of malicious code.	The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being inspected/assessed employs techniques defined in SI-3 (10), CCI 2635 to analyze the characteristics and behavior of malicious code.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-3(10)(b)	CCI-002639	The organization incorporates the results from malicious code analysis into organizational incident response processes.	The organization being inspected/assessed incorporates the results from malicious code analysis into organizational incident response processes.	The organization conducting the inspection/assessment obtains and examines the organizational incident response processes to ensure the organization being inspected/assessed incorporates the results from malicious code analysis into organizational incident response processes.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-3(10)(b)	CCI-002640	The organization incorporates the results from malicious code analysis into organizational flaw remediation processes.	The organization being inspected/assessed incorporates the results from malicious code analysis into organizational flaw remediation processes.	The organization conducting the inspection/assessment obtains and examines the flaw remediation processes to ensure the organization being inspected/assessed incorporates the results from malicious code analysis into organizational flaw remediation processes.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(a)(1)	CCI-002641	The organization monitors the information system to detect attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives.	The organization being inspected/assessed documents and implements a process to monitor the information system to detect attacks and indicators of potential attacks in accordance with sensor placement and monitoring requirements within CJCSI 6510.01F. The organization must maintain an audit trail of monitoring. DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect attacks and indicators of potential attacks in accordance with sensor placement and monitoring requirements within CJCSI 6510.01F.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(a)(2)	CCI-002642	The organization monitors the information system to detect unauthorized local connections.	The organization being inspected/assessed documents and implements a process to monitor the information system to detect unauthorized local connections. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized local connections.	LOW	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-4(a)(2)	CCI-002643	The organization monitors the information system to detect unauthorized network connections.	The organization being inspected/assessed documents and implements a process to monitor the information system to detect unauthorized network connections. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized network connections.	LOW	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(a)(2)	CCI-002644	The organization monitors the information system to detect unauthorized remote connections.	The organization being inspected/assessed documents and implements a process to monitor information system to detect unauthorized remote connections. The organization must maintain an audit trail of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to ensure the organization being inspected/assessed monitors the information system to detect unauthorized remote connections.	LOW	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(b)	CCI-002645	The organization defines the techniques and methods to be used to identify unauthorized use of the information system.	The organization being inspected/assessed defines and documents the techniques and methods to be used to identify unauthorized use of the information system. DoD has determined the techniques and methods are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being inspected/assessed defines the techniques and methods to be used to identify unauthorized use of the information system. DoD has determined the techniques and methods are not appropriate to define at the Enterprise level.	LOW	X	X	X					3.13.3 Information System Monitoring	No requirements for Information System Monitoring given by the client	
N/A	SI-4(b)	CCI-002646	The organization identifies unauthorized use of the information system through organization-defined techniques and methods.	The organization being inspected/assessed identifies unauthorized use of the information system through techniques and methods defined in SI-4, CCI 2645. The organization must maintain an audit trail of identified instances of unauthorized use.	The organization conducting the inspection/assessment obtains and examines the audit trail of identified instances of unauthorized use to ensure the organization being inspected/assessed identifies unauthorized use of the information system through techniques and methods defined in SI-4, CCI 2645.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(d)	CCI-002647	The organization protects information obtained from intrusion-monitoring tools from unauthorized access.	The organization being inspected/assessed documents and implements a process to protect information obtained from intrusion-monitoring tools from unauthorized access.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects information obtained from intrusion-monitoring tools from unauthorized access.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(d)	CCI-002648	The organization protects information obtained from intrusion-monitoring tools from unauthorized modification.	The organization being inspected/assessed documents and implements a process to protect information obtained from intrusion-monitoring tools from unauthorized modification.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects information obtained from intrusion-monitoring tools from unauthorized modification.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(d)	CCI-002649	The organization protects information obtained from intrusion-monitoring tools from unauthorized deletion.	The organization being inspected/assessed documents and implements a process to protect information obtained from intrusion-monitoring tools from unauthorized deletion.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects information obtained from intrusion-monitoring tools from unauthorized deletion.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(g)	CCI-002650	The organization defines the information system monitoring information that is to be provided the organization-defined personnel or roles.	The organization being inspected/assessed defines and documents the information system monitoring information that is to be provided the organization-defined personnel or roles. DoD has determined the information system monitoring information is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system monitoring information to ensure the organization being inspected/assessed defines the information system monitoring information that is to be provided the organization-defined personnel or roles. DoD has determined the information system monitoring information is not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(g)	CCI-002651	The organization defines the personnel or roles that are to be provided organization-defined information system monitoring information.	The organization being inspected/assessed defines and documents the personnel or roles that are to be provided organization-defined information system monitoring information. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles that are to be provided organization-defined information system monitoring information. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(g)	CCI-002652	The organization defines the frequency at which the organization will provide the organization-defined information system monitoring information to organization-defined personnel or roles	The organization being inspected/assessed defines and documents the frequency at which the organization will provide the organization-defined information system monitoring information to organization-defined personnel or roles DoD has determined the frequency is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented frequency to ensure the organization being inspected/assessed defines the frequency at which the organization will provide the organization-defined information system monitoring information to organization-defined personnel or roles. DoD has determined the frequency is not appropriate to define at the Enterprise level.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(g)	CCI-002654	The organization provides organization-defined information system monitoring information to organization-defined personnel or roles as needed or per organization-defined frequency.	The organization being inspected/assessed provides information system monitoring information defined in SI-4, CCI 2650 to personnel or roles defined in SI-4, CCI 2651 as needed or per the frequency defined in SI-4, CCI 2652. The organization must maintain an audit trail of when information is provided.	The organization conducting the inspection/assessment obtains and examines the audit trail of when information is provided to ensure the organization being inspected/assessed provides information system monitoring information defined in SI-4, CCI 2650 to personnel or roles defined in SI-4, CCI 2651 as needed or per the frequency defined in SI-4, CCI 2652.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(1)	CCI-002655	The organization connects individual intrusion detection tools into an information system-wide intrusion detection system.	The organization being inspected/assessed connects individual intrusion detection tools into an information system-wide intrusion detection system.	The organization conducting the inspection/assessment examines the information system-wide intrusion detection system architecture and individuals tools to ensure the organization being inspected/assessed connects individual intrusion detection tools into an information system-wide intrusion detection system.	MOD	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(1)	CCI-002656	The organization configures individual intrusion detection tools into an information system-wide intrusion detection system.	The organization being inspected/assessed configures individual intrusion detection tools into an information system-wide intrusion detection system. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2656.	The organization conducting the inspection/assessment examines the information system-wide intrusion detection system to ensure the organization being inspected/assessed configures individual intrusion detection tools into an information system-wide intrusion detection system. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2656.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-4(4)	CCI-002659	The organization defines the frequency on which it will monitor inbound communications for unusual or unauthorized activities or conditions.	DoD has defined the frequency as continuously.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as continuously.	MOD	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-4(4)	CCI-002660	The organization defines the frequency on which it will monitor outbound communications for unusual or unauthorized activities or conditions.	DoD has defined the frequency as continuously.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as continuously.	MOD	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below Enclave	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-4(4)	CCI-002661	The information system monitors inbound communications traffic per organization-defined frequency for unusual or unauthorized activities or conditions.	The organization being inspected/assessed configures the information system to monitor inbound communications traffic continuously for unusual or unauthorized activities or conditions. DoD has defined the frequency as continuously.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to monitor inbound communications traffic continuously for unusual or unauthorized activities or conditions. DoD has defined the frequency as continuously.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(4)	CCI-002662	The information system monitors outbound communications traffic per organization-defined frequency for unusual or unauthorized activities or conditions.	The organization being inspected/assessed configures the information system to monitor outbound communications traffic continuously for unusual or unauthorized activities or conditions. DoD has defined the frequency as continuously.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to monitor outbound communications traffic continuously for unusual or unauthorized activities or conditions. DoD has defined the frequency as continuously.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(5)	CCI-002663	The organization defines the personnel or roles to receive information system alerts when organization-defined indicators of compromise or potential compromise occur.	DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	MOD	X			X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-4(5)	CCI-002664	The information system alerts organization-defined personnel or roles when organization-defined compromise indicators reflect the occurrence of a compromise or a potential compromise.	The organization being inspected/assessed configures the information system to alert at a minimum, the ISSM and ISSO when real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B reflect the occurrence of a compromise or a potential compromise. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2664. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO. DoD has defined the compromise indicators as real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to alert at a minimum, the ISSM and ISSO when real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B reflect the occurrence of a compromise or a potential compromise. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2664. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO. DoD has defined the compromise indicators as real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW incident categories I, II, IV, & VII within CJCSM 6510.01B.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(10)	CCI-002665	The organization defines the encrypted communications traffic that are to be visible to organization-defined information system monitoring tools.	The organization being inspected/assessed defines and documents the encrypted communications traffic that are to be visible to organization-defined information system monitoring tools. DoD has determined the encrypted traffic is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented encrypted traffic to ensure the organization being inspected/assessed defines the encrypted communications traffic that are to be visible to organization-defined information system monitoring tools. DoD has determined the encrypted traffic is not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(10)	CCI-002666	The organization defines the information system monitoring tools that will have visibility into organization-defined encrypted communications traffic.	The organization being inspected/assessed defines and documents the information system monitoring tools that will have visibility into organization-defined encrypted communications traffic. DoD has determined the information system monitoring tools are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system monitoring tools to ensure the organization being inspected/assessed defines the information system monitoring tools that will have visibility into organization-defined encrypted communications traffic. DoD has determined the information system monitoring tools are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
SC-18	SI-4(10)	CCI-002667	The organization makes provisions so that organization-defined encrypted communications traffic is visible to organization-defined information system monitoring tools.	The organization being inspected/assessed makes provisions so that encrypted communications traffic defined in SI-4 (10), CCI 2665 is visible to information system monitoring tools defined in SI-4 (10), CCI 2666.	The organization conducting the inspection/assessment examines the information system architecture to verify that the encrypted communications traffic is visible to information system monitoring tools defined in SI-4 (10), CCI 2666.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
SC-18	SI-4(11)	CCI-002668	The organization defines the interior points within the information system (e.g., subnetworks, subsystems) where outbound communications will be analyzed to discover anomalies.	The organization being inspected/assessed defines and documents the interior points within the information system (e.g., subnetworks, subsystems) where outbound communications will be analyzed to discover anomalies. DoD has determined the interior points are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented interior points to ensure the organization being inspected/assessed defines the interior points within the information system (e.g., subnetworks, subsystems) where outbound communications will be analyzed to discover anomalies. DoD has determined the interior points are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
SC-18	SI-4(19)	CCI-002673	The organization defines the additional monitoring to be implemented for individuals identified as posing an increased level of risk.	The organization being inspected/assessed defines and documents the additional monitoring to be implemented for individuals identified as posing an increased level of risk. DoD has determined the additional monitoring is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented additional monitoring to ensure the organization being inspected/assessed defines the additional monitoring to be implemented for individuals identified as posing an increased level of risk. DoD has determined the additional monitoring is not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
SC-18	SI-4(19)	CCI-002674	The organization defines the sources that may be used to identify individuals who pose an increased level of risk.	The organization being inspected/assessed defines and documents the sources that may be used to identify individuals who pose an increased level of risk. DoD has determined the sources are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented sources to ensure the organization being inspected/assessed defines the sources that may be used to identify individuals who pose an increased level of risk. DoD has determined the sources are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
SC-18	SI-4(19)	CCI-002675	The organization implements organization-defined additional monitoring of individuals who have been identified by organization-defined sources as posing an increased level of risk.	The organization being inspected/assessed implements additional monitoring defined in SI-4 (19), CCI 2673 of individuals who have been identified by sources defined in SI-4 (19), CCI 2674 as posing an increased level of risk. The organization must maintain an audit trail of additional monitoring.	The organization conducting the inspection/assessment obtains and examines the audit trail of additional monitoring to ensure the organization being inspected/assessed implements additional monitoring defined in SI-4 (19), CCI 2673 of individuals who have been identified by sources defined in SI-4 (19), CCI 2674 as posing an increased level of risk.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
SC-18	SI-4(20)	CCI-002676	The organization defines additional monitoring to be implemented for privileged users.	The organization being inspected/assessed defines and documents additional monitoring to be implemented for privileged users. DoD has determined the additional monitoring is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented additional monitoring to ensure the organization being inspected/assessed defines additional monitoring to be implemented for privileged users. DoD has determined the additional monitoring is not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(20)	CCI-002677	The organization implements organization-defined additional monitoring of privileged users.	The organization being inspected/assessed implements additional monitoring defined in SI-4 (20), CCI 2676 of privileged users. The organization must maintain an audit trail of additional monitoring.	The organization conducting the inspection/assessment obtains and examines the audit trail of additional monitoring to ensure the organization being inspected/assessed implements additional monitoring defined in SI-4 (20), CCI 2676 of privileged users.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(22)	CCI-002681	The organization defines the authorization or approval process for network services.	DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	MOD			X		X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(22)	CCI-002682	The organization defines the personnel or roles to be alerted when unauthorized or unapproved network services are detected.	DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	MOD			X		X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-4(22)	CCI-002683	The information system detects network services that have not been authorized or approved by the organization-defined authorization or approval processes.	The organization being inspected/assessed documents and implements a process to detect network services that have not been authorized or approved by at a minimum, the ISSO and ISSM. For network service detection mechanisms that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2683. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines the documented process, and examines the implemented detection mechanisms to ensure the organization being inspected/assessed implements a process to detect network services that have not been authorized or approved by at a minimum, the ISSO and ISSM. For network service detection mechanisms that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2683. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	MOD	X		X		X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
CM-6	SI-4(22)	CCI-002684	The information system audits and/or alerts organization-defined personnel when unauthorized network services are detected.	The organization being inspected/assessed configures the information system to audit and/or alert at a minimum, the ISSO and ISSM when unauthorized network services are detected. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2684. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to audit and/or alert at a minimum, the ISSO and ISSM when unauthorized network services are detected. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2684. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	MOD	X		X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
CM-6	SI-4(23)	CCI-002685	The organization defines the host-based monitoring mechanisms to be implemented at organization-defined information system components.	DoD has defined the host-based monitoring mechanisms as HBSS.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the host-based monitoring mechanisms as HBSS.	MOD	X		X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
CM-6	SI-4(23)	CCI-002686	The organization defines the information system components at which organization-defined host-based monitoring mechanisms are to be implemented.	DoD has defined the information system components as all components.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system components as all components.	MOD		X	X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
CM-6	SI-4(23)	CCI-002687	The organization implements organization-defined host-based monitoring mechanisms at organization-defined information system components.	The organization being inspected/assessed documents and implements HBSS at all components. DoD has defined the host-based monitoring mechanisms as HBSS. DoD has defined the information system components as all components.	The organization conducting the inspection/assessment obtains and examines documentation of the use of HBSS to ensure the organization being inspected/assessed implements HBSS at all components. The organization being inspected/assessed may be required to demonstrate use of HBSS. DoD has defined the host-based monitoring mechanisms as HBSS. DoD has defined the information system components as all components.	MOD	X		X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-5(a)	CCI-002692	The organization defines the external organizations from which it receives information system security alerts, advisories and directives.	DoD has defined the external organizations as at a minimum, USCYBERCOM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the external organizations as at a minimum, USCYBERCOM.	LOW	X				X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-5(c)	CCI-002693	The organization defines the elements within the organization to whom the organization will disseminate security alerts, advisories and directives.	DoD has determined the elements are not applicable as elements are not selected as recipients of security alerts, advisories and directives.	DoD has determined the elements are not applicable as elements are not selected as recipients of security alerts, advisories and directives.	LOW	X		X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-5(c)	CCI-002694	The organization defines the external organizations to whom the organization will disseminate security alerts, advisories and directives.	DoD has defined the external organizations as CNDSP Tier 1 for vetting. The CNDSP Tier 1 will pass the information to the accredited Tier 2 CNDSPs. Tier 2 CNDSPs are responsible for ensuring all Tier 3 entities receive the information. Tier 3 organizations will ensure all local Op Centers/LAN shops receive information (i.e. Component IT System and Security Personnel) (e.g. ISSM, ISSOs, and system administrators).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the external organizations as CNDSP Tier 1 for vetting. The CNDSP Tier 1 will pass the information to the accredited Tier 2 CNDSPs. Tier 2 CNDSPs are responsible for ensuring all Tier 3 entities receive the information. Tier 3 organizations will ensure all local Op Centers/LAN shops receive information (i.e. Component IT System and Security Personnel) (e.g. ISSM, ISSOs, and system administrators).	LOW				X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-7	CCI-002703	The organization defines the software, firmware, and information which will be subjected to integrity verification tools to detect unauthorized changes.	The organization being inspected/assessed defines and documents the software, firmware, and information which will be subjected to integrity verification tools to detect unauthorized changes. DoD has determined the software, firmware, and information are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented software, firmware, and information to ensure the organization being inspected/assessed defines the software, firmware, and information which will be subjected to integrity verification tools to detect unauthorized changes. DoD has determined the software, firmware, and information are not appropriate to define at the Enterprise level.	MOD	X	X						---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-7	CCI-002704	The organization employs integrity verification tools to detect unauthorized changes to organization-defined software, firmware, and information.	The organization being inspected/assessed designs the information system to employ integrity verification tools to detect unauthorized changes to software, firmware, and information defined in SI-7, CCI 2703.	The organization conducting the inspection/assessment obtains and examines the hardware/software lists and any other documentation applicable to integrity verification tools to ensure the organization being inspected/assessed employs integrity verification tools to detect unauthorized changes to software, firmware, and information defined in SI-7, CCI 2703.	MOD	X		X					3.13.2 Software, Firmware, and Information Integrity In MODERATE Impact Systems		CCI requirements are addressed within subparagraph "Software, Firmware, and Information Integrity In MODERATE Impact Systems" of UFGS 25 05 11.
N/A	SI-7(1)	CCI-002705	The organization defines the software on which integrity checks will be performed.	The organization being inspected/assessed defines and documents the software on which integrity checks will be performed. DoD has determined the software is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented software to ensure the organization being inspected/assessed defines the firmware on which integrity checks will be performed. DoD has determined the software is not appropriate to define at the Enterprise level.	MOD	X	X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-7(1)	CCI-002706	The organization defines the firmware on which integrity checks will be performed.	The organization being inspected/assessed defines and documents the firmware on which integrity checks will be performed. DoD has determined the firmware is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented firmware to ensure the organization being inspected/assessed defines the firmware on which integrity checks will be performed. DoD has determined the firmware is not appropriate to define at the Enterprise level.	MOD	X	X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-7(1)	CCI-002707	The organization defines the information on which integrity checks will be performed.	The organization being inspected/assessed defines and documents the information on which integrity checks will be performed. DoD has determined the information is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information to ensure the organization being inspected/assessed defines the information on which integrity checks will be performed. DoD has determined the information is not appropriate to define at the Enterprise level.	MOD	X	X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-7(1)	CCI-002708	The organization defines the transitional state or security-relevant events when the information system will perform integrity checks on software, firmware and information.	The organization being inspected/assessed defines and documents the transitional state or security-relevant events when the information system will perform integrity checks on software, firmware and information. DoD has determined the transitional state or security-relevant events are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented transitional state or security-relevant event to ensure the organization being inspected/assessed defines the transitional state or security-relevant events when the information system will perform integrity checks on software, firmware and information. DoD has determined the transitional state or security-relevant events are not appropriate to define at the Enterprise level.	MOD	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-7(1)	CCI-002709	The organization defines the frequency at which it will perform integrity checks of software, firmware and information.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	MOD					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-7(1)	CCI-002710	The information system performs an integrity check of organization-defined software at startup, at organization-defined transitional states or security-relevant events, or on organization-defined frequency.	The organization being inspected/assessed configures the information system to perform an integrity check of software defined in SI-7 (1), CCI 2705 at startup, at transitional states or security-relevant events defined in SI-7 (1), CCI 2708, or annually. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2710. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to perform an integrity check of software defined in SI-7 (1), CCI 2705 at startup, at transitional states or security-relevant events defined in SI-7 (1), CCI 2708, or annually. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2710. DoD has defined the frequency as annually.	MOD	X	X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-7(1)	CCI-002711	The information system performs an integrity check of organization-defined firmware at startup, at organization-defined transitional states or security-relevant events, or on organization-defined frequency.	The organization being inspected/assessed configures the information system to perform an integrity check of firmware defined in SI-7 (1), CCI 2706 at startup, at transitional states or security-relevant events defined in SI-7 (1), CCI 2708, or annually. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2711. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to perform an integrity check of firmware defined in SI-7 (1), CCI 2706 at startup, at transitional states or security-relevant events defined in SI-7 (1), CCI 2708, or annually. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2711. DoD has defined the frequency as annually.	MOD	X	X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-7(1)	CCI-002712	The information system performs an integrity check of organization-defined information at startup, at organization-defined transitional states or security-relevant events, or on organization-defined frequency.	The organization being inspected/assessed configures the information system to perform an integrity check of information defined in SI-7 (1), CCI 2707 at startup, at transitional states or security-relevant events defined in SI-7 (1), CCI 2708, or annually. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2712. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to perform an integrity check of information defined in SI-7 (1), CCI 2707 at startup, at transitional states or security-relevant events defined in SI-7 (1), CCI 2708, or annually. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2712. DoD has defined the frequency as annually.	MOD	X	X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-7(7)	CCI-002719	The organization defines the unauthorized security-relevant changes to the information system that are to be incorporated into the organizational incident response capability.	The organization being inspected/assessed defines and documents the unauthorized security-relevant changes to the information system that are to be incorporated into the organizational incident response capability. DoD has determined the security-relevant changes to the information are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security-relevant changes to the information to ensure the organization being inspected/assessed defines the unauthorized security-relevant changes to the information system that are to be incorporated into the organizational incident response capability. DoD has determined the security-relevant changes to the information are not appropriate to define at the Enterprise level.	MOD	X		X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-7(7)	CCI-002720	The organization incorporates the detection of unauthorized organization-defined security-relevant changes to the information system into the organizational incident response capability.	The organization being inspected/assessed incorporates the detection of unauthorized security-relevant changes to the information system defined in SI-7 (7), CCI 2719 into the organizational incident response capability.	The organization conducting the inspection/assessment examines the organizational incident response capability to ensure the organization being inspected/assessed incorporates the detection of unauthorized security-relevant changes to the information system defined in SI-7 (7), CCI 2719.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-7(8)	CCI-002721	The organization defines the personnel or roles that are to be alerted by the information system when it detects a potential integrity violation.	DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SI-7(8)	CCI-002722	The organization defines other actions that can be taken when the information system detects a potential integrity violation.	The organization being inspected/assessed defines and documents other actions that can be taken when the information system detects a potential integrity violation. DoD has determined the other actions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented other actions to ensure the organization being inspected/assessed defines other actions that can be taken when the information system detects a potential integrity violation. DoD has determined the other actions are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-7(8)	CCI-002723	The information system, upon detection of a potential integrity violation, provides the capability to audit the event.	The organization being inspected/assessed configures the information system to provide the capability to audit the event upon detection of a potential integrity violation. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2723.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability to audit the event upon detection of a potential integrity violation. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2723.	MOD		X	X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-7(8)	CCI-002724	The information system, upon detection of a potential integrity violation, initiates one or more of following actions: generates an audit record; alerts current user; alerts organization-defined personnel or roles; and/or organization-defined other actions.	The organization being inspected/assessed configures the information system to initiate one or more of following actions: generates an audit record; alerts current user; alerts at a minimum, the ISSO and ISSM; and/or other actions defined in SI-7 (8), CCI 2722 upon detection of a potential integrity violation. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2724. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to initiate one or more of following actions: generates an audit record; alerts current user; alerts at a minimum, the ISSO and ISSM; and/or other actions defined in SI-7 (8), CCI 2722 upon detection of a potential integrity violation. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2724. DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM.	MOD		X	X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-7(14)(a)	CCI-002737	The organization prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code.	The organization being inspected/assessed prohibits the use of binary or machine-executable code obtained from sources without vendor support or with no warranty and without the provision of source code.	The organization conducting the inspection/assessment obtains and examines the software list and examines the information system to ensure the organization being inspected/assessed prohibits the use of binary or machine-executable code obtained from sources without vendor support or with no warranty and without the provision of source code.	MOD		X	X	X				1.10 SOFTWARE LICENSING		CCI requirements are addressed within subparagraph "Software Licensing" of UFGS 25 05 11.
N/A	SI-7(14)(b)	CCI-002738	The organization provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.	The organization being inspected/assessed documents and provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.	The organization conducting the inspection/assessment obtains and examines the documented exceptions to the source code requirement to ensure the organization being inspected/assessed provides justification and approval of the authorizing official for all exceptions to the source code requirement.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-8(a)	CCI-002741	The organization employs spam protection mechanisms at information system entry points to detect and take action on unsolicited messages.	The organization being inspected/assessed implements spam protection mechanisms at information system entry points to detect and take action on unsolicited messages.	The organization conducting the inspection/assessment obtains and examines the hardware/software list to ensure the organization being inspected/assessed implements spam protection mechanisms at information system entry points to detect and take action on unsolicited messages. The organization may be required to demonstrate the use of the identified spam protection mechanisms.	MOD				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-8(a)	CCI-002742	The organization employs spam protection mechanisms at information system exit points to detect and take action on unsolicited messages.	The organization being inspected/assessed implements spam protection mechanisms at information system exit points to detect and take action on unsolicited messages.	The organization conducting the inspection/assessment obtains and examines the hardware/software list to ensure the organization being inspected/assessed implements spam protection mechanisms at information system exit points to detect and take action on unsolicited messages. The organization may be required to demonstrate the use of the identified spam protection mechanisms.	MOD				X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-10	CCI-002744	The organization defines the inputs the information system is to conduct validity checks.	The organization being inspected/assessed defines and documents specific inputs which do not require validity checks. DoD has defined the information inputs as all inputs except those identified specifically by the organization.	The organization conducting the DoD has defined the information inputs as all inputs except those identified specifically by the organization.	MOD		X			X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-10(3)	CCI-002754	The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.	The organization being inspected/assessed documents proper behavior that reflects organizational and system objectives for when invalid inputs are received. The organization being inspected/assessed configures the information system to behave in the documented manner when invalid inputs are received. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2754.	The organization conducting the inspection/assessment obtains and examines the documented behavior to ensure the organization being inspected/assessed documents proper behavior that reflects organizational and system objectives for when invalid inputs are received. The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to behave in the documented manner when invalid inputs are received. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2754.	MOD		X		X				3.8 SAFE MODE AND FAIL SAFE OPERATION		CCI requirements are addressed within subparagraph "Safe Mod and Fail Safe Operation" of UFGS 25 05 11.
N/A	SI-11(b)	CCI-002759	The organization defines the personnel or roles to whom error messages are to be revealed.	DoD has defined the personnel or roles as the ISSO, ISSM, and SCA.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSO, ISSM, and SCA.	MOD			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SI-17	CCI-002773	The organization defines the fail-safe procedures to be implemented by the information system when organization-defined failure conditions occur.	The organization being inspected/assessed defines and documents the fail-safe procedures to be implemented by the information system when organization-defined failure conditions occur. DoD has determined the fail-safe procedures are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented fail-safe procedures to ensure the organization being inspected/assessed defines the fail-safe procedures to be implemented by the information system when organization-defined failure conditions occur. DoD has determined the fail-safe procedures are not appropriate to define at the Enterprise level.	LOW		X						1.9.4 Control System Inventory Report 3.8 SAFE MODE AND FAIL SAFE OPERATION		Cybersecurity design requires the contractor to document the inventory of components within the control system and submit a Control System Inventory Report. This design requirement is captured in Sub-Paragraphs "Control System Inventory Report" within Part 1 and "SAFE MODE AND FAIL SAFE OPERATION" within Part 3
N/A	SI-17	CCI-002774	The organization defines the failure conditions which, when they occur, will result in the information system implementing organization-defined fail-safe procedures.	The organization being inspected/assessed defines and documents the failure conditions which, when they occur, will result in the information system implementing organization-defined fail-safe procedures. DoD has determined the failure conditions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented failure conditions to ensure the organization being inspected/assessed defines the failure conditions which, when they occur, will result in the information system implementing organization-defined fail-safe procedures. DoD has determined the failure conditions are not appropriate to define at the Enterprise level.	LOW		X						1.9.4 Control System Inventory Report 3.8 SAFE MODE AND FAIL SAFE OPERATION		Cybersecurity design requires the contractor to document the inventory of components within the control system and submit a Control System Inventory Report. This design requirement is captured in Sub-Paragraphs "Control System Inventory Report" within Part 1 and "SAFE MODE AND FAIL SAFE OPERATION" within Part 3
N/A	SI-17	CCI-002775	The information system implements organization-defined fail-safe procedures when organization-defined failure conditions occur.	The organization being inspected/assessed configures the information system to implement fail-safe procedures defined in SI-17, CCI 2773 when failure conditions defined in SI-17, CCI 2774 occur. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2775.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement fail-safe procedures defined in SI-17, CCI 2773 when failure conditions defined in SI-17, CCI 2774 occur. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2775.	LOW		X						1.9.4 Control System Inventory Report 3.8 SAFE MODE AND FAIL SAFE OPERATION		Cybersecurity design requires the contractor to document the inventory of components within the control system and submit a Control System Inventory Report. This design requirement is captured in Sub-Paragraphs "Control System Inventory Report" within Part 1 and "SAFE MODE AND FAIL SAFE OPERATION" within Part 3
N/A	IR-1(a)	CCI-002776	The organization defines the personnel or roles to whom the incident response policy is disseminated.	DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-1(a)	CCI-002777	The organization defines the personnel or roles to whom the incident response procedures are disseminated.	DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as all personnel identified as stakeholders in the incident response process, as well as the ISSM and ISSO.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-2(a)	CCI-002778	The organization defines the time period in which information system users whom assume an incident response role or responsibility receive incident response training.	DoD has defined the time period as 30 working days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as 30 working days.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-2(b)	CCI-002779	The organization provides incident response training to information system users consistent with assigned roles and responsibilities when required by information system changes.	The organization being inspected/assessed documents and implements a process to provide incident response training to information system users, other than general users, consistent with assigned roles and responsibilities when required by information system changes. For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training. The organization must maintain a record of training.	The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of information system users to ensure the organization being inspected/assessed provides incident response training to information system users, other than general users, consistent with assigned roles and responsibilities when required by information system changes. For general users, DoD components are automatically compliant with the requirement based on DoDD 8570.01 requirements for IA awareness training.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-3(2)	CCI-002780	The organization coordinates incident response testing with organizational elements responsible for related plans.	The organization being inspected/assessed documents within their incident response testing plan, the necessary support from all responsible organizational elements for incident response testing.	The organization conducting the inspection/assessment obtains and examines the incident response testing plan to ensure the organization being inspected/assessed coordinates incident response testing with organizational elements responsible for related plans.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-4(6)	CCI-002782	The organization implements incident handling capability for insider threats.	The organization being inspected/assessed documents within their incident response plan and implements plans to respond to incidents related to insider threats.	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as a sampling of incident after action reports to ensure the organization being inspected/assessed implements incident handling capability for insider threats.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-4(7)	CCI-002783	The organization coordinates incident handling capability for insider threats across organization-defined components or elements of the organization.	The organization being inspected/assessed documents within their incident response plan, the responsibilities of each element of the organization defined in IR-4 (7), CCI 2784.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed coordinates incident handling capability for insider threats across components or elements of the organization defined in IR-4 (7), CCI 2784.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IR-4(7)	CCI-002784	The organization defines components or elements of the organization in which incident handling capability for insider threats will be coordinated.	The organization being inspected/assessed defines and documents components or elements of the organization in which incident handling capability for insider threats will be coordinated. DoD has determined the components or elements are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented components or elements to ensure the organization being inspected/assessed defines components or elements of the organization in which incident handling capability for insider threats will be coordinated. DoD has determined the components or elements are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-4(8)	CCI-002785	The organization coordinates with organization-defined external organizations to correlate and share organization-defined incident information to achieve a cross-organization perspective on incident awareness and more effective incident responses.	The organization being inspected/assessed coordinates with external organizations defined in IR-4 (8), CCI 2786 to correlate and share incident information defined in IR-4 (8), CCI 2787 to achieve a cross-organization perspective on incident awareness and more effective incident responses.	The organization conducting the inspection/assessment obtains and examines reports, meeting minutes, or other evidence that the organization being inspected/assessed is coordinating with external organizations defined in IR-4 (8), CCI 2786 to correlate and share incident information defined in IR-4 (8), CCI 2787 to achieve a cross-organization perspective on incident awareness and more effective incident responses.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IR-4(8)	CCI-002786	The organization defines external organizations to correlate and share organization-defined incident information.	The organization being inspected/assessed defines and documents external organizations with whom they will correlate and share organization-defined incident information. DoD has determined the external organizations are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented external organizations to ensure the organization being inspected/assessed defines external organizations to correlate and share organization-defined incident information. DoD has determined the external organizations are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IR-4(8)	CCI-002787	The organization defines incident information to correlate and share with organization-defined external organizations.	The organization being inspected/assessed defines and documents what incident information will be correlated and shared with each external organization defined in IR-4 (8), CCI 2786. DoD has determined the incident information is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented incident information to ensure the organization being inspected/assessed defines what incident information will be correlated and shared with each external organization defined in IR-4 (8), CCI 2786. DoD has determined the incident information is not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IR-6(b)	CCI-002791	The organization defines authorities to whom security incident information is reported.	DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the authorities as the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).	LOW				X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
IA-5	IR-6(2)	CCI-002792	The organization defines personnel or roles to whom information system vulnerabilities associated with reported security incident information are reported.	The organization being inspected/assessed defines and documents personnel or roles to whom information system vulnerabilities associated with reported security incident information are reported. The personnel shall be identified IAW CJCSM 6510.01B. DoD has determined the personnel are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel to ensure the organization being inspected/assessed defines personnel or roles to whom information system vulnerabilities associated with reported security incident information are reported IAW CJCSM 6510.01B.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
IA-5	IR-8(a)	CCI-002794	The organization develops an incident response plan.	The organization being inspected/assessed develops and documents an incident response plan.	The organization conducting the inspection/assessment obtains and examines the documented incident response plan to ensure the organization being inspected/assessed develops an incident response plan.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
IA-5	IR-8(a)(1)	CCI-002795	The organization's incident response plan provides the organization with a roadmap for implementing its incident response capability.	The organization being inspected/assessed defines and documents within their incident response plan, a roadmap for implementing its incident response capability.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed provides within their plan, a roadmap for implementing its incident response capability.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
IA-5	IR-8(a)(2)	CCI-002796	The organization's incident response plan describes the structure and organization of the incident response capability.	The organization being inspected/assessed defines and documents within their incident response plan, the structure and organization of the incident response capability.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed describes within their plan, the structure and organization of the incident response capability.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-8(a)(3)	CCI-002797	The organization's incident response plan provides a high-level approach for how the incident response capability fits into the overall organization.	The organization being inspected/assessed defines and documents within their incident response plan, a high-level approach for how the incident response capability fits into the overall organization.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed provides within their plan, a high-level approach for how the incident response capability fits into the overall organization.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IR-8(a)(4)	CCI-002798	The organization's incident response plan meets the unique requirements of the organization, which relate to mission, size, structure, and functions.	The organization being inspected/assessed will ensure their incident response plan meets the unique requirements of the organization, which relate to mission, size, structure, and functions.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure it meets the unique requirements of the organization being inspected/assessed, which relate to mission, size, structure, and functions.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IR-8(a)(5)	CCI-002799	The organization's incident response plan defines reportable incidents.	The organization being inspected/assessed defines and document within their incident response plan, reportable incidents IAW CJCSM 6510.01B Table B-A-2.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed defines reportable incidents IAW CJCSM 6510.01B Table B-A-2.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IR-8(a)(6)	CCI-002800	The organization's incident response plan provides metrics for measuring the incident response capability within the organization.	The organization being inspected/assessed defines and documents within their incident response plan, metrics for measuring the incident response capability within the organization IAW CJCSM 6510.01B, Enclosure A.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed defines metrics for measuring the incident response capability within the organization IAW CJCSM 6510.01B, Enclosure A.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IR-8(a)(7)	CCI-002801	The organization's incident response plan defines the resources and management support needed to effectively maintain and mature an incident response capability.	The organization being inspected/assessed defines and documents within their incident response plan, the resources and management support needed to effectively maintain and mature an incident response capability.	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being inspected/assessed defines within their plan, the resources and management support needed to effectively maintain and mature an incident response capability.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IR-8(a)(8)	CCI-002802	The organization defines personnel or roles to review and approve the incident response plan.	DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	IR-8(e)	CCI-002803	The organization defines incident response personnel (identified by name and/or by role) and organizational elements to whom the incident response plan changes will be communicated.	DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the incident response personnel as all stakeholders identified in the incident response plan, not later than 30 days after the change is made.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	IR-8(f)	CCI-002804	The organization protects the incident response plan from unauthorized disclosure and modification.	The organization being inspected/assessed protects the incident response plan from unauthorized disclosure and modification.	The organization conducting the inspection/assessment obtains and examines artifacts which identify how the incident response plan is protected to ensure the organization being inspected/assessed protects the incident response plan from unauthorized disclosure and modification.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-9(3)	CCI-002818	The organization implements organization-defined procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.	The organization being inspected/assessed implements procedures defined in IR-9 (3), CCI 2819 to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.	The organization conducting the inspection/assessment obtains and examines the documented procedures defined in IR-9 (3), CCI 2819 as well as after action reports of incidents to ensure the organization being inspected/assessed implements procedures defined in IR-9 (3), CCI 2819 to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	IR-9(3)	CCI-002819	The organization defines procedures to implement to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.	The organization being inspected/assessed defines and documents procedures to implement to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions. DoD has determined the procedures are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented procedures to ensure the organization being inspected/assessed defines procedures to implement to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions. DoD has determined the procedures are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	IR-10	CCI-002822	The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.	The organization being inspected/assessed establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel. The organization appoints team members and defines and documents roles and responsibilities for each member.	The organization conducting the inspection/assessment obtains and examines appointments to the integrated team as well as the documented roles and responsibilities to ensure the organization being inspected/assessed establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SI-16	CCI-002823	The organization defines the security safeguards to be implemented to protect the information system's memory from unauthorized code execution.	The organization being inspected/assessed defines and documents the security safeguards to be implemented to protect the information system's memory from unauthorized code execution. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to be implemented to protect the information system's memory from unauthorized code execution. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	MOD	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SI-16	CCI-002824	The information system implements organization-defined security safeguards to protect its memory from unauthorized code execution.	The organization being inspected/assessed configures the information system to implement security safeguards defined in SI-16, CCI 2823 to protect its memory from unauthorized code execution. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2824.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement security safeguards defined in SI-16, CCI 2823 to protect its memory from unauthorized code execution. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2824.	MOD	X			X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-1(a)(1)	CCI-002825	The organization defines personnel or roles to whom the contingency planning policy is to be disseminated.	DoD has defined the personnel or roles as all stakeholders identified in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all stakeholders identified in the contingency plan.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-1(a)(2)	CCI-002826	The organization defines personnel or roles to whom the contingency planning procedures are disseminated.	DoD has defined the personnel or roles as all stakeholders identified in the contingency plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all stakeholders identified in the contingency plan.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-2(8)	CCI-002828	The organization identifies critical information system assets supporting essential missions.	The organization being inspected/assessed identifies and documents critical information system assets supporting essential missions.	The organization conducting the inspection/assessment obtains and examines the documented list of critical information system assets supporting essential missions to ensure the organization being inspected/assessed identifies those assets.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(8)	CCI-002829	The organization identifies critical information system assets supporting essential business functions.	The organization being inspected/assessed identifies and documents critical information system assets supporting essential business functions.	The organization conducting the inspection/assessment obtains and examines the documented list of critical information system assets supporting essential business functions to ensure the organization being inspected/assessed identifies those assets.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-2(a)(6)	CCI-002830	The organization defines the personnel or roles who review and approve the contingency plan for the information system.	DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSM and ISSO.	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-2(f)	CCI-002831	The organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to whom contingency plan changes are to be communicated.	DoD has defined the list as all stakeholders identified in the contingency plan	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the list as all stakeholders identified in the contingency plan	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-2(g)	CCI-002832	The organization protects the contingency plan from unauthorized disclosure and modification.	The organization being inspected/assessed documents and implements a process to protect the contingency plan from unauthorized disclosure and modification.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects the contingency plan from unauthorized disclosure and modification.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-3(a)	CCI-002833	The organization defines the time period that contingency training is to be provided to information system users consistent with assigned roles and responsibilities within assuming a contingency role or responsibility.	DoD has defined the time period as at a maximum, 10 working days.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as at a maximum, 10 working days.	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-3(b)	CCI-002834	The organization provides contingency training to information system users consistent with assigned roles and responsibilities when required by information system changes.	The organization being inspected/assessed will update contingency training materials when required by information system changes and provide that training to personnel with contingency roles and responsibilities IAW CP-2, CCI 449. The organization will maintain documentation of the training activity dates, location, and personnel for audit trail purposes and future reference (e.g., scheduling refresher training, etc.).	The organization conducting the inspection/assessment obtains and examines training materials and documentation of training activities to determine whether the materials are accurate in consideration of the state of the information system and content of the contingency plan. The organization ensures that training is provided to users consistent with assigned roles and responsibilities.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
SC-7	CP-6(b)	CCI-002836	The organization ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.	The organization being inspected/assessed documents the information security safeguards that are in place at both the primary and alternate sites and evidence that the alternate site was approved based on an assessment that security is equivalent at the alternate site.	The organization conducting the inspection/assessment obtains and examines the documentation of the primary/alternate site information security safeguards that are in place as well as evidence that the alternate site was approved based on an assessment that security is equivalent at the alternate site.	MOD	X							---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-7(a)	CCI-002839	The organization defines information system operations that are permitted to transfer and resume at an alternate processing sites for essential missions/business functions when the primary processing capabilities are unavailable.	The organization being inspected/assessed defines and documents information system operations that are permitted to transfer and resume at an alternate processing sites for essential missions/business functions when the primary processing capabilities are unavailable. DoD has determined the information system operations are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system operations to ensure the organization being inspected/assessed defines information system operations that are permitted to transfer and resume at an alternate processing sites for essential missions/business functions when the primary processing capabilities are unavailable. DoD has determined the information system operations are not appropriate to define at the Enterprise level.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-8	CCI-002840	The organization defines the information system operations to be resumed for essential missions within the organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	The organization being inspected/assessed defines and documents the information system operations to be resumed for essential missions within the organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. DoD has determined the information system operations are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system operations to ensure the organization being inspected/assessed defines the information system operations to be resumed for essential missions within the organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. DoD has determined the information system operations are not appropriate to define at the Enterprise level.	MOD	X							---	Per UFC 4-010-06 "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	CP-8	CCI-002841	The organization defines the information system operations to be resumed for essential business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	The organization being inspected/assessed defines and documents the information system operations to be resumed for essential business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. DoD has determined the information system operations are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system operations to ensure the organization being inspected/assessed defines the information system operations to be resumed for essential business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. DoD has determined the information system operations are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	CP-12	CCI-002855	The information system, when organization-defined conditions are detected, enters a safe mode of operation with organization-defined restrictions of safe mode of operation.	The organization being inspected/assessed configures the information system to enter a safe mode of operation with restrictions of safe mode of operation defined in CP-12, CCI 2857 when conditions defined in CP-12, CCI 2856 are detected. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2855.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to enter a safe mode of operation with restrictions of safe mode of operation defined in CP-12, CCI 2857 when conditions defined in CP-12, CCI 2856 are detected. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2855.	LOW		X						3.8 SAFE MODE AND FAIL SAFE OPERATION		CCI requirements are addressed within subparagraph "Safe Mod and Fail Safe Operation" of UFGS 25 05 11.
N/A	CP-12	CCI-002856	The organization defines the conditions, that when detected, the information system enters a safe mode of operation with organization-defined restrictions of safe mode of operation.	The organization being inspected/assessed defines and documents the conditions, that when detected, the information system enters a safe mode of operation with organization-defined restrictions of safe mode of operation. DoD has determined the conditions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure the organization being inspected/assessed defines the conditions, that when detected, the information system enters a safe mode of operation with organization-defined restrictions of safe mode of operation. DoD has determined the conditions are not appropriate to define at the Enterprise level.	LOW		X						3.8 SAFE MODE AND FAIL SAFE OPERATION		CCI requirements are addressed within subparagraph "Safe Mod and Fail Safe Operation" of UFGS 25 05 11.
N/A	CP-12	CCI-002857	The organization defines the restrictions of safe mode of operation that the information system will enter when organization-defined conditions are detected.	The organization being inspected/assessed defines and documents the restrictions of safe mode of operation that the information system will enter when organization-defined conditions are detected. DoD has determined the restrictions on safe mode of operation are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented restrictions to ensure the organization being inspected/assessed defines the restrictions of safe mode of operation that the information system will enter when organization-defined conditions are detected. DoD has determined the restrictions on safe mode of operation are not appropriate to define at the Enterprise level.	LOW		X						3.8 SAFE MODE AND FAIL SAFE OPERATION		CCI requirements are addressed within subparagraph "Safe Mod and Fail Safe Operation" of UFGS 25 05 11.
N/A	MA-1(a)	CCI-002861	The organization defines the personnel or roles to whom a system maintenance policy is disseminated.	DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	MA-1(a)	CCI-002862	The organization defines the personnel or roles to whom system maintenance procedures are to be disseminated.	DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.	LOW					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-2(a)	CCI-002866	The organization schedules maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed schedules maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of maintenance.	The organization conducting the inspection/assessment obtains and examines the record of maintenance to ensure the organization being inspected/assessed schedules maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-2(a)	CCI-002867	The organization performs maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed implements a process to perform maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of maintenance procedures followed.	The organization conducting the inspection/assessment obtains and examines the record of maintenance procedures followed to ensure the organization being inspected/assessed performs maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	MA-2(a)	CCI-002868	The organization documents maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed documents maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization conducting the inspection/assessment obtains and examines documentation of maintenance to ensure the organization being inspected/assessed documents maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-2(a)	CCI-002869	The organization reviews records of maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed documents and implements a process to review records of maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews records of maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-2(a)	CCI-002870	The organization schedules repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements	The organization being inspected/assessed schedules repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of repairs.	The organization conducting the inspection/assessment obtains and examines the record of repairs to ensure the organization being inspected/assessed schedules repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-2(a)	CCI-002871	The organization performs repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed implements a process to perform repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of repair procedures followed.	The organization conducting the inspection/assessment obtains and examines the record of repair procedures followed to ensure the organization being inspected/assessed performs repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-2(a)	CCI-002872	The organization documents repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed documents repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization conducting the inspection/assessment obtains and examines documentation of repairs to ensure the organization being inspected/assessed documents repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-2(a)	CCI-002873	The organization reviews records of repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	The organization being inspected/assessed documents and implements a process to review records of repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews records of repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-2(c)	CCI-002874	The organization defines the personnel or roles who can explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.	The organization being inspected/assessed defines and documents the personnel or roles who can explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles who can explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-2(f)	CCI-002875	The organization includes organization-defined maintenance-related information in organizational maintenance records.	The organization being inspected/assessed includes maintenance-related information defined in MA-2, CCI 2876 in organizational maintenance records.	The organization conducting the inspection/assessment obtains and examines maintenance records to ensure they include maintenance-related information defined in MA-2, CCI 2876.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-2(f)	CCI-002876	The organization defines the maintenance-related information to include in organizational maintenance records.	The organization being inspected/assessed defines and documents the maintenance-related information to include in organizational maintenance records. DoD has determined the maintenance-related information is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented maintenance-related information to ensure the organization being inspected/assessed defines the maintenance-related information to include in organizational maintenance records. DoD has determined the maintenance-related information is not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-4(1)(a)	CCI-002884	The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.	The organization being inspected/assessed configures the information system to audit nonlocal maintenance and diagnostic sessions' organization-defined audit events. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2884.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to audit nonlocal maintenance and diagnostic sessions' organization-defined audit events. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2884.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-4(1)(a)	CCI-002885	The organization defines the nonlocal maintenance and diagnostic session audit events to audit.	The organization being inspected/assessed defines and documents the nonlocal maintenance and diagnostic session audit events to audit. DoD has determined the audit events are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented audit events to ensure the organization being inspected/assessed defines the nonlocal maintenance and diagnostic session audit events to audit. DoD has determined the audit events are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	MA-4(1)(b)	CCI-002886	The organization reviews the records of the nonlocal maintenance and diagnostic sessions.	The organization being inspected/assessed documents and implements a process to review the records of the nonlocal maintenance and diagnostic sessions. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the records of the nonlocal maintenance and diagnostic sessions.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	MA-4(6)	CCI-002890	The information system implements cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2890.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2890.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-4(7)	CCI-002891	The information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.	The organization being inspected/assessed configures the information system to implement remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2891.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2891.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-5(b)	CCI-002894	The organization ensures that non-escorted personnel performing maintenance on the information system have required access authorizations.	The organization being inspected/assessed documents and implements a process to ensure that non-escorted personnel performing maintenance on the information system have required access authorizations. The organization must maintain a record of personnel performing maintenance on the information system.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of personnel performing maintenance on the information system to ensure the organization being inspected/assessed ensures that non-escorted personnel performing maintenance on the information system have required access authorizations.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-5(c)	CCI-002895	The organization designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	The organization being inspected/assessed defines and documents organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	The organization conducting the inspection/assessment obtains and examines documented organizational personnel to ensure the organization being inspected/assessed designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-6	CCI-002896	The organization defines the information system components for which it obtains maintenance support and/or spare parts.	The organization being inspected/assessed defines and documents the information system components for which it obtains maintenance support and/or spare parts. DoD has determined the information system components are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components for which it obtains maintenance support and/or spare parts. DoD has determined the information system components are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	MA-6	CCI-002897	The organization defines a time period for obtaining maintenance support and/or spare parts for organization-defined information system components after a failure.	DoD has defined the time period as within 24 hours (Low and Moderate Availability) or immediately upon failure for (High Availability).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as within 24 hours (Low and Moderate Availability) or immediately upon failure for (High Availability).	MOD				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	RA-5(5)	CCI-002906	The organization defines the vulnerability scanning activities in which the information system implements privileged access authorization to organization-identified information system components.	The organization being inspected/assessed defines and documents the vulnerability scanning activities in which the information system implements privileged access authorization to organization-identified information system components. DoD has determined the vulnerability scanning activities are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented vulnerability scanning activities to ensure the organization being inspected/assessed defines the vulnerability scanning activities in which the information system implements privileged access authorization to organization-identified information system components. DoD has determined the vulnerability scanning activities are not appropriate to define at the Enterprise level.	MOD	X	X						2.3 DATABASE AND WEB SERVER SOFTWARE FO... 3.11 VULNERABILITY SCANNING	FRCS has no computer-based databases in scope. FRCS has no IP devices to scan.	
N/A	PE-1(a)	CCI-002908	The organization defines the personnel or roles to whom a physical and environmental protection policy is disseminated.	DoD has defined the roles as organizational personnel with physical and environmental protection responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with physical and environmental protection responsibilities.	LOW			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-1(a)	CCI-002909	The organization defines the personnel or roles to whom the physical and environmental protection procedures are disseminated.	DoD has defined the roles as organizational personnel with physical and environmental protection responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with physical and environmental protection responsibilities.	LOW			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-2(a)	CCI-002910	The organization approves a list of individuals with authorized access to the facility where the information system resides.	The organization being inspected/assessed formally approves a list of individuals currently authorized to access the facility where the information system resides.	The organization conducting the inspection/assessment obtains and examines the list of individuals currently authorized to access the facility where the information system resides and ensures it is formally approved.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-2(a)	CCI-002911	The organization maintains a list of individuals with authorized access to the facility where the information system resides.	The organization being inspected/assessed maintains a list of individuals currently authorized to access the facility where the information system resides.	The organization conducting the inspection/assessment obtains and examines the list of individuals to ensure the organization being inspected/assessed maintains a list of individuals currently authorized to access the facility where the information system resides.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(a)	CCI-002915	The organization defines the entry/exit points to the facility where the information system resides.	The organization being inspected/assessed defines and documents the entry/exit points to the facility where the information system resides. DoD has determined the entry/exit points are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented entry/exit points and inspects the facility to ensure that all entry/exit points are documented. DoD has determined the entry/exit points are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(a)(2)	CCI-002916	The organization defines the physical access control systems/devices or guards that control ingress/egress to the facility.	The organization being inspected/assessed defines and documents the physical access control systems/devices or guards that control ingress/egress to the facility. DoD has determined the physical access control systems/devices are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented physical access control systems/devices to ensure the organization being inspected/assessed defines the physical access control systems/devices or guards that control ingress/egress to the facility. DoD has determined the physical access control systems/devices are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PE-3(b)	CCI-002917	The organization maintains physical access audit logs for organization-defined entry/exit points.	The organization being inspected/assessed maintains physical access audit logs for entry/exit points defined in PE-3, CCI 2918.	The organization conducting the inspection/assessment obtains and examines the physical access audit logs and compares the logged entry with known access to those entry points to ensure the organization being inspected/assessed maintains physical access audit logs for entry/exit points defined in PE-3, CCI 2918. Instances of access that will be compared with the audit logs include, at a minimum, access as part of the inspection/assessment. Comparison of other entry/exit events required elsewhere in system documentation that would have occurred before the inspection/assessment such as daily checks and scheduled maintenance are strongly encouraged and help to establish a history of compliance/non-compliance.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(b)	CCI-002918	The organization defines entry/exit points that require physical access audit logs be maintained.	The organization being inspected/assessed defines and documents entry/exit points that require physical access audit logs be maintained. DoD has determined the entry/exit points are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented entry/exit points to ensure the organization being inspected/assessed defines entry/exit points that require physical access audit logs be maintained. DoD has determined the entry/exit points are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
AC-2	PE-3(c)	CCI-002919	The organization provides organization-defined security safeguards to control access to areas within the facility officially designated as publicly accessible.	The organization being inspected/assessed provides security safeguards defined in PE-3, CCI 2920 to control access to areas within the facility officially designated as publicly accessible. The organization must document which areas are officially designated as publicly accessible.	The organization conducting the inspection/assessment obtains and examines the documentation of areas officially designated as publicly accessible to ensure the organization being inspected/assessed provides security safeguards defined in PE-3, CCI 2920 to control access to areas within the facility officially designated as publicly accessible.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(c)	CCI-002920	The organization defines security safeguards to control access to areas within the facility officially designated as publicly accessible.	The organization being inspected/assessed defines and documents security safeguards to control access to areas within the facility officially designated as publicly accessible. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines security safeguards to control access to areas within the facility officially designated as publicly accessible. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-3(d)	CCI-002921	The organization escorts visitors during organization-defined circumstances requiring visitor escorts.	The organization being inspected/assessed documents and implements a process to escort visitors during circumstances defined in PE-3, CCI 2922 requiring visitor escorts.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed escorts visitors during circumstances defined in PE-3, CCI 2922 requiring visitor escorts.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-3(d)	CCI-002922	The organization defines circumstances requiring visitor escorts.	The organization being inspected/assessed defines and documents circumstances requiring visitor escorts. DoD has determined the circumstances are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented circumstances to ensure the organization being inspected/assessed defines circumstances requiring visitor escorts. DoD has determined the circumstances are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-3(d)	CCI-002923	The organization monitors visitor activity during organization-defined circumstances requiring visitor monitoring.	The organization being inspected/assessed documents and implements a process to monitor visitor activity during circumstances defined in PE-3, CCI 2924 requiring visitor monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed monitors visitor activity during circumstances defined in PE-3, CCI 2924 requiring visitor monitoring.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-3(d)	CCI-002924	The organization defines circumstances requiring visitor monitoring.	The organization being inspected/assessed defines and documents circumstances requiring visitor monitoring. DoD has determined the circumstances are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented circumstances to ensure the organization being inspected/assessed defines circumstances requiring visitor monitoring. DoD has determined the circumstances are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-3(f)	CCI-002925	The organization defines the physical access devices to inventory.	DoD has defined the physical access devices as minimally keys or any other physical token used to gain access.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the physical access devices as minimally keys or any other physical token used to gain access.	LOW				X	X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-3(1)	CCI-002926	The organization defines the physical spaces containing one or more components of the information system that require physical access authorizations and controls at the facility.	The organization being inspected/assessed defines and documents the physical spaces containing one or more components of the information system that require physical access authorizations and controls at the facility. DoD has determined the physical spaces are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented physical spaces to ensure the organization being inspected/assessed defines the physical spaces containing one or more components of the information system that require physical access authorizations and controls at the facility. DoD has determined the physical spaces are not appropriate to define at the Enterprise level.	MOD		X	X					3.3.6 Pysical Security in MODERATE Impact…		CCI requirements are addressed within subparagraph "Physical Security in MODERATE Impact Systems" of UFGS 25 05 11.
N/A	PE-4	CCI-002930	The organization defines information system distribution and transmission lines within organizational facilities to control physical access using organization-defined security safeguards.	The organization being inspected/assessed defines and documents information system distribution and transmission lines within organizational facilities to control physical access using organization-defined security safeguards. If transmission lines carry classified information, a protected distribution system (PDS) must be used to transmit unencrypted classified information through an area of lesser classification or control. For additional information, see NSTISSI No. 7003. DoD has determined the information system distribution and transmission lines are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information system distribution and transmission lines to ensure the organization being inspected/assessed defines information system distribution and transmission lines within organizational facilities to control physical access using organization-defined security safeguards. DoD has determined the information system distribution and transmission lines are not appropriate to define at the Enterprise level.	MOD		X	X					3.3.6 Pysical Security in MODERATE Impact…		CCI requirements are addressed within subparagraph "Physical Security in MODERATE Impact Systems" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PE-4	CCI-002931	The organization defines security safeguards to control physical access to organization-defined information system distribution and transmission lines within organizational facilities.	The organization being inspected/assessed defines and documents security safeguards to control physical access to organization-defined information system distribution and transmission lines within organizational facilities. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines security safeguards to control physical access to organization-defined information system distribution and transmission lines within organizational facilities. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	MOD		X	X					3.3.6 Pysical Security in MODERATE Impact…		CCI requirements are addressed within subparagraph "Physical Security in MODERATE Impact Systems" of UFGS 25 05 11.
N/A	PE-6(a)	CCI-002939	The organization monitors physical access to the facility where the information system resides to detect and respond to physical security incidents.	The organization being inspected/assessed will implement monitoring procedures to ensure physical access intrusion alarms and surveillance equipment are actively monitored to detect and respond to all physical access security incidents.	The organization conducting the inspection/assessment obtains and examines the inspected organization's monitoring procedures addressing physical access monitoring. Organizational personnel with physical access monitoring responsibilities are to be interviewed. The objective of the reviews and interviews is to validate the organization is actively monitoring its physical access intrusion alarms and surveillance equipment to detect and respond to all physical access security incidents.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-6(b)	CCI-002940	The organization reviews physical access logs upon occurrence of organization-defined events or potential indications of events	The organization being inspected/assessed documents and implements a process to review physical access logs upon occurrence of events or potential indications of events defined in PE-6, CCI 2941. The organization must maintain records of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of reviews to ensure the organization being inspected/assessed reviews physical access logs upon occurrence of events or potential indications of events defined in PE-6, CCI 2941.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-6(b)	CCI-002941	The organization defines events or potential indications of events requiring review of physical access logs.	The organization being inspected/assessed defines and documents events or potential indications of events requiring review of physical access logs. DoD has determined the events or potential indications of events are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented events or potential indications of events to ensure the organization being inspected/assessed defines events or potential indications of events requiring review of physical access logs. DoD has determined the events or potential indications of events are not appropriate to define at the Enterprise level.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-6(4)	CCI-002950	The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as organization-defined physical spaces containing one or more components of the information system.	The organization being inspected/assessed documents and implements a process to monitor physical access to the information system in addition to the physical access monitoring of the facility as physical spaces containing one or more components of the information system defined in PE-6 (4), CCI 2951. The organization must maintain records of monitoring.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of monitoring to ensure the organization being inspected/assessed monitors physical access to the information system in addition to the physical access monitoring of the facility as physical spaces containing one or more components of the information system defined in PE-6 (4), CCI 2951.	MOD			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-6(4)	CCI-002951	The organization defines physical spaces containing one or more components of the information system in which physical access is monitored.	The organization being inspected/assessed defines and documents physical spaces containing one or more components of the information system in which physical access is monitored. DoD has determined the physical spaces are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented physical spaces to ensure the organization being inspected/assessed defines physical spaces containing one or more components of the information system in which physical access is monitored. DoD has determined the physical spaces are not appropriate to define at the Enterprise level.	MOD			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PE-8(a)	CCI-002952	The organization defines the time period to maintain visitor access records to the facility where the information system resides.	DoD has defined the time period as at least one year.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as at least one year.	LOW				X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PE-11	CCI-002955	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to long-term alternate power in the event of a primary power source loss.	The organization being inspected/assessed implements an uninterruptible power supply with sufficient capacity to support orderly shutdown of the system or transition the system to long-term alternate power in the event of a primary power source loss.	The organization conducting the inspection/assessment obtains and examines documentation identifying the capacity of the implemented uninterruptible power supply, documentation identifying the power requirements of the system, and documentation identifying the contingency plan in the event of primary power source loss to ensure the organization being inspected/assessed provides uninterruptible power supply with sufficient capacity to support orderly shutdown of the system or transition the system to long-term alternate power in the event of a primary power source loss.	LOW	X	X		X		X	NIST 800-53 does not have this in a LOW baseline. NIST 800-82 included it with the rationale "ICS may support critical activities….". By definition, a CS supporting "critical activities" is not a LOW system.	3.10 DEVICE POWER		CCI requirements are addressed within subparagraph "Device Power" of UFGS 25 05 11.
SC-8	PE-16	CCI-002974	The organization defines types of information system components to authorize, monitor, and control entering and exiting the facility and to maintain records.	DoD has defined the types of information system components as all system components.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the types of information system components as all system components.	LOW	X		X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PM-1(a)(3)	CCI-002984	The organization develops an organization-wide information security program plan that reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical).	DoDI 8500.01 and the Knowledge Service meet the requirement for this CCI; individual organizations and system owners must provide documentation of common control implementation in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PM-1(a)(1)	CCI-002985	The organization disseminates an organization-wide information security program plan that provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) and the Knowledge Service is available via: https://rmfks.osd.mil. DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PM-1(a)(2)	CCI-002986	The organization disseminates an organization-wide information security program plan that includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) and the Knowledge Service is available via: https://rmfks.osd.mil. DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-1(a)(3)	CCI-002987	The organization disseminates an organization-wide information security program plan that reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical).	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) and the Knowledge Service is available via: https://rmfks.osd.mil. DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
CM-7	PM-1(a)(4)	CCI-002988	The organization disseminates an organization-wide information security program plan that is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.	DoD disseminates DoDI 8500.01 organization-wide via the DoD Issuances website (http://www.dtic.mil/whs/directives/corres/dir.html) and the Knowledge Service is available via: https://rmfks.osd.mil. DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
CM-7	PM-1(d)	CCI-002989	The organization protects the information security program plan from unauthorized disclosure.	DoD documents and implements methods to protect the information security program plan from unauthorized disclosure by marking, labeling, and handling to prevent unauthorized disclosure. DoD ensures that all changes to the information security program plan are approved.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
CM-7	PM-1(d)	CCI-002990	The organization protects the information security program plan from unauthorized modification.	DoD documents and implements methods to protect the information security program plan from unauthorized disclosure by marking, labeling, and handling to prevent unauthorized modification. DoD ensures that all changes to the information security program plan are approved.	DoD components are automatically compliant with this CCI as they are covered at the DoD level by DoDI 8500.01 and the Knowledge Service. If the organization or system owner is utilizing common controls they must be documented in their Security Plan.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-4(a)(1)	CCI-002991	The organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems are developed.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to develop a process for plans of action and milestones for the security program. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to develop a process for plans of action and milestones for the security program. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-4(a)(3)	CCI-002992	The organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems are reported in accordance with OMB FISMA reporting requirements.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to implement a process ensuring that the plans of action and milestones for the security program are reported in accordance with OMB FISMA reporting requirements. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	DoDI 8510.01 and the Knowledge Service meet the DoD requirements to implement a process ensuring that the plans of action and milestones for the security program are reported in accordance with OMB FISMA reporting requirements. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01 and the Knowledge Service.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
CM-6	PM-4(b)	CCI-002993	The organization reviews plans of action and milestones for the security program and associated organization information systems for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	The organization being inspected/assessed documents and implements a process to review plans of action and milestones for the security program and associated organization information systems for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews plans of action and milestones for the security program and associated organization information systems for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-9(c)	CCI-002994	The organization reviews and updates the risk management strategy in accordance with organization-defined frequency or as required, to address organizational changes.	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by the DoD Risk Management Framework (DoDI 8510.01).	DoD Risk Management Framework meets the requirement for a comprehensive organizational risk strategy. DoD components are automatically compliant with this CCI because they are covered by DoD Risk Management Framework (DoDI 8510.01).	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-9(c)	CCI-002995	The organization defines the frequency to review and update the risk management strategy to address organizational changes.	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-12	CCI-002996	The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.	The organization being inspected/assessed documents and implements an insider threat program that includes a cross-discipline insider threat incident handling team.	The organization conducting the inspection/assessment obtains and examines the documented insider threat program to ensure the organization being inspected/assessed implements an insider threat program that includes a cross-discipline insider threat incident handling team.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
AC-18	PM-13	CCI-002997	The organization establishes an information security workforce development and improvement program.	DoD 8570.01-M, "Information Assurance Workforce Improvement Program" meets the DoD requirement to establish an information security workforce development and improvement program. DoD components are automatically complaint with this CCI as they are covered at the DoD level, DoDI 8570.01-M.	DoD 8570.01-M meets the DoD requirement to establish an information security workforce development and improvement program. DoD components are automatically complaint with this CCI as they are covered at the DoD level, DoDI 8570.01-M.	LOW					X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
AC-18	PM-14(a)(1)	CCI-002998	The organization implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are developed.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are developed.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are developed.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
AC-18	PM-14(a)(1)	CCI-002999	The organization implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are maintained.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are maintained.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security testing activities associated with organizational information systems are maintained.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
AC-18	PM-14(a)(1)	CCI-003000	The organization implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are developed.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are developed.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are developed.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
AC-4	PM-14(a)(1)	CCI-003001	The organization implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are maintained.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are maintained.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security training activities associated with organizational information systems are maintained.	LOW			X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
AC-4	PM-14(a)(1)	CCI-003002	The organization implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are developed.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are developed.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are developed.	LOW			X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
AC-4	PM-14(a)(1)	CCI-003003	The organization implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are maintained.	The organization being inspected/assessed documents and implements a process for conducting security monitoring activities associated with organizational information systems are maintained.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems are maintained.	LOW			X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
AC-4	PM-14(a)(2)	CCI-003004	The organization implements a process for ensuring that organizational plans for conducting security testing associated with organizational information systems continue to be executed in a timely manner.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security testing associated with organizational information systems continue to be executed in a timely manner. The organization must maintain records of execution.	The organization conducting the inspection/assessment obtains and examines the documented process as well as records of execution to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security testing associated with organizational information systems continue to be executed in a timely manner.	LOW			X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
AC-4	PM-14(a)(2)	CCI-003005	The organization implements a process for ensuring that organizational plans for conducting security training associated with organizational information systems continue to be executed in a timely manner.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security training associated with organizational information systems continue to be executed in a timely manner. The organization must maintain records of execution.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of execution to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security training associated with organizational information systems continue to be executed in a timely manner.	LOW			X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
AC-4	PM-14(a)(2)	CCI-003006	The organization implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems continue to be executed in a timely manner.	The organization being inspected/assessed documents and implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems continue to be executed in a timely manner. The organization must maintain records of execution.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of execution to ensure the organization being inspected/assessed implements a process for ensuring that organizational plans for conducting security monitoring activities associated with organizational information systems continue to be executed in a timely manner.	LOW			X						---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PM-14(b)	CCI-003007	The organization reviews testing plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	The organization being inspected/assessed documents and implements a process to review testing plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews testing plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-14(b)	CCI-003008	The organization reviews training plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	The organization being inspected/assessed reviews training plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews training plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-14(b)	CCI-003009	The organization reviews monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	The organization being inspected/assessed reviews monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The organization must maintain a record of reviews.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	LOW			X						---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PM-15(a)	CCI-003010	The organization establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel.	The organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel.	The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-15(b)	CCI-003011	The organization establishes and institutionalizes contact with selected groups and associations within the security community to maintain currency with recommended security practices, techniques, and technologies.	The organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to maintain currency with recommended security practices, techniques, and technologies.	The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to maintain currency with recommended security practices, techniques, and technologies.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-15(c)	CCI-003012	The organization establishes and institutionalizes contact with selected groups and associations within the security community to share current security-related information including threats, vulnerabilities, and incidents.	The organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to share current security-related information including threats, vulnerabilities, and incidents.	The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being inspected/assessed establishes and institutionalizes contact with selected groups and associations within the security community to share current security-related information including threats, vulnerabilities, and incidents.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PM-16	CCI-003013	The organization implements a threat awareness program that includes a cross-organization information-sharing capability.	The organization being inspected/assessed documents and implements a threat awareness program that includes a cross-organization information-sharing capability.	The organization conducting the inspection/assessment obtains and examines the documented threat awareness program to ensure the organization being inspected/assessed implements a threat awareness program that includes a cross-organization information-sharing capability.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PS-4(f)	CCI-003016	The organization, upon termination of individual employment, notifies organization-defined personnel or roles within an organization-defined time period.	The organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for revoking credentials immediately or within 24 hours upon termination of individual employment. The organization must maintain records of termination notification. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials. DoD has defined the time period as immediately or within 24 hours.	The organization conducting the inspection/assessment obtains and examines records of termination notification to ensure the organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for revoking credentials immediately or within 24 hours upon termination of individual employment. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials. DoD has defined the time period as immediately or within 24 hours.	LOW				X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
SI-4	PS-1(a)	CCI-003017	The organization defines the personnel or roles to whom a personnel security policy is disseminated.	DoD has defined the roles as organizational personnel with access control responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with access control responsibilities.	LOW			X	X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
SI-4	PS-1(a)	CCI-003018	The organization defines the personnel or roles to whom the personnel security procedures are disseminated.	DoD has defined the roles as organizational personnel with access control responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as organizational personnel with access control responsibilities.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-4(a)	CCI-003022	The organization defines the time period to disable information system access upon termination of individual employment.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.	LOW				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-4(b)	CCI-003023	The organization, upon termination of individual employment, terminates/revokes any authenticators/credentials associated with the individual.	The organization being inspected/assessed documents and implements a process to terminate/revoke any authenticators/credentials associated with the individual upon termination of individual employment. The organization must maintain records of termination/revocation of any authenticators/credentials.	The organization conducting the inspection/assessment obtains and examines the documented process as well as a sampling of records of termination/revocation of any authenticators/credentials to ensure the organization being inspected/assessed terminates/revokes any authenticators/credentials associated with the individual upon termination of individual employment.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-4(c)	CCI-003024	The organization defines information security topics to be discussed while conducting exit interviews.	The organization being inspected/assessed defines and documents information security topics to be discussed while conducting exit interviews. DoD has determined the information security topics are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented information security topics to ensure the organization being inspected/assessed defines information security topics to be discussed while conducting exit interviews. DoD has determined the information security topics are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
RA-5	PS-4(f)	CCI-003025	The organization defines personnel or roles to notify upon termination of individual employment.	DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for revoking credentials.	LOW				X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
RA-5	PS-4(f)	CCI-003026	The organization defines the time period in which to notify organization-defined personnel or roles upon termination of individual employment.	DoD has defined the time period as immediately or within 24 hours.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately or within 24 hours.	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
RA-5	PS-5(c)	CCI-003031	The organization modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.	The organization being inspected/assessed documents and implements a process to modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.	The organization conducting the inspection/assessment obtains and examines the documented process and a sampling of accounts of users recently transferred or reassigned to ensure the organization being inspected/assessed modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
RA-5	PS-5(d)	CCI-003032	The organization notifies organization-defined personnel or roles within an organization-defined time period when individuals are transferred or reassigned to other positions within the organization.	The organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for transferring credentials within 24 hours when individuals are transferred or reassigned to other positions within the organization. The organization must maintain records of transfer/reassignment notifications. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. DoD has defined the time period as within 24 hours.	The organization conducting the inspection/assessment obtains and examines records of transfer/reassignment notifications to ensure the organization being inspected/assessed notifies at a minimum, the ISSO and personnel responsible for transferring credentials within 24 hours when individuals are transferred or reassigned to other positions within the organization. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. DoD has defined the time period as within 24 hours.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
RA-5	PS-5(d)	CCI-003033	The organization defines personnel or roles to be notified when individuals are transferred or reassigned to other positions within the organization.	DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.	LOW					X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
RA-5	PS-5(d)	CCI-003034	The organization defines the time period within which organization-defined personnel or roles are to be notified when individuals are transferred or reassigned to other positions within the organization.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.	LOW				X	X			---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
RA-5	PS-6(a)	CCI-003035	The organization develops and documents access agreements for organizational information systems.	The organization being inspected/assessed develops and documents access agreements for organizational information systems.	The organization conducting the inspection/assessment obtains and examines the documented access agreements to ensure the organization being inspected/assessed develops and documents access agreements for organizational information systems.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
RA-5	PS-6(c)(2)	CCI-003036	The organization ensures that individuals requiring access to organizational information and information systems re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or in accordance with organization-defined frequency.	The organization being inspected/assessed requires that individuals re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or when there is a change to the user's level of access. DoD has defined the frequency as when there is a change to the user's level of access.	The organization conducting the inspection/assessment obtains and examines a sampling of re-signed access agreements to ensure the organization being inspected/assessed requires that individuals re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or when there is a change to the user's level of access. DoD has defined the frequency as when there is a change to the user's level of access.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-6(c)(2)	CCI-003037	The organization defines the frequency for individuals requiring access to organization information and information systems to re-sign access agreements.	DoD has defined the frequency as when there is a change to the user's level of access.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as when there is a change to the user's level of access.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PS-7(b)	CCI-003040	The organization requires third-party providers to comply with personnel security policies and procedures established by the organization.	The organization being inspected/assessed documents and implements a process to require third-party providers to comply with personnel security policies and procedures established by the organization.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires third-party providers to comply with personnel security policies and procedures established by the organization.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-7(d)	CCI-003041	The organization requires third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within an organization-defined time period.	The organization being inspected/assessed documents and implements a process to require third-party providers to notify at a minimum, the ISSO and personnel responsible for transferring credentials of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges immediately. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. DoD has defined the time period as immediately.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires third-party providers to notify at a minimum, the ISSO and personnel responsible for transferring credentials of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges immediately. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials. DoD has defined the time period as immediately.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-7(d)	CCI-003042	The organization defines personnel or roles whom third-party providers are to notify when third-party personnel who possess organizational credentials and /or badges or who have information system privileges are transferred or terminated.	DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO and personnel responsible for transferring credentials.	LOW					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-7(d)	CCI-003043	The organization defines the time period for third party providers to notify organization-defined personnel or roles when third-party personnel who possess organizational credentials and /or badges or who have information system privileges are transferred or terminated.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.	LOW					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-8(b)	CCI-003044	The organization notifies organization-defined personnel or roles within an organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	The organization being inspected/assessed notifies at a minimum, the ISSO immediately when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. The organization must maintain records of notifications of employee sanctions. DoD has defined the personnel or roles as at a minimum, the ISSO. DoD has defined the time period as immediately.	The organization conducting the inspection/assessment obtains and examines the records of notifications of employee sanctions to ensure the organization being inspected/assessed notifies at a minimum, the ISSO immediately when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. DoD has defined the personnel or roles as at a minimum, the ISSO. DoD has defined the time period as immediately.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-8(b)	CCI-003045	The organization defines personnel or roles whom are to be notified when a formal employee sanctions process is initiated.	DoD has defined the personnel or roles as at a minimum, the ISSO.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO.	LOW					X			---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PS-8(b)	CCI-003046	The organization defines the time period to notify organization-defined personnel or roles when a formal employee sanctions process is initiated.	DoD has defined the time period as immediately.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as immediately.	LOW					X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PL-1(a)	CCI-003047	The organization defines the personnel or roles to whom a security planning policy is disseminated.	DoD has defined the roles as all organizational personnel with planning responsibilities or information security responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as all personnel organizational personnel with planning responsibilities or information security responsibilities.	LOW			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PL-1(a)	CCI-003048	The organization defines the personnel or roles to whom the security planning procedures are disseminated.	DoD has defined the roles as all organizational personnel with planning responsibilities or information security responsibilities.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the roles as all organizational personnel with planning responsibilities or information security responsibilities.	LOW			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(a)	CCI-003049	The organization develops a security plan for the information system.	The organization being inspected/assessed develops and documents a security plan for the information system.	The organization conducting the inspection/assessment obtains and examines the documented security plan to ensure the organization being inspected/assessed develops a security plan for the information system.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PL-2(a)(1)	CCI-003050	The organization's security plan for the information system is consistent with the organization's enterprise architecture.	The organization being inspected/assessed defines a security plan for the information system which is consistent with the organization's enterprise architecture.	The organization conducting the inspection/assessment obtains and examines the security plan and the enterprise architecture to ensure the organization's security plan for the information system is consistent with the organization's enterprise architecture.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(a)(2)	CCI-003051	The organization's security plan for the information system explicitly defines the authorization boundary for the system.	The organization being inspected/assessed explicitly defines within the security plan the authorization boundary for the system.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed explicitly defines within the security plan the authorization boundary for the system.	LOW	X	X	X					1.9.6 Cybersecurity Riser Diagram		Cybersecurity Requirements are met by requiring the contractor to submit a "Cybersecurity Riser Diagram" report with Part 1
N/A	PL-2(a)(3)	CCI-003052	The organization's security plan for the information system describes the operational context of the information system in terms of missions and business processes.	The organization being inspected/assessed describes within the security plan the operational context of the information system in terms of missions and business processes.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed describes within the security plan the operational context of the information system in terms of missions and business processes.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(a)(4)	CCI-003053	The organization's security plan for the information system provides the security categorization of the information system including supporting rationale.	The organization being inspected/assessed defines within the security plan the security categorization of the information system including supporting rationale.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed defines within the security plan the security categorization of the information system including supporting rationale.	LOW		X	X					1.9.6 Cybersecurity Riser Diagram		Cybersecurity Requirements are met by requiring the contractor to submit a "Cybersecurity Riser Diagram" report with Part 1
N/A	PL-2(a)(5)	CCI-003054	The organization's security plan for the information system describes the operational environment for the information system and relationships with or connections to other information systems.	The organization being inspected/assessed describes within the security plan the operational environment for the information system and relationships with or connections to other information systems.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed describes within the security plan the operational environment for the information system and relationships with or connections to other information systems.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-2(a)(6)	CCI-003055	The organization's security plan for the information system provides an overview of the security requirements for the system	The organization being inspected/assessed documents within the security plan, an overview of the security requirements for the system.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed their security plan for the information system provides an overview of the security requirements for the system	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(a)(7)	CCI-003056	The organization's security plan for the information system identifies any relevant overlays, if applicable.	The organization being inspected/assessed identifies within the security plan any relevant overlays, if applicable.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed identifies within the security plan any relevant overlays, if applicable.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-2(a)(8)	CCI-003057	The organization's security plan for the information system describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions.	The organization being inspected/assessed describes within the security plan the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed describes within the security plan the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-2(b)	CCI-003059	The organization distributes copies of the security plan to organization-defined personnel or roles.	The organization being inspected/assessed distributes copies of the security plan to, at a minimum, the ISSO, ISSM and SCA via the organization's information sharing portal. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	The organization conducting the inspection/assessment obtains and examines the security plan via the organization's information sharing portal to ensure the organization being inspected/assessed distributes copies of the security plan to at a minimum, the ISSO, ISSM and SCA via the organization's information sharing portal. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-2(b)	CCI-003060	The organization defines the personnel or roles to whom copies of the security plan is distributed.	DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	LOW				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PL-2(b)	CCI-003061	The organization communicates subsequent changes to the security plan to organization-defined personnel or roles.	The organization being inspected/assessed distributes changes to the security plan to, at a minimum, the ISSO, ISSM and SCA via the organization's information sharing portal. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	The organization conducting the inspection/assessment examines the organization's information sharing portal to ensure at a minimum, the ISSO, ISSM and SCA have been provided changes to the security plan. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-2(b)	CCI-003062	The organization defines the personnel or roles to whom changes to the security plan are communicated.	DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM and SCA.	LOW				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
IA-3	PL-2(e)	CCI-003063	The organization protects the security plan from unauthorized disclosure.	The organization being inspected/assessed documents and implements a process to protect the security plan from unauthorized disclosure.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects the security plan from unauthorized disclosure.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
IA-3	PL-2(e)	CCI-003064	The organization protects the security plan from unauthorized modification.	The organization being inspected/assessed documents and implements a process to protect the security plan from unauthorized modification.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed protects the security plan from unauthorized modification.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
IA-3	PL-2(3)	CCI-003065	The organization plans and coordinates security-related activities affecting the information system with organization-defined individuals or groups before conducting such activities in order to reduce the impact on other organizational entities.	The organization being inspected/assessed defines and documents within the security plan, the planning and coordination of security-related activities affecting the information system with individuals or groups defined in PL-2 (3), CCI 3067 before conducting such activities in order to reduce the impact on other organizational entities.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed plans and coordinates of security-related activities affecting the information system with individuals or groups defined in PL-2 (3), CCI 3067 before conducting such activities in order to reduce the impact on other organizational entities.	LOW			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
CM-8	PL-2(3)	CCI-003067	The organization defines the individuals or groups with whom security-related activities are planned and coordinated.	The organization being inspected/assessed defines and documents the individuals or groups with whom security-related activities are planned and coordinated. DoD has determined the individuals or groups are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented individuals or groups to ensure the organization being inspected/assessed defines the individuals or groups with whom security-related activities are planned and coordinated. DoD has determined the individuals or groups are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
CM-8	PL-4(c)	CCI-003068	The organization reviews and updates the rules of behavior in accordance with organization-defined frequency.	The organization being inspected/assessed reviews and updates the rules of behavior annually. The organization must maintain an audit trail of reviews and updates. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the rules of behavior annually. DoD has defined the frequency as annually.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
CM-8	PL-4(c)	CCI-003069	The organization defines the frequency to review and update the rules of behavior.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	LOW				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
CA-9	PL-4(d)	CCI-003070	The organization requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.	The organization being inspected/assessed documents and implements a process to require individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated. The signed acknowledgment portion of this control may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
CA-9	PL-8(a)	CCI-003072	The organization develops an information security architecture for the information system.	The organization being inspected/assessed develops and documents an information security architecture for the information system.	The organization conducting the inspection/assessment obtains and examines the documented information security architecture to ensure the organization being inspected/assessed develops an information security architecture for the information system.	MOD		X	X					1.9.2 Cybersecurity Interconnection Sched... 1.9.3 Network Communication Report 1.9.6 Cybersecurity Riser Diagram		Requirement is met by requiring the contractor to submit the "Cybersecurity Interconnection Schedule", "Network Communications Report", and "Cybersecurity Riser Diagram"
CA-9	PL-8(a)(1)	CCI-003073	The organization's information security architecture for the information system describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.	The organization being inspected/assessed describes within the information security architecture for the information system, the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.	The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization being inspected/assessed describes within the information security architecture for the information system, the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.	MOD		X	X					1.9.2 Cybersecurity Interconnection Sched... 1.9.3 Network Communication Report 1.9.6 Cybersecurity Riser Diagram		Requirement is met by requiring the contractor to submit the "Cybersecurity Interconnection Schedule", "Network Communications Report", and "Cybersecurity Riser Diagram"
CA-9	PL-8(a)(2)	CCI-003074	The organization's information security architecture for the information system describes how the information security architecture is integrated into and supports the enterprise architecture.	The organization being inspected/assessed describes within the information security architecture for the information system, how the information security architecture is integrated into and supports the enterprise architecture.	The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization being inspected/assessed describes within the information security architecture for the information system, how the information security architecture is integrated into and supports the enterprise architecture.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-8(a)(3)	CCI-003075	The organization's information security architecture for the information system describes any information security assumptions about, and dependencies on, external services.	The organization being inspected/assessed describes within the information security architecture for the information system, any information security assumptions about, and dependencies on, external services.	The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization being inspected/assessed describes within the information security architecture for the information system, any information security assumptions about, and dependencies on, external services.	MOD		X	X					1.9.2 Cybersecurity Interconnection Sched... 1.9.3 Network Communication Report 1.9.6 Cybersecurity Riser Diagram		Requirement is met by requiring the contractor to submit the "Cybersecurity Interconnection Schedule", "Network Communications Report", and "Cybersecurity Riser Diagram"
N/A	PL-8(b)	CCI-003076	The organization reviews and updates the information security architecture in accordance with organization-defined frequency to reflect updates in the enterprise architecture.	The organization being inspected/assessed reviews and updates the information security architecture annually to reflect updates in the enterprise architecture. The organization must maintain an audit trail of reviews and updates. DoD has defined the frequency as annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates the information security architecture annually to reflect updates in the enterprise architecture. DoD has defined the frequency as annually.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-8(b)	CCI-003077	The organization defines the frequency to review and update the information system architecture.	DoD has defined the frequency as annually.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually.	MOD				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	PL-8(c)	CCI-003078	The organization ensures that planned information security architecture changes are reflected in the security plan.	The organization being inspected/assessed includes planned information security architecture changes in the security plan.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed includes planned information security architecture changes in the security plan.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-8(c)	CCI-003079	The organization ensures that planned information security architecture changes are reflected in the security Concept of Operations (CONOPS).	The organization being inspected/assessed includes planned information security architecture changes in the security Concept of Operations (CONOPS).	The organization conducting the inspection/assessment obtains and examines security CONOPS to ensure the organization being inspected/assessed includes planned information security architecture changes in the security CONOPS.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
CA-3	PL-8(c)	CCI-003080	The organization ensures that planned information security architecture changes are reflected in organizational procurements/acquisitions.	The organization being inspected/assessed includes planned information security architecture changes in organizational procurements/acquisitions.	The organization conducting the inspection/assessment obtains and examines a sampling of procurement materials to ensure the organization being inspected/assessed includes planned information security architecture changes in organizational procurements/acquisitions.	MOD			X					---	Per UFC 4-010-06 Table G-6 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-8(1)(a)	CCI-003081	The organization designs its security architecture using a defense-in-depth approach that allocates organization-defined security safeguards to organization-defined locations.	The organization being inspected/assessed designs and documents its security architecture using a defense-in-depth approach that allocates security safeguards defined in PL-8 (1), CCI 3083 to locations defined in PL-8 (1), CCI 3085.	The organization conducting the inspection/assessment obtains and examines the security architecture to ensure the organization being inspected/assessed designs its security architecture using a defense-in-depth approach that allocates security safeguards defined in PL-8 (1), CCI 3083 to locations defined in PL-8 (1), CCI 3085.	MOD		X	X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-8(1)(a)	CCI-003082	The organization designs its security architecture using a defense-in-depth approach that allocates organization-defined security safeguards to organization-defined architectural layers.	The organization being inspected/assessed designs and documents its security architecture using a defense-in-depth approach that allocates security safeguards defined in PL-8 (1), CCI 3084 to architectural layers defined in PL-8 (1), CCI 3086.	The organization conducting the inspection/assessment obtains and examines the security architecture to ensure the organization being inspected/assessed designs its security architecture using a defense-in-depth approach that allocates security safeguards defined in PL-8 (1), CCI 3084 to architectural layers defined in PL-8 (1), CCI 3086.	MOD		X	X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	PL-8(1)(a)	CCI-003083	The organization defines the security safeguards to be allocated to organization-defined locations.	The organization being inspected/assessed defines and documents the security safeguards to be allocated to organization-defined locations. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to be allocated to organization-defined locations. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-8(1)(a)	CCI-003084	The organization defines the security safeguards to be allocated to organization-defined architectural layers.	The organization being inspected/assessed defines and documents the security safeguards to be allocated to organization-defined architectural layers. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to be allocated to organization-defined architectural layers. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
CM-2	PL-8(1)(a)	CCI-003085	The organization defines the locations to which it allocates organization-defined security safeguards in the security architecture.	The organization being inspected/assessed defines and documents the locations to which it allocates organization-defined security safeguards in the security architecture. DoD has determined the locations are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented locations to ensure the organization being inspected/assessed defines the locations to which it allocates organization-defined security safeguards in the security architecture. DoD has determined the locations are not appropriate to define at the Enterprise level.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	PL-8(1)(a)	CCI-003086	The organization defines the architectural layers to which it allocates organization-defined security safeguards in the security architecture.	The organization being inspected/assessed defines and documents the architectural layers to which it allocates organization-defined security safeguards in the security architecture. DoD has determined the architectural layers are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented architectural layers to ensure the organization being inspected/assessed defines the architectural layers to which it allocates organization-defined security safeguards in the security architecture. DoD has determined the architectural layers are not appropriate to define at the Enterprise level.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-8(1)(b)	CCI-003087	The organization designs its security architecture using a defense-in-depth approach that ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.	The organization being inspected/assessed designs and documents its security architecture using a defense-in-depth approach that ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.	The organization conducting the inspection/assessment obtains and examines security architecture to ensure the organization being inspected/assessed designs its security architecture using a defense-in-depth approach that ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.	MOD		X	X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-1(a)	CCI-003089	The organization defines the personnel or roles to whom the system and services acquisition policy is disseminated.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.	LOW			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-1(a)	CCI-003090	The organization defines the personnel or roles to whom procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls are disseminated.	DoD has defined the personnel or roles as all personnel.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all personnel.	LOW			X	X	X			---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-2(a)	CCI-003091	The organization determines information security requirements for the information system or information system service in mission/business process planning.	The organization being inspected/assessed determines and documents information security requirements for the information system or information system service in mission/business process planning.	The organization conducting the inspection/assessment obtains and examines the documented information security requirements to ensure the organization being inspected/assessed determines information security requirements for the information system or information system service in mission/business process planning.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-3(a)	CCI-003092	The organization defines a system development life cycle that is used to manage the information system.	The organization being inspected/assessed defines and documents a system development life cycle that is used to manage the information system. DoD has determined the system development life cycle is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented system development life cycle to ensure the organization being inspected/assessed defines a system development life cycle that is used to manage the information system. DoD has determined the system development life cycle is not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-3(d)	CCI-003093	The organization integrates the organizational information security risk management process into system development life cycle activities.	The organization being inspected/assessed documents and implements a process to integrate the organizational information security risk management process into system development life cycle activities.	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed integrates the organizational information security risk management process into system development life cycle activities.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(a)	CCI-003094	The organization includes the security functional requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, the security functional requirements, explicitly or by reference, IAW DoDI 8580.1.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes the security functional requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs including DoDI 8580.1.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(b)	CCI-003095	The organization includes the security strength requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, the security strength requirements, explicitly or by reference, IAW DoDI 8580.1.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes the security strength requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs including DoDI 8580.1.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(c)	CCI-003096	The organization includes the security assurance requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, the security assurance requirements, explicitly or by reference, IAW DoDI 8580.1.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes the security assurance requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs including DoDI 8580.1.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(d)	CCI-003097	The organization includes the security-related documentation requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, the security-related documentation requirements, explicitly or by reference.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes the security-related documentation requirements, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(e)	CCI-003098	The organization includes requirements for protecting security-related documentation, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, requirements for protecting security-related documentation, explicitly or by reference.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes requirements for protecting security-related documentation, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	LOW			X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-4(f)	CCI-003099	The organization includes description of the information system development environment and environment in which the system is intended to operate, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, a description of the information system development environment and environment in which the system is intended to operate, explicitly or by reference.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes a description of the information system development environment and environment in which the system is intended to operate, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	LOW			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
IA-5	SA-4(g)	CCI-003100	The organization includes acceptance criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	The organization being inspected/assessed documents within contracts/agreements for the information system, system component, or information system service, acceptance criteria, explicitly or by reference.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed includes acceptance criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	LOW			X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(2)	CCI-003101	The organization requires the developer of the information system, system component, or information system service to provide design information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code, hardware schematics and/or organization-defined design/information at organization-defined level of detail.	The organization being inspected/assessed defines and documents in contracts/agreements, the design information for the security controls that the developer will employ in the information system to include security-relevant external system interfaces, high-level design, low-level design, source code, hardware schematics and/or design/information defined in SA-4 (2), CCI 3103 at the level of detail defined in SA-4 (2), CCI 3105.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires the developer of the information system, system component, or information system service to provide design information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code and/or hardware schematics and/or design/information defined in SA-4 (2), CCI 3103 at the level of detail defined in SA-4 (2), CCI 3105.	MOD		X	X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-4(2)	CCI-003102	The organization requires the developer of the information system, system component, or information system service to provide implementation information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code and/or hardware schematics organization-defined implementation information at organization-defined level of detail.	The organization being inspected/assessed defines and documents in contracts/agreements, the implementation information for the security controls that the developer will employ in the information system to include security-relevant external system interfaces, high-level design, low-level design, source code and/or hardware schematics and/or implementation information defined in SA-4 (2), CCI 3104 at the level of detail defined in SA-4 (2), CCI 3106.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires the developer of the information system, system component, or information system service to provide implementation information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code and/or hardware schematics and/or implementation information defined in SA-4 (2), CCI 3104 at the level of detail defined in SA-4 (2), CCI 3106.	MOD		X	X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-4(2)	CCI-003103	The organization defines the design information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed.	The organization being inspected/assessed defines and documents the design information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed. DoD has determined the design information is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented design information to ensure the organization being inspected/assessed defines the design information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed. DoD has determined the design information is not appropriate to define at the Enterprise level.	MOD		X	X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-4(2)	CCI-003104	The organization defines the implementation information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed.	The organization being inspected/assessed defines and documents the implementation information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed. DoD has determined the implementation information is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented implementation information to ensure the organization being inspected/assessed defines the implementation information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed. DoD has determined the implementation information is not appropriate to define at the Enterprise level.	MOD		X	X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-4(2)	CCI-003105	The organization defines the level of detail the design information of the security controls is required to be provided by the developer of the information system, system component, or information system services.	The organization being inspected/assessed defines and documents the level of detail the design information of the security controls is required to be provided by the developer of the information system, system component, or information system services. DoD has determined the level of detail is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented level of detail to ensure the organization being inspected/assessed defines the level of detail the design information of the security controls is required to be provided by the developer of the information system, system component, or information system services. DoD has determined the level of detail is not appropriate to define at the Enterprise level.	MOD		X	X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(2)	CCI-003106	The organization defines the level of detail the implementation information of the security controls is required to be provided by the developer of the information system, system component, or information system services.	The organization being inspected/assessed defines and documents the level of detail the implementation information of the security controls is required to be provided by the developer of the information system, system component, or information system services. DoD has determined the level of detail is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented level of detail to ensure the organization being inspected/assessed defines the level of detail the implementation information of the security controls is required to be provided by the developer of the information system, system component, or information system services. DoD has determined the level of detail is not appropriate to define at the Enterprise level.	MOD		X	X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(9)	CCI-003114	The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	The organization being inspected/assessed documents within contracts/agreements, the requirement that the developer of the information system, system component, or information system service identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. Ports identified shall be assessed and planned for in light of DISA's PPSM requirements.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	MOD		X	X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-4(10)	CCI-003116	The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.	The organization being inspected/assessed employs DoD approved PKI tokens for identity verification.	The organization conducting the inspection/assessment examines the information system to ensure DoD approved PKI tokens are implemented for identity verification.	LOW	X	X		X				3.12 FIPS 201-2 REQUIREMENT		CCI requirements are addressed within subparagraph "FIPS 201-2 Requirement" of UFGS 25 05 11.
N/A	MA-4(6)	CCI-003123	The information system implements cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 3123.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 3123.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-5(a)(1)	CCI-003124	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure configuration of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.2.1 HVAC Control System Devices FULLY S... 1.9.8.2.2 All Other HVAC Control System Devic... 1.9.8.3.1 Lighting Control System Devices FUL... 1.9.8.3.2 All Other Lighting Control System D... 1.9.8.5 Default Requirements for Control Sy...		Requirement is met in "Control System Cybersecurity Documentation"
N/A	SA-5(a)(1)	CCI-003125	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure installation of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure installation of the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure installation of the system, component, or service.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.5 Default Requirements for Control Sy...		Requirement is met in "Control System Cybersecurity Documentation"
N/A	SA-5(a)(1)	CCI-003126	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure operation of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure operation of the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure operation of the system, component, or service.	LOW		X	X					1.9.8 Control System Cybersecurity Docume...		Requirement is met in "Control System Cybersecurity Documentation"
N/A	SA-5(a)(2)	CCI-003127	The organization obtains administrator documentation for the information system, system component, or information system services that describes effective use and maintenance of security functions/mechanisms.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe effective use and maintenance of security functions/mechanisms.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe effective use and maintenance of security functions/mechanisms.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.1 Software Applications 1.9.8.2.1 HVAC Control System Devices FULLY S... 1.9.8.2.2 All Other HVAC Control System Devic... 1.9.8.3.1 Lighting Control System Devices FUL... 1.9.8.3.2 All Other Lighting Control System D... 1.9.8.5 Default Requirements for Control Sy...		Requirement is met in "Control System Cybersecurity Documentation"
N/A	SA-5(a)(3)	CCI-003128	The organization obtains administrator documentation for the information system, system component, or information system services that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide administrator documentation for the information system, system component or information system service that describe known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.1 Software Applications 1.9.8.2.1 HVAC Control System Devices FULLY S... 1.9.8.3.1 Lighting Control System Devices FUL... 1.9.8.5 Default Requirements for Control Sy...		Requirement is met in "Control System Cybersecurity Documentation"
N/A	SA-5(b)(1)	CCI-003129	The organization obtains user documentation for the information system, system component, or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide user documentation for the information system, system component or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.1 Software Applications 1.9.8.2.1 HVAC Control System Devices FULLY S... 1.9.8.3.1 Lighting Control System Devices FUL... 1.9.8.5 Default Requirements for Control Sy...		Requirement is met in "Control System Cybersecurity Documentation"
N/A	SA-5(b)(2)	CCI-003130	The organization obtains user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.1 Software Applications 1.9.8.2.1 HVAC Control System Devices FULLY S... 1.9.8.2.2 All Other HVAC Control System Devic... 1.9.8.3.1 Lighting Control System Devices FUL... 1.9.8.3.2 All Other Lighting Control System D... 1.9.8.5 Default Requirements for Control Sy...		Requirement is met in "Control System Cybersecurity Documentation"
N/A	SA-5(b)(3)	CCI-003131	The organization obtains user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer provide user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service.	LOW		X	X					1.9.8 Control System Cybersecurity Docume... 1.9.8.1 Software Applications		Requirement is met in "Control System Cybersecurity Documentation"

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-5(c)	CCI-003132	The organization takes organization-defined actions in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service.	The organization being inspected/assessed takes actions defined in SA-5, CCI 3133 in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service. The organization must maintain a record of actions taken. DoD has determined the actions are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the record of actions taken to ensure the organization being inspected/assessed takes actions defined in SA-5, CCI 3133 in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service. DoD has determined the actions are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-5(c)	CCI-003133	The organization defines actions to be taken in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service.	The organization being inspected/assessed defines and documents actions to be taken in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service. DoD has determined the actions are not appropriate to define at the Enterprise level.	The organization conducting inspection/assessment obtains and examines the documented actions to ensure the organization being inspected/assessed defines action to be taken in response to attempts to obtain either unavailable or nonexistent documentation for information system, system component, or information system service. DoD has determined the actions are not appropriate to define at the Enterprise level.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-5(d)	CCI-003134	The organization protects information system, system component, or information system service documentation as required, in accordance with the risk management strategy.	The organization being inspected/assessed documents and implements processes to store and handle information system, system component, or information system service documentation as required, in accordance with the risk management strategy.	The organization conducting the inspection/assessment obtains and examines the documented processes to ensure the organization being inspected/assessed stores and handles information system, system component, or information system service documentation as required, in accordance with the risk management strategy.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-5(e)	CCI-003135	The organization distributes information system, system component, or information system service documentation to organization-defined personnel or roles.	The organization being inspected/assessed distributes information system, system component, or information system service documentation to at a minimum, the ISSO, ISSM, and SCA, via an information sharing capability. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA.	The organization conducting the inspection/assessment obtains and examines the information system, system component, or information system service documentation via the organization's information sharing capability to ensure the organization being inspected/assessed distributes information system, system component, or information system service documentation to at a minimum, the ISSO, ISSM, and SCA. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA.	LOW			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-5(e)	CCI-003136	The organization defines the personnel or roles the information system, system component, or information system service documentation is to be distributed.	DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and SCA.	LOW				X				---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-9(a)	CCI-003137	The organization defines security controls that providers of external information system services employ in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	DoD has defined the security controls as security controls defined by CNSSI 1253.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the security controls as security controls defined by CNSSI 1253.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-9(c)	CCI-003138	The organization employs organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.	The organization being inspected/assessed implements the processes, methods, and techniques defined in SA-9, CCI 3139 to monitor security control compliance by external service providers on an ongoing basis. The organization must maintain records of monitoring.	The organization conducting the inspection/assessment obtains and examines the records of monitoring to ensure the organization being inspected/assessed implements the processes, methods, and techniques defined in SA-9, CCI 3139 to monitor security control compliance by external service providers on an ongoing basis.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-9(c)	CCI-003139	The organization defines processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis.	The organization being inspected/assessed defines and documents processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis. DoD has determined the processes, methods, and techniques are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented processes, methods, and techniques to ensure the organization being inspected/assessed defines processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis.	LOW	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-9(1)(a)	CCI-003140	The organization conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services.	The organization being inspected/assessed documents and implements a process to conduct an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services. The organization must maintain a record of risk assessment.	The organization conducting the inspection/assessment obtains and examines a list of acquired or outsourced information security services and the record of risk assessment to ensure the organization being inspected/assessed conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-9(1)(b)	CCI-003141	The organization ensures that the acquisition or outsourcing of dedicated information security services is approved by organization-defined personnel or roles.	The organization being inspected/assessed ensures that the acquisition or outsourcing of dedicated information security services is approved by the DoD Component CIO or their delegate(s). The organization must maintain a record of approvals. DoD has defined the personnel or roles the DoD Component CIO or their delegate(s).	The organization conducting the inspection/assessment obtains and examines a list of acquired or outsourced information security services as well as the record of approvals to ensure the organization being inspected/assessed ensures that the acquisition or outsourcing of dedicated information security services is approved by the DoD Component CIO or their delegate(s). DoD has defined the personnel or roles the DoD Component CIO or their delegate(s).	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-9(1)(b)	CCI-003142	The organization defines the personnel or roles authorized to approve the acquisition or outsourcing of dedicated information security services.	DoD has defined the personnel or roles the DoD Component CIO or their delegate(s).	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles the DoD Component CIO or their delegate(s).	MOD			X		X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
N/A	SA-9(2)	CCI-003143	The organization requires providers of organization-defined external information system services to identify the functions, ports, protocols, and other services required for the use of such services.	The organization being inspected/assessed documents within contracts/agreements, the requirement that providers of all external information system services identify the functions, ports, protocols, and other services required for the use of such services. DoD has defined the external information system services as all external information system services.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that providers of all external information system services identify the functions, ports, protocols, and other services required for the use of such services. DoD has defined the external information system services as all external information system services.	MOD	X		X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-9(2)	CCI-003144	The organization defines the external information system services for which the providers are required to identify the functions, ports, protocols, and other services required for the use of such services.	DoD has defined the external information system services as all external information system services.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the external information system services as all external information system services.	MOD	X				X			---	Per UFC 4-10-060 this CCI is considered DoD Defined and will not be addressed within the Cybersecurity Design as it is covered at the DoD level.	
SI-7	SA-10(a)	CCI-003155	The organization requires the developer of the information system, system component, or information system service to perform configuration management during system, component or service design, development, implementation and/or operation.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service perform configuration management during system, component or service design, development, implementation and/or operation. The configuration management process applies to: 1. Documentation developed or used in the lifecycle, including requirements and interface specifications; 2. Elements including design libraries; 3. Tools including design tools and test tools; 4. Technical data including test data; and 5. Information on element and system lifecycle processes	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires the developer of the information system, system component, or information system service perform configuration management during system, component or service design, development, implementation and/or operation.	MOD		X	X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-10(b)	CCI-003156	The organization requires the developer of the information system, system component, or information system service to document the integrity of changes to organization-defined configuration items under configuration management.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service document the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.	MOD		X	X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-10(b)	CCI-003157	The organization requires the developer of the information system, system component, or information system service to manage the integrity of changes to organization-defined configuration items under configuration management.	The organization being inspected/assessed requires within contracts/agreements the requirement that the developer of the information system, system component, or information system service manage the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service manage the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.	MOD		X	X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-10(b)	CCI-003158	The organization requires the developer of the information system, system component, or information system service to control the integrity of changes to organization-defined configuration items under configuration management.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service control the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service control the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.	MOD		X	X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-10(b)	CCI-003159	The organization defines the configuration items under configuration management that require the integrity of changes to be documented, managed and controlled.	The organization being inspected/assessed defines and documents the configuration items under configuration management that require the integrity of changes to be documented, managed and controlled. DoD has determined the configuration items are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented configuration items to ensure the organization being inspected/assessed defines the configuration items under configuration management that require the integrity of changes to be documented, managed and controlled. DoD has determined the configuration items are not appropriate to define at the Enterprise level.	MOD		X	X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-10(d)	CCI-003160	The organization requires the developer of the information system, system component, or information system service to document the potential security impacts of approved changes to the system, component, or service.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service document the potential security impacts of approved changes to the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document the potential security impacts of approved changes to the system, component, or service.	MOD		X	X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-10(e)	CCI-003161	The organization requires the developer of the information system, system component, or information system service to track security flaws within the system, component, or service.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service track security flaws within the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service track security flaws within the system, component, or service.	MOD		X	X	X				---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system...The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-10(e)	CCI-003162	The organization requires the developer of the information system, system component, or information system service to track flaw resolution within the system, component, or service.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service track flaw resolution within the system, component, or service.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service track flaw resolution within the system, component, or service.	MOD		X	X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-10(e)	CCI-003163	The organization requires the developer of the information system, system component, or information system service to report security flaws and flaw resolution within the system, component, or service findings to organization-defined personnel.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service report security flaws and flaw resolution within the system, component, or service findings to at a minimum, the ISSO and ISSM. DoD has defined the personnel as at a minimum, the ISSO and ISSM.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service report security flaws and flaw resolution within the system, component, or service findings to at a minimum, the ISSO and ISSM. DoD has defined the personnel as at a minimum, the ISSO and ISSM.	MOD		X	X	X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-10(e)	CCI-003164	The organization defines the personnel to whom security flaw findings and flaw resolution within the system, component, or service are reported.	DoD has defined the personnel as at a minimum, the ISSO and ISSM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel as at a minimum, the ISSO and ISSM.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
PM-5	SA-11(a)	CCI-003171	The organization requires the developer of the information system, system component, or information system service to create a security assessment plan.	The organization being inspected/assessed requires that the developer create and document a security assessment plan that includes: 1. The types of analyses, testing, evaluation, and reviews of software and firmware components; 2. The degree of rigor to be applied; and 3. The types of artifacts produced during those processes.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service create a security assessment plan.	MOD		X	X	X				3.14 CONTROL SYSTEM CYBERSECURITY TESTIN...		CCI requirements are addressed within subparagraph "CONTROL SYSTEM CYBERSECURITY TESTING" of UFGS 25 05 11.
N/A	SA-11(a)	CCI-003172	The organization requires the developer of the information system, system component, or information system service to implement a security assessment plan.	The organization being inspected/assessed requires that the developer implement the security assessment plan developed in SA-11, CCI 003171.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service implement a security assessment plan.	MOD		X	X	X				3.14 CONTROL SYSTEM CYBERSECURITY TESTIN...		CCI requirements are addressed within subparagraph "CONTROL SYSTEM CYBERSECURITY TESTING" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-11(b)	CCI-003173	The organization requires the developer of the information system, system component, or information system service to perform unit, integration, system, and/or regression testing/evaluation at organization-defined depth and coverage.	The organization being inspected/assessed documents within the contracts/agreements, the requirement that the developer of the information system, system component, or information system service perform unit, integration, system, and/or regression testing/evaluation at depth and coverage defined in SA-11, CCI 3174.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service perform unit, integration, system, and/or regression testing/evaluation at depth and coverage defined in SA-11, CCI 3174.	MOD		X	X	X				3.14 CONTROL SYSTEM CYBERSECURITY TESTIN...		CCI requirements are addressed within subparagraph "CONTROL SYSTEM CYBERSECURITY TESTING" of UFGS 25 05 11.
N/A	SA-11(b)	CCI-003174	The organization defines the depth and coverage to perform unit, integration, system, and/or regression testing/evaluation.	The organization being inspected/assessed defines and documents the depth and coverage to perform unit, integration, system, and/or regression testing/evaluation. Examples of approaches or tool types that could be required are: 1. Approaches such as static analyses, dynamic analyses, binary analysis, or a hybrid of the three approaches; and 2. Tools such as web-based application scanners, static analysis tools, binary analyzers. DoD has determined the depth and coverage are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented depth and coverage to ensure the organization being inspected/assessed defines the depth and coverage to perform unit, integration, system, and/or regression testing/evaluation. DoD has determined the depth and coverage are not appropriate to define at the Enterprise level.	MOD		X	X	X				3.14 CONTROL SYSTEM CYBERSECURITY TESTIN...		CCI requirements are addressed within subparagraph "CONTROL SYSTEM CYBERSECURITY TESTING" of UFGS 25 05 11.
N/A	SA-11(c)	CCI-003175	The organization requires the developer of the information system, system component, or information system service to produce evidence of the execution of the security assessment plan.	The organization being inspected/assessed requires the developer to produce and provide evidence of the execution of the security assessment plan.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service produce evidence of the execution of the security assessment plan.	MOD		X	X	X				3.14 CONTROL SYSTEM CYBERSECURITY TESTIN...		CCI requirements are addressed within subparagraph "CONTROL SYSTEM CYBERSECURITY TESTING" of UFGS 25 05 11.
N/A	SA-11(c)	CCI-003176	The organization requires the developer of the information system, system component, or information system service to produce the results of the security testing/evaluation.	The organization being inspected/assessed requires the developer to produce and provide results of the security testing/evaluation.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service produce the results of the security testing/evaluation.	MOD		X	X	X				3.14 CONTROL SYSTEM CYBERSECURITY TESTIN...		CCI requirements are addressed within subparagraph "CONTROL SYSTEM CYBERSECURITY TESTING" of UFGS 25 05 11.
N/A	SA-11(d)	CCI-003177	The organization requires the developer of the information system, system component, or information system service to implement a verifiable flaw remediation process.	The organization being inspected/assessed requires the developer to implement a verifiable flaw remediation process.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service implement a verifiable flaw remediation process.	MOD		X	X	X				3.14 CONTROL SYSTEM CYBERSECURITY TESTIN...		CCI requirements are addressed within subparagraph "CONTROL SYSTEM CYBERSECURITY TESTING" of UFGS 25 05 11.
N/A	SA-11(e)	CCI-003178	The organization requires the developer of the information system, system component, or information system service to correct flaws identified during security testing/evaluation.	The organization being inspected/assessed requires the developer to correct flaws identified during security testing/evaluation and to document and provide evidence that the flaws were corrected.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service correct flaws identified during security testing/evaluation and provide evidence.	MOD		X	X	X				3.14 CONTROL SYSTEM CYBERSECURITY TESTIN...		CCI requirements are addressed within subparagraph "CONTROL SYSTEM CYBERSECURITY TESTING" of UFGS 25 05 11.
N/A	SA-15	CCI-003233	The organization requires the developer of the information system, system component, or information system service to follow a documented development process.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service to follow a documented development process.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service to follow a documented development process.	MOD		X		X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-15(a)(1)	CCI-003234	The documented information system, system component, or information system service development process explicitly addresses security requirements.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service explicitly addresses security requirements.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service explicitly addresses security requirements.	MOD		X		X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-15(a)(2)	CCI-003235	The documented information system, system component, or information system service development process identifies the standards used in the development process.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service identifies the standards used in the development process, for example, programming languages and computer-aided design (CAD) systems.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service identifies the standards used in the development process.	MOD		X		X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-15(a)(2)	CCI-003236	The documented information system, system component, or information system service development process identifies the tools used in the development process.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service identifies the tools used in the development process, for example, programming languages and computer-aided design (CAD) systems.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service identifies the tools used in the development process.	MOD		X		X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-15(a)(3)	CCI-003237	The documented information system, system component, or information system service development process documents the specific tool options and tool configurations used in the development process.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service documents the specific tool options and tool configurations used in the development process.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service documents the specific tool options and tool configurations used in the development process.	MOD		X		X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-15(a)(4)	CCI-003238	The documented information system, system component, or information system service development process documents changes to the process and/or tools used in development.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service documents changes to the process and/or tools used in development.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service documents changes to the process and/or tools used in development.	MOD		X		X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-15(a)(4)	CCI-003239	The documented information system, system component, or information system service development process manages changes to the process and/or tools used in development.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service document a process to manage changes to the process and/or tools used in development.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document a process to manage changes to the process and/or tools used in development.	MOD		X		X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	
N/A	SA-15(a)(4)	CCI-003240	The documented information system, system component, or information system service development process ensures the integrity of changes to the process and/or tools used in development.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service document the integrity of changes to the process and/or tools used in development.	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being inspected/assessed requires that the developer of the information system, system component, or information system service document the integrity of changes to the process and/or tools used in development.	MOD		X		X				---	Per UFC 4-10-060 this CCI is considered Impractical and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-15(b)	CCI-003241	The organization reviews the development process in accordance with organization-defined frequency to determine if the development process selected and employed can satisfy organization-defined security requirements.	The organization being inspected/assessed documents and implements a process to review the development process before first use and annually thereafter to determine if the development process selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. Reviews of development processes can include, for example, the use of capability maturity model integration (CMMI) to determine the potential effectiveness of such processes. The organization must maintain a record of reviews. DoD has defined the frequency as before first use and annually thereafter.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the development process before first use and annually thereafter to determine if the development process selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. DoD has defined the frequency as before first use and annually thereafter.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-15(b)	CCI-003242	The organization reviews the development standards in accordance with organization-defined frequency to determine if the development standards selected and employed can satisfy organization-defined security requirements.	The organization being inspected/assessed documents and implements a process to review the development standards before first use and annually thereafter to determine if the development standards selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. The organization must maintain a record of reviews. DoD has defined the frequency as before first use and annually thereafter.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the development standards before first use and annually thereafter to determine if the development standards selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. DoD has defined the frequency as before first use and annually thereafter.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-15(b)	CCI-003243	The organization reviews the development tools in accordance with organization-defined frequency to determine if the development tools selected and employed can satisfy organization-defined security requirements.	The organization being inspected/assessed documents and implements a process to review the development tools before first use and annually thereafter to determine if the development tools selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. The organization must maintain a record of reviews. DoD has defined the frequency as before first use and annually thereafter.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the development tools before first use and annually thereafter to determine if the development tools selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. DoD has defined the frequency as before first use and annually thereafter.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-15(b)	CCI-003244	The organization reviews the development tool options/configurations in accordance with organization-defined frequency to determine if the development tool options/configurations selected and employed can satisfy organization-defined security requirements.	The organization being inspected/assessed documents and implements a process to review the development tool options/configurations before first use and annually thereafter to determine if the development tool options/configurations selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. The organization must maintain a record of reviews. DoD has defined the frequency as before first use and annually thereafter.	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the development tool options/configurations before first use and annually thereafter to determine if the development tool options/configurations selected and employed can satisfy the security requirements defined in SA-15, CCI 3246. DoD has defined the frequency as before first use and annually thereafter.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-15(b)	CCI-003245	The organization defines the frequency on which to review the development process, standards, tools, and tool options/configurations to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy organization-defined security requirements.	DoD has defined the frequency as before first use and annually thereafter.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as before first use and annually thereafter.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-15(b)	CCI-003246	The organization defines the security requirements that must be satisfied by conducting a review of the development process, standards, tools, and tool options/configurations.	The organization being inspected/assessed defines and documents the security requirements that must be satisfied by conducting a review of the development process, standards, tools, and tool options/configurations. DoD has determined the security requirements are not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented security requirements to ensure the organization being inspected/assessed defines the security requirements that must be satisfied by conducting a review of the development process, standards, tools, and tool options/configurations. DoD has determined the security requirements are not appropriate to define at the Enterprise level.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-19(a)	CCI-003356	The organization develops anti-counterfeit policy that include the means to detect counterfeit components from entering the information system.	The organization being inspected/assessed develops and documents an anti-counterfeit policy that include the means to detect counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit policy to ensure the organization being inspected/assessed develops an anti-counterfeit policy that include the means to detect counterfeit components from entering the information system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-19(a)	CCI-003357	The organization develops anti-counterfeit policy that include the means to prevent counterfeit components from entering the information system.	The organization being inspected/assessed develops and documents an anti-counterfeit policy that include the means to prevent counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit policy to ensure the organization being inspected/assessed develops an anti-counterfeit policy that include the means to prevent counterfeit components from entering the information system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-19(a)	CCI-003358	The organization develops anti-counterfeit procedures that include the means to detect counterfeit components from entering the information system.	The organization being inspected/assessed develops and documents anti-counterfeit procedures that include the means to detect counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit procedures to ensure the organization being inspected/assessed develops anti-counterfeit procedures that include the means to detect counterfeit components from entering the information system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-19(a)	CCI-003359	The organization develops anti-counterfeit procedures that include the means to prevent counterfeit components from entering the information system.	The organization being inspected/assessed develops and documents anti-counterfeit procedures that include the means to prevent counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit procedures to ensure the organization being inspected/assessed develops anti-counterfeit procedures that include the means to prevent counterfeit components from entering the information system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-19(a)	CCI-003360	The organization implements anti-counterfeit policy that include the means to detect counterfeit components from entering the information system.	The organization being inspected/assessed implements the policy defined in SA-19, CCIs 3356 that include the means to detect counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the policy defined in SA-19, CCIs 3356 and any artifacts applicable to counterfeit components to ensure the organization being inspected/assessed implements the policy defined in SA-19, CCIs 3356 that include the means to detect counterfeit components from entering the information system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table 4-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion when Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SA-19(a)	CCI-003361	The organization implements anti-counterfeit policy that include the means to prevent counterfeit components from entering the information system.	The organization being inspected/assessed implements the policy defined in SA-19, CCIs 3357 that include the means to prevent counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the policy defined in SA-19, CCIs 3357 and any artifacts applicable to counterfeit components to ensure the organization being inspected/assessed implements the policy defined in SA-19, CCIs 3357 that include the means to detect counterfeit components from entering the information system.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	SA-19(a)	CCI-003362	The organization implements anti-counterfeit procedures that include the means to detect counterfeit components from entering the information system.	The organization being inspected/assessed implements the procedures defined in SA-19, CCIs 3358 that include the means to detect counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the procedures defined in SA-19, CCIs 3358 and any artifacts applicable to counterfeit components to ensure the organization being inspected/assessed implements the procedures defined in SA-19, CCIs 3358 that include the means to detect counterfeit components from entering the information system.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-19(a)	CCI-003363	The organization implements anti-counterfeit procedures that include the means to prevent counterfeit components from entering the information system.	The organization being inspected/assessed implements the procedures defined in SA-19, CCIs 3359 that include the means to prevent counterfeit components from entering the information system.	The organization conducting the inspection/assessment obtains and examines the procedures defined in SA-19, CCIs 3359 and any artifacts applicable to counterfeit components to ensure the organization being inspected/assessed implements the procedures defined in SA-19, CCIs 3359 that include the means to prevent counterfeit components from entering the information system.	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-19(b)	CCI-003365	The organization defines the external reporting organizations to whom counterfeit information system components are to be reported.	DoD has defined the external reporting organizations as at a minimum, USCYBERCOM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the external reporting organizations as at a minimum, USCYBERCOM	MOD			X					---	Per UFC 4-010-06 Table G-7 and Section 3-5; "The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system…The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others."	
N/A	SA-19(b)	CCI-003366	The organization defines the personnel or roles to whom counterfeit information system components are to be reported.	DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and PM.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as at a minimum, the ISSO, ISSM, and PM.	MOD			X					---	Per UFC 4-10-060 this CCI is considered Non-Designer and will not be addressed within the Cybersecurity Design.	
N/A	PL-7 (a)	CCI-003071	The organization develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security.	The organization being inspected/assessed develops and documents a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security.	The organization conducting the inspection/assessment obtains and examines the security CONOPS to ensure the organization being inspected/assessed develops a security CONOPS for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security.	LOW		X						1.9 Cybersecurity Documentation		Default requirement in UFGS 25 05 11 for "Cybersecurity Documentation"
N/A	SA-22 (b)	CCI-003374	The organization documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	The organization being inspected/assessed documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	The organization conducting the inspection/assessment obtains and examines the hardware and software lists as well as the documented approvals to ensure the organization being inspected/assessed documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	LOW		X						1.9.8 Control System Cybersecurity Documentation		Requirement is met in "Control System Cybersecurity Documentation"
N/A	AC-11 (1)	CCI-000060	The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	The organization being inspected/assessed configures the information system to conceal, via the session lock, information previously visible on the display with a publicly viewable image. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 60.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to conceal, via the session lock, information previously visible on the display with a publicly viewable image. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 60.	MOD		X		X				3.3.4 Session Lock and Session Termination Requirements In MODERATE Impact Systems		CCI requirements are addressed within subparagraph "Session Lock and Session Termination Requirements In MODERATE Impact Systems:" of UFGS 25 05 11.
N/A	PE-5	CCI-000937	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	The organization being inspected/assessed will identify, document, and execute any additional access controls required for output devices above and beyond physical access controls already in place for the facility IAW DoD 5200.08-R and DoD 5200.01-M (Volumes 1-4).	The organization conducting the inspection/assessment obtains and examines the list of additional access controls for output devices. Physical inspection is required to ensure these access controls are properly implemented.	MOD				X				3.3.6 Physical Security in MODERATE Impact Systems		CCI requirements are addressed within subparagraph "Physical Security in MODERATE Impact Systems" of UFGS 25 05 11.
N/A	AU-14 (3)	CCI-001920	The information system provides the capability for authorized users to remotely view/hear all content related to an established user session in real time.	The organization being inspected/assessed configures the information system to provide the capability for authorized users to remotely view/hear all content related to an established user session in real time. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1920.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to provide the capability for authorized users to remotely view/hear all content related to an established user session in real time. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1920.	LOW		X						3.5.1 Audit Events, Content of Audit Records, and Audit Generation		CCI requirements are met within subparagraph "Audit Events, Contents of Audit Records, and Audit Generation" of UFGS 25 05 11.
N/A	PE-9 (1)	CCI-002953	The organization employs redundant power cabling paths that are physically separated by organization-defined distance.	The organization being inspected/assessed employs redundant power cabling paths that are physically separated by the distance defined in PE-9 (1), CCI 2954.	The organization conducting the inspection/assessment obtains and examines cabling diagrams or, if unavailable, inspects power cabling configuration to ensure the organization being inspected/assessed employs redundant power cabling paths that are physically separated by the distance defined in PE-9 (1), CCI 2954.	MOD				X				3.10 Device Power		CCI requirements are addressed within subparagraph "Device Power" of UFGS 25 05 11.
N/A	PE-9 (1)	CCI-002954	The organization defines the distance to physically separate redundant power cabling paths.	The organization being inspected/assessed defines and documents the distance to physically separate redundant power cabling paths. DoD has determined the distance is not appropriate to define at the Enterprise level.	The organization conducting the inspection/assessment obtains and examines the documented distance to ensure the organization being inspected/assessed defines the distance to physically separate redundant power cabling paths. DoD has determined the distance is not appropriate to define at the Enterprise level.	MOD				X				3.10 Device Power		CCI requirements are addressed within subparagraph "Device Power" of UFGS 25 05 11.
N/A	CM-5 (3)	CCI-001749	The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.	The organization being inspected/assessed documents and implements a process to prevent the installation of software onto any software components when the vendor provides digitally signed products without verification that software has been digitally signed using a certificate and approved by the organization. DoD has defined the software components as any software components when the vendor provides digitally signed products.	The organization conducting the inspection/assessment obtains and examines the documented process for preventing the installation of software onto any software components when the vendor provides digitally signed products without verification that software has been digitally signed using a certificate and approved by the organization. The organization conducting the inspection/assessment reviews software on a sampling of the defined components to ensure that only software digitally signed by a defined CA is installed. DoD has defined the software components as any software components when the vendor provides digitally signed products.	MOD	X	X						3.13.2 Software, Firmware, and Information Integrity In MODERATE Impact Systems		CCI requirements are addressed within subparagraph "Software, Firmware, and Information Integrity In MODERATE Impact Systems" of UFGS 25 05 11.

AFCEC Security Controls	Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applies at or Below	Enclave	Designer	Non -Designer	Impacted/	DoD Defined	Removed from Low baseline	Rationale for removal from Low baseline UFC Table H-3	UFGS 25 05 11 - Reference	Rational for Non-Inclusion within Cybersecurity Design	CCIs incorporated into the UFGS 25 05 11 for the Control System (Include Paragraph Name)
N/A	SI-7 (9)	CCI-002726	The information system verifies the integrity of the boot process of organization-defined devices.	The organization being inspected/assessed configures the information system to verify the integrity of the boot process of all devices capable of verification of the boot process. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2726. DoD has defined the devices as all devices capable of verification of the boot process.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to verify the integrity of the boot process of all devices capable of verification of the boot process. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2726. DoD has defined the devices as all devices capable of verification of the boot process.	MOD	X	X						3.13.2 Software, Firmware, and Information Integrity In MODERATE Impact Systems		CCI requirements are addressed within subparagraph "Software, Firmware, and Information Integrity In MODERATE Impact Systems" of UFGS 25 05 11.

SECTION TABLE OF CONTENTS

DIVISION 26 - ELECTRICAL

SECTION 26 05 00.00 40

COMMON WORK RESULTS FOR ELECTRICAL

PART 1 GENERAL

1.1 REFERENCES
1.2 DEFINITIONS
1.3 SUBMITTALS
1.4 QUALITY CONTROL
1.4.1 Regulatory Requirements
1.4.2 Standard Products

PART 2 PRODUCTS

2.1 EQUIPMENT
2.1.1 Conduits and Raceways
2.1.1.1 Rigid Steel Conduit
2.1.1.2 Electrical Metallic Tubing (EMT)
2.1.1.3 Flexible Metallic Conduit
2.1.1.4 Intermediate Metal Conduit
2.1.1.5 Rigid Nonmetallic Conduit
2.1.1.6 Surface Metal Raceway
2.1.1.7 Surface Nonmetallic Raceway
2.1.2 Wireways
2.1.3 Cable Trays
2.1.4 Outlet Boxes, Pull Boxes and Junction Boxes
2.1.5 Panelboards
2.1.5.1 Circuit Breakers
2.1.6 Dry-Type Distribution Transformers
2.1.6.1 General Requirements
2.1.6.2 Transformer Factory Tests
2.2 MATERIALS
2.2.1 Wire And Cable
2.2.1.1 Insulation
2.2.1.2 Wire and Cable for 400 Hertz (Hz) Circuits
2.2.1.3 Metal-Clad Cable
2.2.1.4 Armored Cable
2.2.1.5 Mineral-Insulated, Metal-Sheathed Cable
2.2.1.6 Cable Tray Cable or Power Limited Tray Cable
2.2.1.7 Cord Sets and Power-Supply Cords
2.2.2 Device Plates
2.2.3 Switches
2.2.3.1 Safety Switches
2.2.3.2 Toggle Switches
2.2.4 Fuses
2.2.4.1 Fuseholders
2.2.4.2 Cartridge, Current Limiting Type (Class R)
2.2.4.3 Cartridge Fuses, High-Interrupting Capacity, Current Limiting Type (Classes J, L, and CC)

2.2.4.4 Cartridge Fuses, Current Limiting Type (Class T)
2.2.5 Receptacles
2.2.5.1 Switched Duplex Receptacles
2.2.5.2 Weatherproof Receptacles
2.2.5.3 Ground-Fault Circuit Interrupter Receptacles
2.2.5.4 Tamper-Resistant Receptacles
2.2.6 Manufacturer's Nameplate
2.2.7 Warning Signs
2.2.8 Firestopping Materials
2.2.9 Metering
2.2.10 Surge Protective Devices

PART 3 EXECUTION

3.1 PREPARATION
3.2 INSTALLATION
3.2.1 Underground Service
3.2.2 Overhead Service
3.2.3 Hazardous Locations
3.2.4 Service Entrance Identification
3.2.5 Labels
3.2.6 Wiring Methods
3.2.6.1 Pull Wire
3.2.6.2 Metal Clad Cable
3.2.6.3 Armored Cable
3.2.6.4 Mineral Insulated, Metal Sheathed (Type MI) Cable Installation
3.2.7 Conduits, Raceways and Fittings
3.2.7.1 Rigid Steel Conduit
3.2.7.2 Electrical Metallic Tubing (EMT)
3.2.7.3 Flexible Metallic Conduit
3.2.7.4 Intermediate Conduit
3.2.7.5 Rigid Nonmetallic Conduit
3.2.7.6 Underground Conduit
3.2.7.7 Conduit for Circuits Rated Greater Than 600 Volts
3.2.7.8 Conduit Installed Under Floor Slabs
3.2.7.9 Conduit Installed Through Floor Slabs
3.2.7.10 Conduit Installed in Concrete Floor Slabs
3.2.7.11 Stub Ups
3.2.7.12 Conduit Support
3.2.7.13 Directional Changes in Conduit Runs
3.2.7.14 Wireway and Auxiliary Gutter
3.2.7.15 Surface Raceways and Assemblies
3.2.7.16 Cable Trays
3.2.8 Wiring
3.2.9 Wiring Devices
3.2.9.1 Wall Switches and Receptacles
3.2.9.2 Device Plates
3.2.10 Splices and Connectors
3.2.11 Conductor Identification
3.2.11.1 Marking Strips
3.2.12 Safety Switches
3.2.13 Boxes and Fittings
3.2.14 Covers and Device Plates
3.2.15 Electrical Penetrations
3.2.16 Panelboards
3.2.17 Dry-Type Distribution Transformers
3.2.18 Surge Protective Devices
3.2.19 Field Fabricated Nameplates

3.2.20 Identification Plates and Warnings
3.3 FIELD FABRICATED NAMEPLATE MOUNTING
3.4 WARNING SIGN MOUNTING
3.5 FIELD APPLIED MOUNTING
3.6 FIELD QUALITY CONTROL

-- End of Section Table of Contents --

SECTION 26 05 00.00 40

COMMON WORK RESULTS FOR ELECTRICAL

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

ANSI C12.1	(2014; Errata 2016) Electric Meters - Code for Electricity Metering

AMERICAN SOCIETY OF CIVIL ENGINEERS (ASCE)

ASCE 7-16	(2017; Errata 2018; Supp 1 2018) Minimum Design Loads and Associated Criteria for Buildings and Other Structures

ASTM INTERNATIONAL (ASTM)

ASTM D709	(2017) Standard Specification for Laminated Thermosetting Materials

ELECTRONIC INDUSTRIES ALLIANCE (EIA)

EIA 480	(1981) Toggle Switches

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE C57.12.28	(2014) Standard for Pad-Mounted Equipment - Enclosure Integrity
IEEE Stds Dictionary	(2009) IEEE Standards Dictionary: Glossary of Terms & Definitions

INTERNATIONAL CODE COUNCIL (ICC)

ICC/ANSI A117.1	(2009) Accessible and Usable Buildings and Facilities

INTERNATIONAL ELECTRICAL TESTING ASSOCIATION (NETA)

NETA ATS	(2021) Standard for Acceptance Testing Specifications for Electrical Power Equipment and Systems

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

ANSI C12.7	(2022) Requirements for Watthour Meter Sockets

ANSI C80.1	(2020) American National Standard for Electrical Rigid Steel Conduit (ERSC)
ANSI C80.3	(2020) American National Standard for Electrical Metallic Tubing (EMT)
ANSI Z535.1	(2017) Safety Colors
ANSI/NEMA OS 1	(2013; R 2020) Sheet-Steel Outlet Boxes, Device Boxes, Covers, and Box Supports
NEMA 250	(2020) Enclosures for Electrical Equipment (1000 Volts Maximum)
NEMA AB 3	(2013) Molded Case Circuit Breakers and Their Application
NEMA FB 1	(2014) Standard for Fittings, Cast Metal Boxes, and Conduit Bodies for Conduit, Electrical Metallic Tubing, and Cable
NEMA FU 1	(2012) Low Voltage Cartridge Fuses
NEMA ICS 1	(2000; R 2015) Standard for Industrial Control and Systems: General Requirements
NEMA ICS 6	(1993; R 2016) Industrial Control and Systems: Enclosures
NEMA KS 1	(2013) Enclosed and Miscellaneous Distribution Equipment Switches (600 V Maximum)
NEMA PB 1	(2011) Panelboards
NEMA RN 1	(2005; R 2013) Polyvinyl-Chloride (PVC) Externally Coated Galvanized Rigid Steel Conduit and Intermediate Metal Conduit
NEMA ST 20	(2014) Dry-Type Transformers for General Applications
NEMA TC 2	(2020) Standard for Electrical Polyvinyl Chloride (PVC) Conduit
NEMA TC 3	(2021) Polyvinyl Chloride (PVC) Fittings for Use With Rigid PVC Conduit and Tubing
NEMA VE 1	(2017) Metal Cable Tray Systems
NEMA WD 1	(1999; R 2020) Standard for General Color Requirements for Wiring Devices
NEMA WD 6	(2021) Wiring Devices Dimensions Specifications

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National

	Electrical Code
NFPA 70E	(2021) Standard for Electrical Safety in the Workplace

UNDERWRITERS LABORATORIES (UL)

UL 1	(2005; Reprint Jan 2020) UL Standard for Safety Flexible Metal Conduit
UL 4	(2004; Reprint Mar 2021) UL Standard for Safety Armored Cable
UL 5	(2016; Reprint Jul 2022) UL Standard for Safety Surface Metal Raceways and Fittings
UL 5A	(2015; Reprint Aug 2020) Nonmetallic Surface Raceways and Fittings
UL 6	(2007; Reprint Sep 2019) UL Standard for Safety Electrical Rigid Metal Conduit-Steel
UL 20	(2018; Reprint Jan 2021) UL Standard for Safety General-Use Snap Switches
UL 50	(2015) UL Standard for Safety Enclosures for Electrical Equipment, Non-Environmental Considerations
UL 67	(2018; Reprint Jul 2020) UL Standard for Safety Panelboards
UL 83	(2017; Reprint Mar 2020) UL Standard for Safety Thermoplastic-Insulated Wires and Cables
UL 198M	(2018) UL Standard for Mine-Duty Fuses
UL 360	(2013; Reprint Aug 2021) UL Standard for Safety Liquid-Tight Flexible Metal Conduit
UL 486A-486B	(2018; Reprint May 2021) UL Standard for Safety Wire Connectors
UL 486C	(2018; Reprint May 2021) UL Standard for Safety Splicing Wire Connectors
UL 489	(2016; Rev 2019) UL Standard for Safety Molded-Case Circuit Breakers, Molded-Case Switches and Circuit-Breaker Enclosures
UL 498	(2017; Reprint Jul 2022) UL Standard for Safety Attachment Plugs and Receptacles
UL 506	(2017; Reprint Jan 2022) UL Standard for Safety Specialty Transformers
UL 514A	(2013; Reprint Jun 2022) UL Standard for Safety Metallic Outlet Boxes

UL 514B	(2012; Reprint May 2020) Conduit, Tubing and Cable Fittings
UL 514C	(2014; Reprint Feb 2020) UL Standard for Safety Nonmetallic Outlet Boxes, Flush-Device Boxes, and Covers
UL 651	(2011; Reprint May 2022) UL Standard for Safety Schedule 40, 80, Type EB and A Rigid PVC Conduit and Fittings
UL 797	(2007; Reprint Mar 2021) UL Standard for Safety Electrical Metallic Tubing -- Steel
UL 817	(2015; Reprint Sep 2021) UL Standard for Safety Cord Sets and Power-Supply Cords
UL 869A	(2006; Reprint Jun 2020) Reference Standard for Service Equipment
UL 870	(2016; Reprint Mar 2019) UL Standard for Safety Wireways, Auxiliary Gutters, and Associated Fittings
UL 943	(2016; Reprint Feb 2018) UL Standard for Safety Ground-Fault Circuit-Interrupters
UL 1242	(2006; Reprint Apr 2022) UL Standard for Safety Electrical Intermediate Metal Conduit -- Steel
UL 1283	(2017) UL Standard for Safety Electromagnetic Interference Filters
UL 1449	(2021) UL Standard for Safety Surge Protective Devices
UL 1561	(2011; Reprint Jun 2015) Dry-Type General Purpose and Power Transformers
UL 1569	(2018) UL Standard for Safety Metal-Clad Cables
UL 4248-1	(2022) UL Standard for Safety Fuseholders - Part 1: General Requirements
UL 4248-12	(2018) UL Standard for Safety Fuseholders - Part 12: Class R

1.2 DEFINITIONS

a. Unless otherwise specified or indicated, electrical and electronics terms used in these specifications, and on the drawings, are as defined in IEEE Stds Dictionary.

b. The technical sections referred to herein are those specification sections that describe products, installation procedures, and equipment operations and that refer to this section for detailed

description of submittal types.

c. Vertical assembly: A vertical assembly is a pole, tower or other such support, mounting hardware, arms, brackets and the load. Load can be a luminaire, siren, loudspeaker or other device. All components of a vertical assembly will be rated by the manufacturer to withstand 150 mph wind loading in accordance with ASCE 7-16.

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Marking Strips; G

SD-03 Product Data

Conduits and Raceways; G

Wire and Cable; G

Splices and Connectors; G

Switches; G

Receptacles; G

Outlet Boxes, Pull Boxes and Junction Boxes; G

Circuit Breakers; G

Panelboards; G

Dry-Type Distribution Transformers; G

Device Plates; G

SD-06 Test Reports

Continuity Test; G

Phase-Rotation Tests; G

Insulation Resistance Test; G

600-Volt Wiring Test; G

Transformer Tests; G

Ground-Fault Receptacle Test; G

Insulation-Resistance Test; G

SD-08 Manufacturer's Instructions

Manufacturer's Instructions

1.4 QUALITY CONTROL

1.4.1 Regulatory Requirements

In each of the publications referred to herein, consider the advisory provisions to be mandatory, as though the word, "shall" had been substituted for "should" wherever it appears. Interpret references in these publications to the "authority having jurisdiction," or words of similar meaning, to mean the Contracting Officer. Ensure equipment, materials, installation, and workmanship are in accordance with the mandatory and advisory provisions of NFPA 70, unless more stringent requirements are specified or indicated.

1.4.2 Standard Products

Provide materials and equipment that are products of manufacturers regularly engaged in the production of such products which are of equal material, design and workmanship. Provide products which have been in satisfactory commercial or industrial use for 2 years prior to bid opening. Ensure the 2-year period includes applications of equipment and materials under similar circumstances and of similar size. Ensure the product has been on sale on the commercial market through advertisements, manufacturers' catalogs, or brochures during the 2-year period. Where two or more items of the same class of equipment are required, these items must be products of a single manufacturer.

PART 2 PRODUCTS

2.1 EQUIPMENT

Provide the standard cataloged materials and equipment of manufacturers regularly engaged in the manufacture of the products. For material, equipment, and fixture lists submittals, show manufacturer's style or catalog numbers, specification and drawing reference numbers, warranty information, and fabrication site.

Provide factory-applied finish on electrical equipment in accordance with the following:

a. NEMA 250 corrosion-resistance test and the additional requirements as specified herein.

b. Interior and exterior steel surfaces of equipment enclosures: thoroughly cleaned followed by a rust-inhibitive phosphatizing or equivalent treatment prior to painting.

c. Exterior surfaces: free from holes, seams, dents, weld marks, loose scale or other imperfections.

d. Interior surfaces: receive not less than one coat of corrosion-resisting paint in accordance with the manufacturer's standard practice.

e. Exterior surfaces: primed, filled where necessary, and given not less than two coats baked enamel with semigloss finish.

f. Equipment located indoors: ANSI Light Gray, and equipment located

outdoors: ANSI Light Gray.

g. Provide manufacturer's coatings for touch-up work and as specified in paragraph FIELD APPLIED PAINTING.

2.1.1 Conduits and Raceways

2.1.1.1 Rigid Steel Conduit

Provide hot dipped galvanized rigid steel conduit complying with NEMA RN 1, ANSI C80.1, UL 6 and UL 5 as applicable. Except where installed underground, or in corrosive areas, provide polyvinylchloride (PVC), or protect from corrosion by painting with bitumastic coating or wrapping with corrosion inhibiting tape..

Use threaded fittings for rigid steel conduit.

Use solid gaskets. Ensure conduit fittings with blank covers have gaskets, except in clean, dry areas or at the lowest point of a conduit run where drainage is required.

Provide covers with captive screws and are accessible after the work has been completed.

2.1.1.2 Electrical Metallic Tubing (EMT)

Ensure EMT is in accordance with UL 797, UL 5, and ANSI C80.3 and is zinc coated steel. Provide zinc-coated couplings and connectors that are raintight, compression type with insulated throat. Crimp, spring, or setscrew type fittings are not acceptable.

2.1.1.3 Flexible Metallic Conduit

Ensure flexible metallic conduit is galvanized steel and complies with UL 1 and UL 360.

Ensure fittings for flexible metallic conduit are specifically designed for such conduit.

Provide liquidtight flexible metallic conduit with a protective jacket of PVC extruded over a flexible interlocked galvanized steel core to protect wiring against moisture, oil, chemicals, and corrosive fumes.

Ensure fittings for liquidtight flexible metallic conduit are specifically designed for such conduit.

2.1.1.4 Intermediate Metal Conduit

Ensure intermediate metal conduit is galvanized steel and complies with UL 1242, NEMA RN 1, ANSI C80.1, UL 6 and UL 5 as applicable.

2.1.1.5 Rigid Nonmetallic Conduit

Ensure rigid nonmetallic conduit complies with NEMA TC 2, NEMA TC 3, and UL 651 as applicable with a wall thickness not less than Schedule 40.

2.1.1.6 Surface Metal Raceway

Ensure surface metal raceways and multi-outlet assemblies conform to

NFPA 70, and have receptacles conforming to NEMA WD 1, Type 5-20R.

UL 5, two-piece painted steel, totally enclosed, snap-cover type. Provide multiple outlet-type raceway with grounding-type receptacle where indicated. Provide receptacles as specified herein, spaced a minimum of one every 18 inches. Wire alternate receptacles on different circuits.

2.1.1.7 Surface Nonmetallic Raceway

UL 5A, nonmetallic totally enclosed, snap-cover type. Provide multiple outlet-type raceway with grounding-type receptacle where indicated. Provide receptacles as specified herein, spaced a minimum of one every 18 inches. Wire alternate receptacles on different circuits.

2.1.2 Wireways

Ensure wireways and auxiliary gutters are a minimum 4 by 4-inch trade size conforming to UL 870.

UL 870. Material: steel galvanized 16 gauge for heights and depths up to 6 by 6 inches, and 14 gauge for heights and depths up to 12 by 12 inches. Provide in length required for the application with screw- cover NEMA 1 enclosure per NEMA ICS 6.

2.1.3 Cable Trays

NEMA VE 1. Provide the following:

a. Cable trays: form a wireway system, with a nominal depth as indicated.

b. Cable trays: constructed of copper-free aluminum.

c. Cable trays: include splice and end plates, dropouts, and miscellaneous hardware.

d. Edges, fittings, and hardware: finished free from burrs and sharp edges.

e. Fittings: ensure not less than load-carrying ability of straight tray sections and have manufacturer's minimum standard radius.

f. Radius of bends as indicated.

Provide basket-type cable trays size as indicated with maximum wire mesh spacing of 2 by 4 inch.

Provide trough-type cable trays size as indicated.

Provide ladder-type cable trays size as indicated with maximum rung spacing of 12 inches.

Provide channel-type cable trays size as indicated.. Provide trays with one-piece construction having slots spaced not more than 4 1/2 inches on centers.

Provide solid bottom-type cable trays size as indicated. Provide solid covers.

Provide cantilever size as indicated. Provide trays with one-piece

construction having slots spaced not more than 4 1/2 inches on centers.

2.1.4 Outlet Boxes, Pull Boxes and Junction Boxes

Ensure outlet boxes for use with conduit systems are in accordance with NEMA FB 1 UL 514A, UL 514B, UL 514C and ANSI/NEMA OS 1 and are not less than 1-1/2 inches deep. Furnish all pull and junction boxes with screw-fastened covers.

2.1.5 Panelboards

Provide panelboards in accordance with NEMA PB 1, UL 67, and UL 50. Ensure panelboards for use as service equipment are also in accordance with UL 869A. Ensure panelboards have current rating, number of phases, and number of wires as indicated or specified herein. Ensure panelboards are rated for 120/208-volt, three-phase or 277/480-volt, three-phase, 60-hertz. Ensure each panelboard, as a complete unit, has a short-circuit current rating equal to or greater than the integrated equipment rating indicated, but in no case less than 10,000 amperes symmetrical.

Provide panelboards with bolt-on circuit breakers only. Use of plug-in style breaker is not permitted. Ensure panelboards are designed such that individual breakers can be removed without disturbing adjacent units or without loosening or removing supplemental insulation supplied as means of obtaining required clearance. Provide main lugs or main circuit breakers mounted "above" or "below" branch breakers with current ratings as indicated. Use of sub-feed breakers is not acceptable unless specifically indicated otherwise. Where "space only" is indicated, make provisions for future installation of breakers.

Submit detail drawings and manufacturer's standard product data for panelboards. Detail drawings consist of fabrication and assembly drawings for all parts of the work in sufficient detail to verify conformity with all requirements. Ensure drawings for panelboards indicate details of bus layout, overall physical features, dimensions, ratings, service requirements, and weights of equipment.

Provide copper buses of the rating indicated, with main lugs or main circuit breaker. Provide all panelboards for use on grounded ac systems with a separate grounding bus in accordance with UL 67 bonded to the panelboard enclosure. Ensure grounding bus is a solid bus bar of rectangular cross section equipped with binding screws for the connection of equipment grounding conductors. Provide three-phase, four-wire and single-phase, three-wire panelboards with an isolated full-capacity bus providing spaces for single-pole circuit breaker switches and spaces indicated as spare.

Provide bus bar connections to the branch circuit breakers that are the "distributed phase" or "phase sequence" type. Ensure single-phase, three-wire panelboard busing is such that when any two adjacent single-pole breakers are connected to opposite phases, two-pole breakers can be installed in any location. Ensure that three-phase, four-wire panelboard busing is such that when any three adjacent single-pole breakers are individually connected to each of the three different phases, two- or three-pole breakers can be installed at any location. Ensure current-carrying parts of the bus assembly are plated.

Support bus bars on bases independent of circuit breakers. Design main buses and back pans so that breakers may be changed without machining,

drilling, or tapping.

2.1.5.1 Circuit Breakers

Provide circuit breakers that conform to UL 489 and NEMA AB 3 and as specified in Section 26 05 71.00 40 LOW VOLTAGE OVERCORRECT PROTECTIVE DEVICES with frame a trip ratings as indicated.

Provide bolt-on type, molded-case, manually operated, trip-free circuit breakers, with inverse-time thermal-overload protection and instantaneous magnetic short-circuit protection. Completely enclose circuit breakers in a molded case, with a factory-sealed, calibrated sensing element to prevent tampering. Plug-in type, tandem, and half-size circuit breakers are not permitted.

Provide inverse-time-delay thermal-overload protection and instantaneous magnetic short-circuit protection. Provide an instantaneous solid-state tripping element that is adjustable and accessible from the front of the breaker on frame sizes larger than 250 ampere. Provide circuit breakers with frame sizes 250 ampere and larger with solid-state trip units equipped with adjustable long-time, short-timeandground-fault settings in addition to instantaneous.

Provide sufficient interrupting capacity of the panel and lighting branch circuit breakers to successfully interrupt the maximum short-circuit current imposed on the circuit at the breaker terminals. Provide circuit breaker interrupting capacities with a minimum of 10,000 A and that conform to NEMA AB 3.

Provide the common-trip-type multipole circuit breakers having a single operating handle and a two-position on/off indication. Provide circuit breakers with temperature compensation for operation in an ambient temperature of 104 degrees F. Provide circuit breakers that have root mean square (rms) symmetrical interrupting ratings sufficient to protect the circuit being supplied. Interrupting ratings may have selective-type tripping (time delay, magnetic, thermal, or ground fault).

Provide a phenolic-composition breaker body capable of having such accessories as handle-extension, handle-locking, and padlocking devices attached where required to meet lock-out/tag-out requirements of NFPA 70E.

2.1.6 Dry-Type Distribution Transformers

2.1.6.1 General Requirements

Ensure that general purpose dry-type transformers with windings 600 volts or less are two-winding, 60 hertz, and self-cooled in accordance with UL 506 and UL 1561. Ensure windings have a minimum of two 2-1/2-percent taps above and below nominal voltage.

Provide transformers in NEMA 1 enclosure.

Transformer insulation system:

a. 220 degrees C insulation system for transformers 15 kVA and greater, with temperature rise not exceeding 115 degrees C under full-rated load in maximum ambient of 40 degrees C.

b. 180 degrees C insulation for transformers rated 10 kVA and less, with

temperature rise not exceeding 115 degrees C under full-rated load in maximum ambient of 40 degrees C.

2.1.6.2 Transformer Factory Tests

Submittal: include routine NEMA ST 20 transformer test results on each transformer and also provide the results of NEMA "design" and "prototype" tests that were made on transformers electrically and mechanically equal to those specified.

2.2 MATERIALS

2.2.1 Wire And Cable

Provide wires and cables in accordance applicable requirements of NFPA 70 and UL for type of insulation, jacket, and conductor specified or indicated. Do not use wires and cables manufactured more than 12 months prior to date of delivery to site.

Provide minimum conductor size in accordance with the following:

a. Branch circuits: No. 12 AWG.

b. Class 1 remote-control and signal circuits: No. 14 AWG.

c. Class 2 low-energy, remote-control and signal circuits: No. 16 AWG.

d. Class 3 low-energy, remote-control, alarm and signal circuits: No. 22 AWG.

Ensure connectors used in wire systems comply with UL 486A-486B and UL 486C as applicable.

Ensure conductors installed in plenums are marked plenum rated.

2.2.1.1 Insulation

Unless specified or indicated otherwise or required by NFPA 70, provide power and lighting wires rated for 600-volts, Type THWN/THHN conforming to UL 83 or Type XHHW, except that grounding wire may be type TW conforming to UL 83; remote-control and signal circuits: Type TW or TF, conforming to UL 83. Where lighting fixtures require 90-degree Centigrade (C) conductors, provide only conductors with 90-degree C insulation or better.

2.2.1.2 Wire and Cable for 400 Hertz (Hz) Circuits

Insulated copper conductors.

2.2.1.3 Metal-Clad Cable

UL 1569; NFPA 70, Type MC cable.

2.2.1.4 Armored Cable

UL 4; NFPA 70, Type AC cable.

2.2.1.5 Mineral-Insulated, Metal-Sheathed Cable

UL listed; NFPA 70, Type MI cable. Do not use sheathing containing

asbestos fibers.

2.2.1.6 Cable Tray Cable or Power Limited Tray Cable

UL listed; type TC or PLTC.

2.2.1.7 Cord Sets and Power-Supply Cords

UL 817.

2.2.2 Device Plates

Provide the following:

a. UL listed, one-piece device plates for outlets to suit the devices installed.

b. For metal outlet boxes, plates on unfinished walls: zinc-coated sheet steel or cast metal having round or beveled edges.

c. For nonmetallic boxes and fittings, other suitable plates may be provided.

f. Screws: machine-type with countersunk heads in color to match finish of plate.

g. Sectional type device plates are not be permitted.

h. Plates installed in wet locations: gasketed and UL listed for "wet locations."

2.2.3 Switches

2.2.3.1 Safety Switches

Ensure safety switches comply with NEMA KS 1, and are the heavy-duty type with enclosure, voltage, current rating, number of poles, and fusing as indicated on the drawings. Ensure fused switch fuse holders comply with UL 4248-1. Ensure switch construction is such that, when the switch handle in the "ON" position, the cover or door cannot be opened. Cover release device is coinproof and so constructed that an external tool is used to open the cover. Make provisions to lock the handle in the "OFF" position. Ensure the switch is not capable of being locked in the "ON" position.

Provide switches of the quick-make, quick-break type and terminal lugs for use with copper conductors.

Ensure safety color coding for identification of safety switches conforms to ANSI Z535.1.

2.2.3.2 Toggle Switches

Ensure toggle switches comply with EIA 480, NEMA WD 1, and UL 20 control Light Emitting Diode (LED), and fluorescent lighting fixtures and are the heavy duty, general purpose, noninterchangeable flush-type.

Provide commercial grade toggle switches, double-pole, three -way two-position devices rated 20 amperes at 120/277 volts, 60 hertz

alternating current (ac) only.

Ensure all toggle switches are products of the same manufacturer.

2.2.4 Fuses

NEMA FU 1. Provide complete set of fuses for each fusible switch. Coordinate time-current characteristics curves of fuses serving motors or connected in series with circuit breakers or other circuit protective devices for proper operation. Submit coordination data for approval. Provide fuses with a voltage rating not less than circuit voltage.

2.2.4.1 Fuseholders

Provide in accordance with UL 4248-1.

2.2.4.2 Cartridge, Current Limiting Type (Class R)

UL 198M, time-delay type. Provide only Class R associated fuseholders in accordance with UL 4248-12.

2.2.4.3 Cartridge Fuses, High-Interrupting Capacity, Current Limiting Type (Classes J, L, and CC)

UL 198M, Class J for zero to 600 amperes, Class L for 601 to 6,000 amperes, and Class CC for zero to 30 amperes.

2.2.4.4 Cartridge Fuses, Current Limiting Type (Class T)

UL 198M, Class T for zero to 1,200 amperes, 300 volts; and zero to 800 amperes, 600 volts.

2.2.5 Receptacles

Provide the following:

a. UL 498, hard use (also designated heavy-duty), grounding-type.

b. Ratings and configurations: as indicated.

c. Bodies: white as per NEMA WD 1.

d. Face and body: thermoplastic supported on a metal mounting strap.

e. Dimensional requirements: per NEMA WD 6.

f. Screw-type, side-wired wiring terminals or of the solderless pressure type having suitable conductor-release arrangement.

g. Grounding pole connected to mounting strap.

h. The receptacle: containing triple-wipe power contacts and double or triple-wipe ground contacts.

2.2.5.1 Switched Duplex Receptacles

Provide separate terminals for each ungrounded pole. Top receptacle: switched when installed.

2.2.5.2 Weatherproof Receptacles

Provide receptacles, UL listed for use in "wet locations." Include cast metal box with gasketed, hinged, lockable and weatherproof while-in-use, polycarbonate, UV resistant/stabilized cover plate.

2.2.5.3 Ground-Fault Circuit Interrupter Receptacles

UL 943, duplex type for mounting in standard outlet box. Provide device capable of detecting current leak of 6 milliamperes or greater and tripping per requirements of UL 943 for Class A ground-fault circuit interrupter devices. Provide screw-type, side-wired wiring terminals or pre-wired (pigtail) leads.

2.2.5.4 Tamper-Resistant Receptacles

Provide duplex receptacle with mechanical sliding shutters that prevent the insertion of small objects into its contact slots.

2.2.6 Manufacturer's Nameplate

Ensure each item of equipment has a nameplate bearing the manufacturer's name, address, model number, and serial number securely affixed in a conspicuous place; the nameplate of the distributing agent is not acceptable.

2.2.7 Warning Signs

Provide warning signs for the enclosures of electrical equipment including substations, pad-mounted transformers, pad-mounted switches, generators, and switchgear having a nominal rating exceeding 600 volts.

a. Enclosure integrity to conform with IEEE C57.12.28, such as for pad-mounted transformers. Provide self-adhesive warning signs on the outside of the high voltage compartment door(s). Provide decal signs with nominal dimensions of 7 by 10 inches. Print the legend "DANGER HIGH VOLTAGE" in two lines of nominal 2 inch high letters. Show the word "DANGER" in white letters on a red background and the words "HIGH VOLTAGE" in black letters on a white background.

2.2.8 Firestopping Materials

Provide firestopping around electrical penetrations in accordance with Section 07 84 00, FIRESTOPPING.

2.2.9 Metering

ANSI C12.1. Provide a self-contained, socket-mounted, electronic programmable outdoor watthour meter. Meter: either programmed at the factory or programmed in the field. Turn field programming device over to the Contracting Officer at completion of project. Coordinate meter to system requirements.

a. Design: Provide watthour meter designed for use on a single-phase, three-wire, 480/240 volt system. Include necessary KYZ pulse initiation hardware for Energy Monitoring and Control System (EMCS).

b. Class: 200; Form: 2S, accuracy: plus or minus 1.0 percent; Finish: Class II.

c. Cover: Polycarbonate and lockable to prevent tampering and unauthorized removal.

d. Kilowatt-hour Register: five digit electronic programmable type.

e. Demand Register:

(1) Provide solid state.

(2) Meter reading multiplier: Indicate multiplier on the meter face.

(3) Demand interval length: programmed for 60 minutes with rolling demand up to six subintervals per interval.

f. Socket: ANSI C12.7. Provide NEMA Type 3R, box-mounted socket, ringless, having manual circuit-closing bypass and having jaws compatible with requirements of the meter. Provide manufacturers standard enclosure color unless otherwise indicated.

2.2.10 Surge Protective Devices

Provide parallel type surge protective devices (SPD) which comply with UL 1449 at the service entrance, panelboards. Provide surge protectors in a NEMA 1 enclosure per NEMA ICS 6. Use Type 1 or Type 2 SPD and connect on the load side of a dedicated circuit breaker.

Provide the following modes of protection:

FOR SINGLE PHASE AND THREE PHASE WYE CONNECTED SYSTEMS-
Phase to phase (L-L)
Each phase to neutral (L-N)

SPDs at the service entrance: provide with a minimum surge current rating of 80,000 amperes for L-L mode minimum and 40,000 amperes for other modes (L-N, L-G, and N-G) and downstream SPDs rated 40,000 amperes for L-L mode minimum and 20,000 amperes for other modes (L-N, L-G, and N-G).

Provide SPDs per NFPA 780 for the lightning protection system.

Maximum L-N, L-G, and N-G Voltage Protection Rating:

600V for 208Y/120V, three phase system
1,200V for 480Y/277V, three phase system

Maximum L-L Voltage Protection Rating:

1,200V for 208Y/120V, three phase system
1,200V for 480Y/277V, three phase system

The minimum MCOV (Maximum Continuous Operating Voltage) rating for L-N and L-G modes of operation: 120% of nominal voltage for 240 volts and below; 115% of nominal voltage above 240 volts to 480 volts.

Provide EMI/RFI filtering per UL 1283 for each mode with the capability to attenuate high frequency noise. Minimum attenuation: 20db.

PART 3 EXECUTION

3.1 PREPARATION

Submit manufacturer's instructions including special provisions required to install equipment components and system packages. Special provisions include impedances, hazards and safety precautions.

Clean and paint conduit, supports, fittings, cabinets, pull boxes, and racks as specified in Section 09 90 00 PAINTS AND COATINGS.

Protect metallic materials against corrosion. Provide equipment enclosures with the standard finish by the manufacturer when used for most indoor installations. For harsh indoor environments (any area subjected to chemical and abrasive action), and all outdoor installations, refer to Section 09 90 00 PAINTS AND COATINGS. Do not use aluminum when in contact with earth or concrete and, where connected to dissimilar metal, protect by using approved fittings and treatment. Except where other equivalent protective treatment is specifically approved in writing, provide hot-dip galvanized ferrous metals for items such as, anchors, bolts, braces, boxes, bodies, clamps, fittings, guards, nuts, pins, rods, shims, thimbles, washers, and miscellaneous items not made of corrosion-resistant steel.

3.2 INSTALLATION

3.2.1 Underground Service

Underground service conductors and associated conduit: continuous from service entrance equipment to outdoor power system connection.

3.2.2 Overhead Service

Overhead service conductors into buildings: terminate at service entrance fittings or weatherhead outside building.

3.2.3 Hazardous Locations

Perform work in hazardous locations, as defined by NFPA 70, in strict accordance with NFPA 70 for particular "Class," "Division," and "Group" of hazardous locations involved. Provide conduit and cable seals where required by NFPA 70. Provide conduit with tapered threads.

3.2.4 Service Entrance Identification

Service entrance disconnect devices, switches, and enclosures: labeled and identified as such.

3.2.5 Labels

Wherever work results in service entrance disconnect devices in more than one enclosure, as permitted by NFPA 70, label each enclosure, new and existing, as one of several enclosures containing service entrance disconnect devices. Label, at minimum: indicate number of service disconnect devices housed by enclosure and indicate total number of enclosures that contain service disconnect devices. Provide laminated plastic labels conforming to paragraph FIELD FABRICATED NAMEPLATES. Use lettering of at least 0.25 inch in height, and engrave on black-on-white matte finish. Service entrance disconnect devices in more than one

enclosure: provided only as permitted by NFPA 70.

3.2.6 Wiring Methods

Provide insulated conductors installed in rigid steel conduit, IMC, rigid nonmetallic conduit, or EMT, except where specifically indicated or specified otherwise or required by NFPA 70 to be installed otherwise. Grounding conductor: separate from electrical system neutral conductor. Provide insulated green equipment grounding conductor for circuit(s) installed in conduit and raceways. Shared neutral, or multi-wire branch circuits, are not permitted with arc-fault circuit interrupters. Minimum conduit size: 1/2 inch in diameter for low voltage lighting and power circuits. Vertical distribution in multiple story buildings: made with metal conduit in fire-rated shafts, with metal conduit extending through shafts for minimum distance of 6 inches. Firestop conduit which penetrates fire-rated walls, fire-rated partitions, or fire-rated floors in accordance with Section 07 84 00, FIRESTOPPING.

3.2.6.1 Pull Wire

Install pull wires in empty conduits. Pull wire: plastic having minimum 200-pound force tensile strength. Leave minimum 36 inches of slack at each end of pull wire.

3.2.6.2 Metal Clad Cable

Install in accordance with NFPA 70, Type MC cable.

3.2.6.3 Armored Cable

Install in accordance with NFPA 70, Type AC cable.

3.2.6.4 Mineral Insulated, Metal Sheathed (Type MI) Cable Installation

Mineral-insulated, metal-sheathed cable system, Type MI, may be used in lieu of exposed conduit and wiring. Conductor sizes: not less than those indicated for the conduit installation. Fasten cables within 12 inches of each turn or offset and at 33 inches maximum intervals. Make cable terminations in accordance with NFPA 70 and cable manufacturer's recommendations. Terminate single-conductor cables of a circuit, having capacities of more than 50 amperes, in a single box or cabinet opening. Color code individual conductors in all outlets and cabinets.

3.2.7 Conduits, Raceways and Fittings

Ensure that conduit runs between outlet and outlet, between fitting and fitting, or between outlet and fitting does not contain more than the equivalent of three 90-degree bends, including those bends located immediately at the outlet or fitting.

Do not install crushed or deformed conduit. Avoid trapped conduit runs where possible. Take care to prevent the lodgment of foreign material in the conduit, boxes, fittings, and equipment during the course of construction. Clear any clogged conduit of obstructions or replace conduit.

Conduit and raceway runs concealed in or behind walls, above ceilings, or exposed on walls and ceilings 5 feet or more above finished floors and not subject to mechanical damage may be electrical metallic tubing (EMT).

Unless indicated otherwise, conceal conduit under floor slabs and within finished walls, ceilings, and floors. Keep conduit minimum 6 inches away from parallel runs of flues and steam or hot water pipes. Install conduit parallel with or at right angles to ceilings, walls, and structural members where located above accessible ceilings and where conduit will be visible after completion of project.3.2.7.1 Rigid Steel Conduit

Make field-made bends and offsets with approved Hickey bending tool or conduit bending machine. Use long radius conduit for elbows larger than 2-1/2 inches.

Provide a flush coupling for all conduit stubbed-up through concrete floors for connections to free-standing equipment with the exception of motor-control centers, cubicles, and other such items of equipment, when the floor slab is of sufficient thickness. Otherwise, provide a floor box set flush with the finished floor. For conduits installed for future use, terminate with a coupling and plug; set flush with the floor.

3.2.7.2 Electrical Metallic Tubing (EMT)

Ground EMT in accordance with NFPA 70, using pressure grounding connectors especially designed for EMT.

3.2.7.3 Flexible Metallic Conduit

Use flexible metallic conduit to connect recessed fixtures from outlet boxes in ceilings, transformers, and other approved assemblies.

Use bonding wires in flexible conduit as specified in NFPA 70, for all circuits. Flexible conduit is not considered a ground conductor.

Make electrical connections to vibration-isolated equipment with flexible metallic conduit.

Use liquidtight flexible metallic conduit in wet and oily locations and to complete the connection to motor-driven equipment.

Provide flexible steel conduit between 3 and 6 feet in length for recessed and semirecessed lighting fixtures; for equipment subject to vibration, noise transmission, or movement; and for motors. Install flexible conduit to allow 20 percent slack. Minimum flexible steel conduit size: 1/2 inch diameter. Provide liquidtight flexible conduit in wet and damp locations and in fire pump rooms for equipment subject to vibration, noise transmission, movement or motors. Provide separate ground conductor across flexible connections.

3.2.7.4 Intermediate Conduit

Make all field-made bends and offsets with approved Hickey bending tool or conduit bending machine. Use intermediate metal conduit only for indoor installations.

3.2.7.5 Rigid Nonmetallic Conduit

Install a green insulated copper grounding conductor in conduit with conductors and solidly connect to ground at each end. Size grounding wires in accordance with NFPA 70.

3.2.7.6 Underground Conduit

Plastic-coated rigid steel; plastic-coated steel IMC; PVC, Type EPC-40. Convert nonmetallic conduit, other than PVC Schedule 40 or 80, to plastic-coated rigid, or IMC, steel conduit before rising through floor slab. Plastic coating: extend minimum 6 inches above floor.

3.2.7.7 Conduit for Circuits Rated Greater Than 600 Volts

Rigid metal conduit or IMC only.

3.2.7.8 Conduit Installed Under Floor Slabs

Conduit run under floor slab: located a minimum of 12 inches below the vapor barrier. Seal around conduits at penetrations thru vapor barrier.

3.2.7.9 Conduit Installed Through Floor Slabs

Where conduits rise through floor slabs, do not allow curved portion of bends to be visible above finished slab.

3.2.7.10 Conduit Installed in Concrete Floor Slabs

PVC, Type EPC-40, unless indicated otherwise. Locate so as not to adversely affect structural strength of slabs. Install conduit within middle one-third of concrete slab. Do not stack conduits. Space conduits horizontally not closer than three diameters, except at cabinet locations. Curved portions of bends must not be visible above finish slab. Increase slab thickness as necessary to provide minimum one inch cover over conduit. Where embedded conduits cross building and/or expansion joints, provide suitable watertight expansion/deflection fittings and bonding jumpers. Expansion/deflection fittings must allow horizontal and vertical movement of raceway. Conduit larger than one inch trade size: installed parallel with or at right angles to main reinforcement; when at right angles to reinforcement, install conduit close to one of supports of slab. Where nonmetallic conduit is used, convert raceway to plastic coated rigid steel or plastic coated steel IMC before rising above floor, unless specifically indicated.

3.2.7.11 Stub Ups

Provide conduits stubbed up through concrete floor for connection to free-standing equipment with adjustable top or coupling threaded inside for plugs, set flush with finished floor. Extend conductors to equipment in rigid steel conduit, except that flexible metal conduit may be used 6 inches above floor. Where no equipment connections are made, install screwdriver-operated threaded flush plugs in conduit end.

3.2.7.12 Conduit Support

Support conduit by pipe straps, wall brackets, threaded rod conduit hangers, or ceiling trapeze. Fasten by wood screws to wood; by toggle bolts on hollow masonry units; by concrete inserts or expansion bolts on concrete or brick; and by machine screws, welded threaded studs, or spring-tension clamps on steel work. Threaded C-clamps may be used on rigid steel conduit only. Do not weld conduits or pipe straps to steel structures. Do not exceed one-fourth proof test load for load applied to fasteners. Provide vibration resistant and shock-resistant fasteners attached to concrete ceiling. Do not cut main reinforcing bars for any

holes cut to depth of more than 1 1/2 inches in reinforced concrete beams or to depth of more than 3/4 inch in concrete joints. Fill unused holes. In partitions of light steel construction, use sheet metal screws. In suspended-ceiling construction, run conduit above ceiling. Do not support conduit by ceiling support system. Conduit and box systems: supported independently of both (a) tie wires supporting ceiling grid system, and (b) ceiling grid system into which ceiling panels are placed. Do not share supporting means between electrical raceways and mechanical piping or ducts. Coordinate installation with above-ceiling mechanical systems to assure maximum accessibility to all systems. Spring-steel fasteners may be used for lighting branch circuit conduit supports in suspended ceilings in dry locations. For conduits greater than 2 1/2 inches inside diameter, provide supports to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction.

3.2.7.13 Directional Changes in Conduit Runs

Make changes in direction of runs with symmetrical bends or cast-metal fittings. Make field-made bends and offsets with hickey or conduit-bending machine. Do not install crushed or deformed conduits. Avoid trapped conduits. Prevent plaster, dirt, or trash from lodging in conduits, boxes, fittings, and equipment during construction. Free clogged conduits of obstructions.

3.2.7.14 Wireway and Auxiliary Gutter

Bolt together straight sections and fittings to provide a rigid, mechanical connection and electrical continuity. Close dead ends of wireways and auxiliary gutters. Plug all unused conduit openings.

Support wireways for overhead distribution and control circuits at maximum 5-foot intervals.

Ensure auxiliary gutters used to supplement wiring spaces for equipment not contained in a single enclosure contains no switches, overcurrent devices, appliances, or apparatus and is not more than 30 feet long.

3.2.7.15 Surface Raceways and Assemblies

Mount surface raceways plumb and level, with the base and cover secured. Minimum circuit run is three-wire, with one wire designated as ground.

3.2.7.16 Cable Trays

Support cable trays from ceiling hangers, equipment bays, or floor or wall supports. Cable trays may be mounted on equipment racks. Provide support when the free end extends beyond 3 feet. Maximum support spacing is 6 feet. Support trays 10-inches wide or less by one hanger. Support trays greater than 10 inches wide by two hangers. Bond cable trays at splices.

3.2.8 Wiring

Color code feeder and branch circuit conductors as follows:

CONDUCTOR	COLOR AC
Phase A	Black (208VAC); Brown (480VAC)
Phase B	Red (208VAC); Orange (480VAC)
Phase C	Blue (208VAC); Yellow (480VAC)
Neutral	White (208VAC); Natural Gray (480VAC)
Equipment Grounds	Green

Use conductors up to and including AWG No. 2 that are manufactured with colored insulating materials. For conductors larger than AWG No. 2, have ends identified with color plastic tape in outlet, pull, or junction boxes.

Splice in accordance with the NFPA 70. Provide conductor identification within each enclosure where a tap, splice, or termination is made and at the equipment terminal of each conductor. Match terminal and conductor identification as indicated.

Where several feeders pass through a common pullbox, tag the feeders to clearly indicate the electrical characteristics, circuit number, and panel designation.

3.2.9 Wiring Devices

3.2.9.1 Wall Switches and Receptacles

Install wall switches and receptacles so that when device plates are applied, the plates are aligned vertically to within 1/16 inch.

Bond ground terminal of each flush-mounted receptacle to the outlet box with an approved green bonding jumper when used with dry wall type construction.

3.2.9.2 Device Plates

Ensure device plates for switches are suitably engraved with a description of the loads when not within sight of the loads controlled.

Mark device plates and receptacle cover plates for receptacles other than 125-volt, single-phase, duplex, convenience outlets. Show the circuit number, voltage, frequency, phasing, and amperage available at the receptacle. Use self-adhesive labels having 1/4 inch embossed letters.

Similarly mark device plates for convenience outlets indicating the supply panel and circuit number.

3.2.10 Splices and Connectors

Make all splices in AWG No. 8 and smaller with approved insulated electrical type.

Make all splices in AWG No. 6 and larger with insulated electrical lugs type. Wrap joints with an insulating tape that has an insulation and

temperature rating equivalent to that of the conductor.

3.2.11 Conductor Identification

Provide conductor identification within each enclosure where tap, splice, or termination is made. For conductors No. 6 AWG and smaller diameter, provide color coding by factory-applied, color-impregnated insulation. For conductors No. 4 AWG and larger diameter, provide color coding by plastic-coated, self-sticking markers; colored nylon cable ties and plates; or heat shrink-type sleeves. Identify control circuit terminations in accordance with manufacturer's recommendations. Provide telecommunications system conductor identification as specified in Section 27 10 00 BUILDING TELECOMMUNICATIONS CABLING SYSTEMS.

3.2.11.1 Marking Strips

Provide marking strips in accordance with the following:

a. Provide white or other light-colored plastic marking strips, fastened by screws to each terminal block, for wire designations.

b. Use permanent ink for the wire numbers

c. Provide reversible marking strips to permit marking both sides, or provide two marking strips with each block.

d. Size marking strips to accommodate the two sets of wire numbers.

e. Assign a device designation in accordance with NEMA ICS 1 to each device to which a connection is made. Mark each device terminal to which a connection is made with a distinct terminal marking corresponding to the wire designation used on the Contractor's schematic and connection diagrams.

f. The wire (terminal point) designations used on the Contractor's wiring diagrams and printed on terminal block marking strips may be according to the Contractor's standard practice; however, provide additional wire and cable designations for identification of remote (external) circuits for the Government's wire designations.

g. Prints of the marking strips drawings submitted for approval will be so marked and returned to the Contractor for addition of the designations to the terminal strips and tracings, along with any rearrangement of points required.

3.2.12 Safety Switches

Securely fasten switches to the supporting structure or wall, utilizing a minimum of four 1/4 inch bolts. Do not use sheet metal screws and small machine screws for mounting. Do not mount switches in an inaccessible location or where the passageway to the switch may become obstructed. Mounting height 5 feet above floor level, when possible.

3.2.13 Boxes and Fittings

Provide pullboxes where necessary in the conduit system to facilitate conductor installation. For conduit runs longer than 100 feet or with more than three right-angle bends, install a pullbox at a convenient intermediate location.

Securely mount boxes and enclosures to the building structure using supports that are independent of the conduit entering or leaving the boxes.

Select the mounting height of wall-mounted outlet and switch boxes, as measured between the bottom of the box and the finished floor, in accordance with ICC/ANSI A117.1 and as follows, unless otherwise indicated:

LOCATION	MOUNTING HEIGHT (inches)
Receptacles in offices	18
Receptacles in corridors	18
Receptacles in shops and laboratories	48
Receptacles in rest rooms	48
Switches for light control	48

3.2.14 Covers and Device Plates

Install with edges in continuous contact with finished wall surfaces without use of mats or similar devices. Plaster fillings are not permitted. Install plates with alignment tolerance of 1/16 inch. Use of sectional-type device plates are not permitted. Provide gasket for plates installed in wet locations.

3.2.15 Electrical Penetrations

Seal openings around electrical penetrations through fire resistance-rated walls, partitions, floors, or ceilings in accordance with Section 07 84 00 FIRESTOPPING.

3.2.16 Panelboards

Securely mount panelboards so that the top operating handle does not exceed 72-inches above the finished floor. Do not mount equipment within 36-inches of the front of the panel. Ensure directory card information is complete and legible.

3.2.17 Dry-Type Distribution Transformers

Connect dry-type transformers with flexible metallic conduit.

3.2.18 Surge Protective Devices

Connect the surge protective devices in parallel to the power source, keeping the conductors as short and straight as practically possible. Maximum allowed lead length is 3 feet.

3.2.19 Field Fabricated Nameplates

Ensure nameplates conform to ASTM D709. Provide laminated plastic nameplates for each equipment enclosure, relay, switch, and device, as specified or as indicated on the drawings. Each nameplate inscription identifies the function and, when applicable, the position. Provide

nameplates that are melamine plastic, 0.125-inch thick, white with black center core and a matte finish surface . Accurately align lettering and engrave into the core. Minimum size of nameplates is 1 by 2.5 inches. Lettering is a minimum of 0.25-inch high normal block style.

3.2.20 Identification Plates and Warnings

Provide identification plates for lighting and power panelboards, motor control centers, all line voltage heating and ventilating control panels, fire detector and sprinkler alarms, door bells, pilot lights, disconnect switches, manual starting switches, and magnetic starters. Attach identification plates to process control devices and pilot lights.

Install identification plates for all line voltage enclosed circuit breakers, identifying the equipment served, voltage, phase(s) and power source. For circuits 480 volts and above, install conspicuously located warning signs in accordance with OSHA requirements.

3.3 FIELD FABRICATED NAMEPLATE MOUNTING

Provide number, location, and letter designation of nameplates as indicated. Fasten nameplates to the device with a minimum of two sheet-metal screws or two rivets.

3.4 WARNING SIGN MOUNTING

Provide the number of signs required to be readable from each accessible side. Space the signs in accordance with NFPA 70E.

3.5 FIELD APPLIED MOUNTING

Paint electrical equipment as required to match finish of adjacent surfaces or to meet the indicated or specified safety criteria. Where field painting of enclosures for panelboards, load centers or the like is specified to match adjacent surfaces, to correct damage to the manufacturer's factory applied coatings, or to meet the indicated or specified safety criteria, provide manufacturer's recommended coatings and apply in accordance to manufacturer's instructions.

3.6 FIELD QUALITY CONTROL

After completion of the installation and splicing, and prior to energizing the conductors, perform wire and cable continuity and insulation tests as herein specified before the conductors are energized.

Provide all necessary test equipment, labor, and personnel to perform the tests, as herein specified.

Isolate completely all wire and cable from all extraneous electrical connections at cable terminations and joints. Use substation and switchboard feeder breakers, disconnects in combination motor starters, circuit breakers in panel boards, and other disconnecting devices to isolate the circuits under test.

Perform insulation-resistance test on each field-installed conductor with respect to ground and adjacent conductors. Applied potential is 500 volts dc for 300 volt rated cable and 1000 volts dc for 600 volt rated cable. Take readings after 1 minute and until the reading is constant for 15 seconds. Minimum insulation-resistance values is not less than 25 Megohms for 300 volt rated cable and 100 Megohms for 600 volt rated cable. For

circuits with conductor sizes AWG No. 8 and smaller insulation resistance testing is not required.

Perform continuity test to insure correct cable connection end-to-end (i.e correct phase conductor, grounded conductor, and grounding conductor wiring). Repair and verify any damages to existing or new electrical equipment resulting from mis-wiring. Receive approval for all repairs prior to commencement of the repair.

Conduct phase-rotation tests on all three-phase circuits using a phase-rotation indicating instrument. Perform phase rotation of electrical connections to connected equipment in a clockwise direction, facing the source.

Perform 600-volt wiring test on wiring rated 600 volt and less to verify that no short circuits or accidental grounds exist. Perform insulation resistance tests on wiring No. 6 AWG and larger diameter using instrument which applies voltage of approximately 500 volts to provide direct reading of resistance. Minimum resistance: 250,000 ohms.

Perform the standard, not optional, transformer tests in accordance with the Inspection and Test Procedures for transformers, dry type, air-cooled, 600 volt and below; as specified in NETA ATS. Measure primary and secondary voltages for proper tap settings. Tests need not be performed by a recognized independent testing firm or independent electrical consulting firm.

Perform ground-fault receptacle test for ground-fault receptacles with a "load" (such as a plug in light) to verify that the "line" and "load" leads are not reversed.

Submit test reports in accordance with referenced standards in this section.

Final acceptance requires the successful performance of wire and cable under test. Do not energize any conductor until the final test reports are reviewed and approved.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 26 - ELECTRICAL

SECTION 26 05 13.00 40

MEDIUM-VOLTAGE CABLES

PART 1 GENERAL

1.1 REFERENCES
1.2 DEFINITIONS
1.3 ADMINISTRATIVE REQUIREMENTS
1.3.1 Pre-Installation Meetings
1.4 SUBMITTALS
1.5 QUALITY CONTROL
1.5.1 Regulatory Requirements
1.5.2 Standard Products
1.6 DELIVERY, STORAGE, AND HANDLING

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION
2.2 EQUIPMENT
2.2.1 Multiple-Conductor Shielded Cables
2.2.1.1 Synthetic Rubber with Interlocked Armor
2.2.1.2 Cross-Linked Polyethylene
2.2.1.3 Ethylene Propylene Rubber (EPR) with Jacketed Interlocked Armor
2.2.2 Multiple-Conductor, Nonshielded Cables
2.2.2.1 Synthetic Rubber with Neoprene Jacket
2.2.2.2 Cross-Linked Polyethylene with PVC Jacket
2.2.2.3 Ethylene-Propylene with PVC Jacket
2.2.3 Single-Conductor Shielded Cables
2.2.3.1 Cross-Linked Polyethylene with PVC Jacket
2.2.3.2 Cross-Linked Polyethylene with Interlocked Armor
2.2.3.3 Ethylene-Propylene-Rubber-Insulated with PVC Jacket
2.2.4 Single-Conductor Nonshielded Cables
2.2.4.1 Cross-Linked Polyethylene
2.2.4.2 Ethylene-Propylene-Rubber-Insulated with PVC Jacket
2.2.5 Portable Cables
2.2.6 Insulated Medium Voltage Connectors
2.2.7 Splices
2.2.8 Terminations
2.2.9 Cable Supports and Fittings
2.2.10 Polyethylene Cable Tags
2.2.11 Fireproof Tape
2.3 MATERIALS
2.3.1 Conductors
2.3.2 Insulation
2.3.3 Cable Identification
2.3.4 Non-metallic Insulation Shield
2.3.5 Concentric Neutral Shield
2.3.6 Jacket

2.3.7 Interlock Armored Cable
2.4 TESTS, INSPECTIONS, AND VERIFICATIONS
2.4.1 FACTORY TESTING

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Protection During Splicing Operations
3.1.2 Duct Cleaning
3.1.3 Pulling Cables in Ducts, Manholes and Utility Tunnels
3.1.3.1 Allowable Sidewall Pressure
3.1.3.2 Minimum Bending Radius
3.1.3.3 Coating of Cables
3.1.3.4 Pulling Speed
3.1.3.5 Cable Splice Support And Sealing
3.1.4 Splices and Terminations
3.1.5 Fireproofing
3.1.6 Cable Tag Installation
3.2 FIELD QUALITY CONTROL
3.3 CLOSEOUT ACTIVITIES

-- End of Section Table of Contents --

SECTION 26 05 13.00 40

MEDIUM-VOLTAGE CABLES

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ASSOCIATION OF EDISON ILLUMINATING COMPANIES (AEIC)

AEIC CS1	(2012) Impregnated-Paper-Insulated, Metallic Sheathed Cable, Solid Type
AEIC CS8	(2013) Specification for Extruded Dielectric Shielded Power Cables Rated 5 Through 46 kV

ASTM INTERNATIONAL (ASTM)

ASTM B3	(2013) Standard Specification for Soft or Annealed Copper Wire
ASTM B8	(2011; R 2017) Standard Specification for Concentric-Lay-Stranded Copper Conductors, Hard, Medium-Hard, or Soft
ASTM D746	(2014) Standard Test Method for Brittleness Temperature of Plastics and Elastomers by Impact

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 48	(2020) Test Procedures and Requirements for Alternating-Current Cable Terminations Used on Shielded Cables Having Laminated Insulation Rated 2.5 kV through 765 kV or Extruded Insulation Rated 2.5 kV through 500 kV
IEEE 386	(2016) Separable Insulated Connector Systems for Power Distribution Systems Rated 2.5 kV through 35 kV
IEEE 400.2	(2013) Guide for Field Testing of Shielded Power Cable Systems Using Very Low Frequency (VLF)
IEEE 404	(2012) Standard for Extruded and Laminated Dielectric Shielded Cable Joints Rated 2500 V to 500,000 V

IEEE C2	(2023) National Electrical Safety Code

INTERNATIONAL ELECTRICAL TESTING ASSOCIATION (NETA)

NETA ATS	(2021) Standard for Acceptance Testing Specifications for Electrical Power Equipment and Systems

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

ANSI C119.1	(2016) Electric Connectors - Sealed Insulated Underground Connector Systems Rated 600 Volts
ANSI/NEMA WC 71/ICEA S-96-659	(2014) Standard for Nonshielded Cables Rated 2001-5000 Volts for use in the Distribution of Electric Energy
NEMA WC 70	(2021) Power Cable Rated 2000 Volts or Less for the Distribution of Electrical Energy
NEMA WC 74/ICEA S-93-639	(2012) 5-46 kV Shielded Power Cable for Use in the Transmission and Distribution of Electric Energy
NEMA WC 27500	(2020) Standard for Aerospace and Industrial Electrical Cable

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National Electrical Code
NFPA 70B	(2019) Recommended Practice for Electrical Equipment Maintenance
NFPA 70E	(2021) Standard for Electrical Safety in the Workplace

1.2 DEFINITIONS

Medium-voltage power cables include all cables rated above 600 volts up to 35,000 volts.

1.3 ADMINISTRATIVE REQUIREMENTS

1.3.1 Pre-Installation Meetings

No later than 30 days of Contract Award, coordinate with the Contracting Officer to schedule a pre-installation meeting. Submit the following for review and approval prior to the meeting:

a. Pulling Plan including calculations of pulling tension and side wall pressure anticipated, and the maximum allowable pulling tension for each pull. Do not perform any pull until Government reviews and approves the pulling plan.

b. Splicer/Terminator Certifications

c. List of Splices and Terminations to be Installed by Splicer/Terminator

d. Manufacturer's catalog data for all cables, cable supports and fittings, cable tags, fireproof tape, splice kits, terminations, and any other product data required to complete the work.

e. Certificates showing that the cable manufacturer has made factory-conducted tests on each shipping length (reel) of cable. Include certified copies of test data showing conformance with the referenced standards and approval prior to delivery of cable.

1.4 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

List of Splices and Terminations to be Installed by Splicer/Terminator; G

SD-02 Shop Drawings

Pulling Plan; G

SD-03 Product Data

Multiple-Conductor Shielded Cables; G

Multiple-Conductor Nonshielded Cables; G

Single-Conductor Shielded Cables; G

Single-Conductor Nonshielded Cables; G

Portable Cables; G

Cable Supports and Fittings; G

Polyethylene Cable Tags; G

Fireproof Tape; G

Splices; G

Terminations; G

Polyethylene Cable Tags; G

SD-06 Test Reports

Field Testing; G

Qualification Test Reports; G

Radiographic Tests; G

SD-07 Certificates

Splicer/Terminator Certifications; G

SD-08 Manufacturer's Instructions

Medium-Voltage Power Cables; G

Terminations; G

Splices; G

1.5 QUALITY CONTROL

1.5.1 Regulatory Requirements

In each of the publications referred to herein, consider the advisory provisions to be mandatory, as though the word, "shall" had been substituted for "should" wherever it appears. Interpret references in these publications to the "authority having jurisdiction," or words of similar meaning, to mean the Contracting Officer. Ensure equipment, materials, installation, and workmanship are in accordance with the mandatory and advisory provisions of NFPA 70, IEEE C2 unless more stringent requirements are specified or indicated.

1.5.2 Standard Products

Provide materials and equipment that are products of manufacturers regularly engaged in the production of such products which are of equal material, design and workmanship. Provide products which have been in satisfactory commercial or industrial use for 2 years prior to bid opening. Ensure the 2-year period includes applications of equipment and materials under similar circumstances and of similar size. Ensure the product has been on sale on the commercial market through advertisements, manufacturers' catalogs, or brochures during the 2-year period. Where two or more items of the same class of equipment are required, these items must be products of a single manufacturer.

Qualifications`

Verify personnel performing Medium Voltage (MV) splicing or terminations have 5 years minimum experience in cable splicing and terminations of the type used in this project. Submit splicer/terminator certifications issued by the cable splice and termination manufacturer who has examined and tested a test splice or termination of each type required by this contract for each cable splicer. Ensure the certification identifies which splices and terminations it applies to. Require each individual, certified or not, with the required medium voltage splicing and terminating experience, who is to perform cable splicing or terminating, to perform a minimum of one splice or termination of each type in the presence of the manufacturer's and Government's representative. Supply all materials and tools required for the demonstration splices and terminations. Submit each splice or termination performed by individuals without manufacturer's certification to the manufacturer for testing and subsequent certification. Certification is not required for load break elbows and dead break connectors.

Once a splice or termination has been started by a splicer, ensure the

same splicer completes that particular splice, and that each termination and splice is started and completed in one continuous work period.

Maintain and submit a list of splices and terminations to be installed by splicer/terminator. Ensure the list includes the following for each splice or termination completed.

a. Name of splicer/terminator.

b. Date splice or termination was performed.

c. Location of splice or termination. For terminations at equipment indicate equipment number as required to completely define the location.

1.6 DELIVERY, STORAGE, AND HANDLING

Ship cables on reels in a way that protects the cable from mechanical injury. Hermetically seal end of each cable length using heat-shrinkable molded cable end caps to exclude moisture and securely attached to the reel.

Make the minimum reel drum diameter 14 times the overall diameter of the cable. Ensure that each cable length is installed with a pulling eye installed by the manufacturer, for installation in ducts, manholes, and utility tunnels.

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION

Provide medium-voltage power cables including multiple- and single-conductor cables rated 15,000 volts, ungrounded neutral, on 12,470 -volt three-phase, 60-hertz, phase-to-phase, for grounded and ungrounded neutral systems.

Provide conductor cable assemblies consisting of:

a. Conductor core with an extruded semiconductor shield over the conductors

b. Insulation

c. A polyethylene (PE) jacket.

d. An extruded semiconductor insulation shield, a concentric neutral

2.2 EQUIPMENT

Ensure that ethylene-propylene rubber and cross-linked polyethylene-insulated conductors are lead-free.

2.2.1 Multiple-Conductor Shielded Cables

2.2.1.1 Synthetic Rubber with Interlocked Armor

Provide multiple-conductor, synthetic-rubber-insulated, interlocked-armor-covered, shielded cable that conforms to NEMA WC 70, ANSI/NEMA WC 71/ICEA S-96-659 and NEMA WC 74/ICEA S-93-639.

Apply close-fitting, interlocked-armor tape of galvanized steel over the jacket.

2.2.1.2 Cross-Linked Polyethylene

Provide multiple-conductor, cross-linked polyethylene-insulated, shielded cable that conforms to NEMA WC 70, ANSI/NEMA WC 71/ICEA S-96-659, NEMA WC 74/ICEA S-93-639 and AEIC CS8. Provide taped shielding that consists of 5-mil thick copper shielding lap applied over 12-mil thick semiconducting tape. Wrap both helically with 10 -percent overlap, providing 100-percent coverage.

Shield cross-linked polyethylene (XLP) single- and multiple-conductor cables for grounded and ungrounded neutral voltage ratings of 2,000 volts or more.

2.2.1.3 Ethylene Propylene Rubber (EPR) with Jacketed Interlocked Armor

Provide multiple-conductor ethylene propylene rubber insulated interlocked armor covered shielded cables that conforms to NEMA WC 70, ANSI/NEMA WC 71/ICEA S-96-659, NEMA WC 74/ICEA S-93-639 and AEIC CS8.

Shield ethylene propylene (EP) or ethylene propylene rubber (EPR), single- and multiple-conductor cables for grounded or ungrounded neutral voltage ratings of more than 8,000 volts.

2.2.2 Multiple-Conductor, Nonshielded Cables

2.2.2.1 Synthetic Rubber with Neoprene Jacket

Provide multiple-conductor, synthetic-rubber-insulated, neoprene-jacketed, nonshielded cable that conforms to NEMA WC 70, ANSI/NEMA WC 71/ICEA S-96-659 and NEMA WC 74/ICEA S-93-639.

2.2.2.2 Cross-Linked Polyethylene with PVC Jacket

Provide multiple-conductor, polyethylene-insulated, nonshielded cable that conforms to NEMA WC 70, ANSI/NEMA WC 71/ICEA S-96-659, NEMA WC 74/ICEA S-93-639 and AEIC CS8.

2.2.2.3 Ethylene-Propylene with PVC Jacket

Provide multiple-conductor, ethylene-propylene-insulated, PVC-jacketed, nonshielded cable that conforms to NEMA WC 70, ANSI/NEMA WC 71/ICEA S-96-659, NEMA WC 74/ICEA S-93-639 and AEIC CS8.

2.2.3 Single-Conductor Shielded Cables

2.2.3.1 Cross-Linked Polyethylene with PVC Jacket

Provide single-conductor, polyethylene-insulated, PVC-jacketed, shielded cable that conforms to NEMA WC 70, ANSI/NEMA WC 71/ICEA S-96-659, NEMA WC 74/ICEA S-93-639 and AEIC CS8.

2.2.3.2 Cross-Linked Polyethylene with Interlocked Armor

Provide single-conductor, polyethylene-insulated, PVC-jacketed, shielded cable with interlocked armor that conforms to NEMA WC 70,

ANSI/NEMA WC 71/ICEA S-96-659, NEMA WC 74/ICEA S-93-639 and AEIC CS8.

Apply a close-fitting, interlocked-armor tape of galvanized steel over the jacket.

2.2.3.3 Ethylene-Propylene-Rubber-Insulated with PVC Jacket

Provide single-conductor 15 kV rated cable assemblies that consist of the following: Class B stranded copper conductors, an extruded semiconducting shield over the conductors, 220 mils of ethylene propylene rubber insulation, an extruded or other approved semiconducting shield, a 5-mil minimum copper tape shield wrapped helically with a minimum 12.5 percent overlap and a PVC jacket.

Provide single-conductor, ethylene-propylene-insulated, PVC-jacketed, shielded cable that conforms to NEMA WC 70, ANSI/NEMA WC 71/ICEA S-96-659, NEMA WC 74/ICEA S-93-639 and AEIC CS8.

2.2.4 Single-Conductor Nonshielded Cables

2.2.4.1 Cross-Linked Polyethylene

Provide single-conductor, cross-linked polyethylene-insulated, nonshielded cable that conforms to NEMA WC 70, ANSI/NEMA WC 71/ICEA S-96-659, and NEMA WC 74/ICEA S-93-639.

2.2.4.2 Ethylene-Propylene-Rubber-Insulated with PVC Jacket

Provide single-conductor, ethylene-propylene-rubber-insulated, PVC-jacketed, nonshielded cable that conforms to NEMA WC 70, ANSI/NEMA WC 71/ICEA S-96-659, and NEMA WC 74/ICEA S-93-639.

2.2.5 Portable Cables

Provide SHD multiple-conductor, butyl-rubber-insulated, neoprene-jacketed, shielded portable cable conforming to NEMA WC 70, ANSI/NEMA WC 71/ICEA S-96-659 and NEMA WC 74/ICEA S-93-639.

2.2.6 Insulated Medium Voltage Connectors

Provide connector with a steel reinforced hook-stick eye, grounding eye, test point, and arc-quenching contact material per IEEE 386. Ensure connections are compatible with equipment bushings. Provide connectors as follows:

a. 200 Ampere loadbreak connector ratings: Voltage: 15kV, 95kV BIL. Short time rating: 10,000 amperes rms, symmetrical for a time duration of 0.17 seconds.

b. 600 Ampere deadbreak connector ratings: Voltage: 15kV, 95kV BIL. Short time rating: 27,000 ampere rms, symmetrical for a time duration of 4.0 seconds.

c. Provide connectors with a steel reinforced hook-stick eye, grounding eye, test point, and arc-quenching contact material per IEEE 386. Provide hot line voltage indicators on all connectors.

Ensure connections are compatible with equipment bushings.

2.2.7 Splices

Provide heat shrink splice kits which are the product of a single manufacturer. Ensure the power cable splice meets the requirements of IEEE 404 for a 15 kV rating, and must be rated by the manufacturer for use on 15 kV class cable systems. Ensure splices are rated for continuous operation at 221 degrees F, with an emergency overload temperature rating of 284 degrees F. Ensure the kit is capable of splicing cables with copper conductors sized as indicated in the contract drawings or accommodate a conductor size transition. Provide splices specifically designed for the cable and grounding provisions.

Provide heat shrink splices which include but are not limited to the following:

a. Inner heat shrink stress control tube with external end sealant, additional heat shrink tube over inner tube and inner tube end sealant.

b. Heat shrink outer wraparound sleeve with heat sensitive indications on both the tube and rail/channel area to indicate proper torch heating, stress relief material, mastic, sealant, shielding mesh, and silicone grease.

2.2.8 Terminations

Provide Class 1 terminations per IEEE 48.

2.2.9 Cable Supports and Fittings

Provide cable supports, related fittings, and accessories for use in corrosive underground locations, such as manholes and utility tunnels, with a factory-applied coating of PVC of at least 20 mils thick. Provide PVC coated items that have a uniform thickness and are free of blisters, breaks, and holidays. Provide PVC compound that conforms to ASTM D746.

Provide cable racks, cable tray supports and related fittings that are UL-listed heavy-duty nonmetallic polycarbonate.

2.2.10 Polyethylene Cable Tags

Provide tags of polyethylene that have an average tensile strength of 4500 pounds per square inch, and are 0.035-inch thick, non-corrosive non-conductive. Ensure tags are resistive to acids, alkalis, organic solvents, salt water, and are distortion resistant to 300 degrees F. Provide a one-piece nylon, self-locking tie at each end of the cable tag. Ensure ties have a minimum loop tensile strength of 175 pounds. Provide cable tags with block letters, numbers, and symbols 1 inch high on a yellow background. Ensure letters, numbers, and symbols do not fall off or change positions regardless of the cable tags orientation.

2.2.11 Fireproof Tape

Provide fireproof tape approximately 30 mils thick by 3 inches wide, consisting of a flexible, unsupported elastomer that expands in fire to provide a thick char buildup between the flame and the cable. Ensure the tape does not give off a smoke when subjected to flames or support combustion. Also, ensure tape does not deteriorate when subjected to oil, water, gases, salt water, sewage and fungus.

2.3 MATERIALS

2.3.1 Conductors

Ensure that conductors conform to the applicable requirements of NEMA WC 70, ANSI/NEMA WC 71/ICEA S-96-659, or NEMA WC 74/ICEA S-93-639.

Ensure that conductors are solid copper core conforming to ASTM B3 and ASTM B8 and that they are bare, or tin-alloy-coated, according to the type of insulation used. Do not intermix copper and aluminum conductors in the same raceway.

Provide Class B stranded conductors.

2.3.2 Insulation

Ensure the provided cables are rated for minimum 221 degrees F continuous conductor temperature and 266 degrees F emergency overload.

Provide cables with 100 percent insulation. Ensure insulation thickness is in accordance with the following:

Voltage Rating (kV)	Insulation Level (%)	Typical Insulation Thickness	
		mm	mils
5	100	2.29	90
	137	2.92	115
	173	3.56	140
8	100	2.92	115
	133	3.56	140
	173	4.45	175
15	100	4.45	175
	133	5.59	220
	173	6.6	260
25	100	6.6	260
	133	8.13	320
	173	10.67	420

Voltage Rating (kV)	Insulation Level (%)	Typical Insulation Thickness	
		mm	mils
35	100	8.76	345
	133	10.67	420
	173	14.73	580

2.3.3 Cable Identification

Provide cables with printing on the outer jacket showing the cable type, name of the manufacturer, the year in which the cable was manufactured, sequential cable reel length markings and a unique number for identification purposes. Closely group the information on the tape at 6 foot maximum intervals to permit complete identification.

2.3.4 Non-metallic Insulation Shield

Provide extruded insulation shield made of an extruded thermoset material compatible with the insulation and jacket. Ensure insulation shield is applied directly over and bonded to the insulation, and complies with AEIC CS8.

2.3.5 Concentric Neutral Shield

Provide copper wires helically applied over the insulation shield, where the minimum total cross sectional area (of the shield wires) is full core conductor for the cable. Minimum size of an individual shield wire is No. 14 AWG.

2.3.6 Jacket

Provide polyethylene (PE) jacketed cable extruded over the cable to a minimum thickness of 80 mils.

2.3.7 Interlock Armored Cable

Provide a nonmetallic, corrosion-resistant jacket over interlock-armored cable that is black polyethylene conforming to NEMA WC 27500, NEMA WC 70, ANSI/NEMA WC 71/ICEA S-96-659 and NEMA WC 74/ICEA S-93-639.

2.4 TESTS, INSPECTIONS, AND VERIFICATIONS

2.4.1 FACTORY TESTING

Submit certified evidence that the cable manufacturer has made factory-conducted tests on each shipping length (reel) of cable. Submit certified copies of test data in accordance with applicable provisions of the referenced standard. Include in tests on each length of cable to include:

(1) Conductor Resistance

(2) Accelerated Water Absorption Test

(3) Water Immersion Test

(4) Ionization

(5) High-Voltage

(6) Partial Discharge Test

Contracting Officer or designee has the option of witnessing required factory testing at no additional cost. Provide a schedule of manufacturing and testing in advance to permit such witnessing, if requested.

Submit certified qualification test reports in accordance with AEIC CS8 made in accordance with the applicable referenced standards. Ensure certified copies of test data show conformance to the requirements of referenced standards and submit for approval prior to shipment of the cable.

Prior to manufacturing, provide data regarding degradation of proposed insulating material and cable performance due to water immersion test as specified in this specification to the Contracting Officer or designee. Indicate in information AC breakdown stress in kV/mm or V/mil versus immersion time. Ensure a complete description and condition under which cable was tested accompanies the test information. Submit an accelerated water absorption test.

PART 3 EXECUTION

3.1 INSTALLATION

Install medium-voltage cables in accordance with NFPA 70, NFPA 70E; and IEEE C2.

Refer to contract provisions for safety submittals and requirements associated with working in the vicinity of energized cables and equipment. The use of arc-flash and shock prevention equipment and personal protective equipment is mandatory.

Notify the Contracting Officer 14 working days prior to an outage that requires testing for phasing and phase rotation of medium voltage electrical systems. The Government will identify and tag the phasing of equipment and provide to the Contractor, in writing, the results of phasing and phase rotation tests. The Contractor is responsible for maintaining the phasing and phase rotation tests, and is responsible for maintaining the phasing, and matching the existing phase rotation and phasing when installing conductors in existing electrical systems.

Install the cables in the following locations:

Exterior:

a. In underground duct banks

b. In conduit above and below grade

c. In manholes

d. And by direct burial

Inside Buildings:

a. By open wire method

b. On insulator hooks

c. On racks

d. In wall and ceiling mounted cable trays

Secure cables with heavy-duty cable ties in existing or new trays mounted horizontally, where the cable rests on the tray bottom. Install cable ties at a minimum of 10 foot intervals.

Secure cables with non-metallic cable clamps, straps, hangers, or other approved supporting devices to tunnel walls, ceilings, and in new or existing cable trays mounted vertically, where the tray bottom is in a vertical plane.

When field cuts or other damage occurs to the PVC coating, apply a liquid PVC patch to maintain the integrity of the coating. After the installation is complete, perform an inspection to ensure that the coating has no voids, pinholes, or cuts.

Before installing new armored cable, ensure that cable trays are properly secured and supported. Add new permanent or temporary tray support devices as required to preclude cable tray failure during cable pulling or after cable is installed.

Installed cable or conductors of a primary distribution system will be rejected by the Government when placed:

a. Openly in cable trays or openly racked along interior walls

b. In the same raceway or conduit with AC/DC control circuits or AC power circuits operating at less than 600 volts

c. In a manner allowing the cable to support its own weight

3.1.1 Protection During Splicing Operations

Provide a blower to force fresh air into manholes or confined areas where free movement or circulation of air is obstructed. Have waterproof protective coverings available on the work site to protect against moisture while a splice is being made. Use pumps to keep manholes dry during splicing operations. Never make a splice or termination with the interior of a cable exposed to moisture. Moisture-test the conductor insulation paper before the splice is made. Use a manhole ring at least 6 inches above ground around the manhole entrance to keep surface water from entering the manhole. Before starting the splice, plug unused ducts and stop water seepage through ducts in use.

3.1.2 Duct Cleaning

Thoroughly clean ducts before installation of power cables. Pull a standard flexible mandrel through each duct to loosen particles of earth, sand, or foreign material in the line. Use a mandrel that is not less than

12 inches long with a diameter 1/2 inch less than the inside diameter of the duct. Then pull a brush with stiff bristles through each duct to remove the loosened particles. Use a brush with a diameter that is the same as or slightly larger than the diameter of the duct.

3.1.3 Pulling Cables in Ducts, Manholes and Utility Tunnels

Submit a Pulling Plan including calculations of pulling tension and side wall pressure anticipated, and the maximum allowable pulling tension for each pull. Do not perform any pull until Government reviews and approves the pulling plan.

Pull medium-voltage cables into ducts and utility tunnels with equipment designed for this purpose, including a power-driven winch, cable-feeding flexible tube guide, cable grips, and lubricants. Employ a sufficient number of trained personnel and equipment to ensure correct installation of the cable.

Set up the cable reel at the side of the manhole or tunnel hatch opening and above the duct or hatch level, allowing the cable to enter through the opening without reverse bending. Install a flexible tube guide through the opening in a manner that prevents the cable from rubbing against the edges of structural members.

Ensure that the pulling force for a cable grip on lead-sheathed cable does not exceed 1,500 pounds per square inch of sheath cross-sectional area. Use a dynamometer in the pulling line to ensure that the pulling force is not exceeded. Ensure that the pulling force for a nonmetallic-sheathed cable does not exceed the smaller of 1,000 pounds or a value computed from the following equation:

TM = 0.036 X N X CM

Where: TM = maximum allowable pulling tension in pounds

N = number of conductors in the cable

CM = cross-sectional area of each conductor in circular mils

3.1.3.1 Allowable Sidewall Pressure

The allowable sidewall pressure is the smaller of 500 pounds per foot of bend radius or the cable manufacturer's recommended maximum value. Show in the pulling plan submittal the calculations for allowable tension and sidewall pressure as well as the anticipated tension and sidewall pressure for each pull in the project.

Unreel cable from the top of the reel, carefully controlling payout. Attach cable to be pulled through a swivel to the main pulling wire by means of a pulling eye installed by the factory or approved cable splicer.

Attach pulling eyes to the cable conductors of the 3-1/C circuit to prevent damage to the cable structure. Pull the entire 3-1/C circuit simultaneously.

3.1.3.2 Minimum Bending Radius

Minimum bending radius during cable pulling operations is 30 inches. For permanent cable bending/racking the minimum bending radius is 12 times

cable diameter.

3.1.3.3 Coating of Cables

Liberally coat cables with a suitable cable-pulling lubricant as it enters the tube guide or duct. Do not use greaser and oil lubricants. Cover nonmetallic sheathed cables with wire-pulling compounds, when required, which have no deleterious effects on the cable. Use rollers, sheaves or tube guides, around which the cable is pulled, conforming to the 30 inches minimum bending radius of the cable during the pulling operations.

3.1.3.4 Pulling Speed

Pull cables into ducts at a speed not to exceed 50 feet per minute and not in excess of maximum permissible pulling tension specified by the cable manufacturer. Cable pulling using a vehicle is not be permitted. Stop pulling operations immediately with any indication of binding or obstruction and do not resume until such difficulty is corrected. Provide sufficient slack for free movement of cable due to expansion or contraction.

3.1.3.5 Cable Splice Support And Sealing

Firmly support cable splices made up in manholes on cable racks as indicated. Do not pull cable splices in ducts. Overlap cable ends at the ends of a section to provide sufficient undamaged cable for splicing. Overlap cables to be spliced in manholes to the centerline of the proposed joint by not less than 2 feet.

Immediately seal cut ends of cables cut in the field to prevent entrance of moisture with heat-shrinkable molded cable end caps.

3.1.4 Splices and Terminations

Make splices in manholes or tunnels except where cable terminations are specifically indicated. Expedite splicing and terminating of cables in order to minimize exposure and cable deterioration.

Use only equipment and materials recommended by the splice manufacturer including calibrated cutting equipment to ensure consistent cut depths when preparing cable ends for the application of the splice kit. Connect the cable concentric neutral/shield wires across one side of the splice by split bundling the splice neutral wiring and connecting each bundle set to a continuous No. 4 AWG solid bare copper conductor via two compression conductors. Ensure the No. 4 AWG conductor extrudes from the cable splice jacket and connects to the manholes grounding system. Make all connections within the splice utilizing long barrel-type compression connectors and appropriate compression tools with proper size dies to ensure a satisfactory mechanical and electrical joint. Ensure bare connections of concentric neutral/shield wires are either contained within the splice kit or sealed via an additional outer covering,consisting of a heavy wall, heat-shrinkable tubing containing adhesive material (mastic) that melts as heat is applied and the outer tubing shrinks to form a moisture proof environmental seal. Provide outer tubing conforming to ANSI C119.1. Ensure splice meets the requirements of IEEE 404 for a 15 kV rating and is rated by the manufacturer for use on 15 kV class feeder cable systems. Take extra precautions to seal around the exit area of the bare copper jumpers with an additional mastic per the splice manufacturer's recommendations.

Terminate cables in approved cable terminations, rated Class 1 per IEEE 48. Dry terminations with medium voltage pennants, preformed, and hand wrapped stress cones can be used for terminating cables. Provide terminations with adequate means for making external connections to the cable conductors of single-conductor cables (phase and concentric neutral), protecting the cable insulation against moisture, oil, or other contaminants. Take extra precautions in physically protecting and supporting cables, and maintaining the insulation level of the cable.

Ensure that installation includes built-up or prefabricated heat or cold shrink stress-relief cones at the terminals of all shielded cables and at the terminals of single-conductor lead-covered cables rated 15 kV and above, ungrounded.

Field-fabricate cable splices from splicing kits supplied by and in accordance with the cable manufacturer's recommendations for the type, size, and electrical characteristics of the cable specified. Locate cable splices in manholes midway between the cable racks on the walls of the manholes and supported with cable arms at approximately the same elevation as the enclosing duct.

If cable splices in the tunnel are not installed in cable trays, install the cable splices on cable racks or by other approved methods that minimize physical stress on the splice connections. Support splices at approximately the same elevation as the installed cable except where space limitations or existing cable length limitations make this method impractical or impossible.

Support all universal demountable splices in a manner that minimizes physical stress on the splice connections. Support each cable end termination using a pair of saddle supports under the cable end termination or cable with a minimum 12 inches and a maximum 30 inches separation between the supports. Secure the cable end termination and cable to the supports in a manner that prevents movement of termination or cable at the support. Install saddle supports on a galvanized steel framing channel that is anchored to the wall, securely fastened to the cable tray, or installed by other approved methods.

3.1.5 Fireproofing

Provide fireproofing (Arc Proofing) for individual cable conductor in manholes, handholes and vaults which carry current at 2200 volts or more.

Tightly wrap strips of fireproofing tape around each cable spirally in half-lapped wrapping. Extend the tape 1 inch into the ducts. To prevent unraveling, random wrap the fireproofing tape the entire length of the fireproofing with pressure-sensitive glass cloth tape.

3.1.6 Cable Tag Installation

Install cable tags in each manhole and at each termination as specified. Install cable tags over the fireproofing and position the tags so that they are clearly visible without disturbing any cabling or wiring in the manholes and equipment.

3.2 FIELD QUALITY CONTROL

After the installation of power cables has been completed, including

splices, joints, and terminations, and before the cable is energized, subject each medium voltage cable to field testing in accordance with the following requirements:

a. Provide test equipment, labor, and trained technical personnel as necessary to perform the electrical acceptance tests.

b. Record all tests on an approved medium voltage cable test form and submit completed forms to the Contracting Officer.

c. Make arrangements to have tests witnessed and approved by the Contracting Officer.

d. Isolate each power-cable installation completely from extraneous electrical connections at cable splices/terminations and joints. Observe all safety precautions.

e. Ensure each power cable is first given an insulation resistance test using a meg-ohmmeter with a voltage output of at least 2,500-volts. Apply test for a long enough time to fully charge the cable (no less than one minute). Record readings as indicated on forms provided. The minimum reading is 5000 megohms at an ambient temperature of 68 degrees F. Correct readings taken at other than 68 degrees F ambient temperatures accordingly.

f. Conform testing to NETA ATS, and NFPA 70B.

Upon successful completion of the insulation resistance test, subject the cable to a Very Low Frequency (VLF) AC high potential test. Adhere general VLF testing measures, parameters, considerations, and results to the following:

a. Ensure test voltage duration is continuous duty for 30 minutes (non-interrupted)

b. Provide the test equipment to test the cable capacity in microfarads.

c. Provide the test equipment to generate the test voltages required for the 30 minute test duration and adhere to the following table:

VLF Test Voltage for Sinusoidal Waveform		
Cable Rating phase to phase	Acceptance (phase to ground test values)	Acceptance (phase to ground test values)
	(New cable)	(Existing cable spliced to new cable)
(rms voltage, KV)	(peak voltage, KV)	(peak voltage, KV)
5	14	10
15	28	22; (EPR TO EPR)

VLF Test Voltage for Sinusoidal Waveform		
Cable Rating phase to phase	Acceptance (phase to ground test values)	Acceptance (phase to ground test values)
	(New cable)	(Existing cable spliced to new cable)
15	15	15; (EPR TO NON-EPR)

d. Ensure the sinusoidal test frequency is 0.1 Hertz.

e. Do not perform test on cable attached to equipment.

Ensure Splices/terminations are clean, dry, and tested per IEEE 48 and IEEE 400.2.

Upon successful completion of the insulation resistance tests, subject the cable to a direct-current high-potential test for 5 minutes applying test voltages in accordance with AEIC CS1 and IEEE 400.2 for paper-impregnated, lead-covered cable; AEIC CS8 and IEEE 400.2 for cross-linked, polyethylene-insulated cable; and AEIC CS8 and IEEE 400.2 for ethylene propylene rubber-insulated cable.

Record leakage current readings every 30 seconds during the first 2 minutes and every minute thereafter for the remainder of the test. When the leakage current continues to increase after the first minute, immediately terminate the test and take steps to find and correct the fault. When a second test becomes necessary, repeat this test procedure.

Upon satisfactory completion of the high-potential test, give the cable a second insulation resistance test as before.

Provide results of the second insulation resistance test that agree with the first test and that indicate no evidence that the cable has been permanently injured by the high-potential test.

Record test data identifying the cable and location, megohm readings versus time, leakage current readings versus time, and cable temperature versus time.

Final acceptance depends upon the satisfactory performance of the cable under test. Do not energize cable until recorded test data has been approved by the Contracting Officer.

Perform radiographic tests on all potheads at the discretion of the Contracting Officer to determine if voids exist in the pothead. Rework unacceptable terminations at no additional expense to the Government.

3.3 CLOSEOUT ACTIVITIES

Provide manufacturer's instructions showing the recommended sequence and method of installation for medium-voltage power cables.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 26 - ELECTRICAL

SECTION 26 05 26.00 40

GROUNDING AND BONDING FOR ELECTRICAL SYSTEMS

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 QUALITY CONTROL
1.3.1 Regulatory Requirements
1.3.2 Standard Products
1.3.3 Ground Resistance Test Equipment
1.3.4 Micro-Ohmmeter Test Equipment

PART 2 PRODUCTS

2.1 MATERIALS
2.1.1 Ground Rods
2.1.2 Ground Wires
2.1.2.1 Bare
2.1.2.2 Insulated
2.1.3 Connectors and Fasteners
2.1.3.1 Exothermic Welds
2.1.3.2 Irreversible Compression Lugs
2.1.3.3 Mechanical
2.1.3.4 Fasteners
2.1.4 Test Wells
2.1.5 Conductive Corrosion Inhibiting Compounds
2.1.6 Ground Buses

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Ground Rods
3.1.2 Conductors
3.1.3 Counterpoise
3.1.4 Ground Buses
3.1.5 Building Grounds
3.1.6 Equipment Grounding
3.1.6.1 Equipment and Enclosure Bonding
3.1.6.2 Bonding of Conduit and Raceway Systems
3.1.6.3 Cable Tray Bonding
3.1.7 Bonding Materials And Methods
3.1.7.1 Brazing
3.1.7.2 Welding
3.1.7.3 Clamping
3.1.7.4 Cleaning of Bonding Surfaces
3.1.7.5 Protection of Finished Bonds
3.2 FIELD QUALITY CONTROL
3.2.1 Bond Resistance Test

3.2.2 Ground Resistance Tests
3.2.3 Ground Isolation Test
3.2.4 Equipment Continuity Test
3.3 CLOSEOUT ACTIVITIES

-- End of Section Table of Contents --

SECTION 26 05 26.00 40

GROUNDING AND BONDING FOR ELECTRICAL SYSTEMS

PART 1 GENERAL

Section 26 41 00 LIGHTNING PROTECTION SYSTEMS applies to work specified in this section.

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN WELDING SOCIETY (AWS)

AWS A3.0M/A3.0	(2020) Standard Welding Terms and Definitions
AWS A5.8/A5.8M	(2019) Specification for Filler Metals for Brazing and Braze Welding
AWS B2.1/B2.1M	(2021) Specification for Welding Procedure and Performance Qualification

ASTM INTERNATIONAL (ASTM)

ASTM B3	(2013) Standard Specification for Soft or Annealed Copper Wire
ASTM B8	(2011; R 2017) Standard Specification for Concentric-Lay-Stranded Copper Conductors, Hard, Medium-Hard, or Soft
ASTM B187/B187M	(2020) Standard Specification for Copper, Bus Bar, Rod and Shapes and General Purpose Rod, Bar and Shapes

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 81	(2012) Guide for Measuring Earth Resistivity, Ground Impedance, and Earth Surface Potentials of a Ground System
IEEE C2	(2023) National Electrical Safety Code

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

ANSI/NEMA GR 1	(2007) Grounding Rod Electrodes and Grounding Rod Electorode Couplings

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National Electrical Code

NFPA 780 (2023) Standard for the Installation of Lightning Protection Systems

TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)

TIA-607 (2019d) Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises

U.S. DEPARTMENT OF DEFENSE (DOD)

MIL-STD-889 (2021; Rev D) Galvanic Compatibility of Electrically Conductive Materials

UNDERWRITERS LABORATORIES (UL)

UL 467 (2022) UL Standard for Safety Grounding and Bonding Equipment

UL 546 (2008) UL Outline of Investigation for Conductor Termination Compounds

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-03 Product Data

Ground Rods; G

Ground Wires; G

Connectors and Fasteners; G

Test Wells; G

Conductive Corrosion Inhibiting Compounds; G

Ground Buses; G

SD-06 Test Reports

Bond Resistance Test; G

Ground Resistance Tests; G

Ground Isolation Test; G

Equipment Continuity Test; G

SD-07 Certificates

Ground Resistance Test Equipment; G

Micro-Ohmmeter Test Equipment; G

SD-11 Closeout Submittals

Record Drawings

1.3 QUALITY CONTROL

1.3.1 Regulatory Requirements

In each of the publications referred to herein, consider the advisory provisions to be mandatory, as though the word, "shall" had been substituted for "should" wherever it appears. Interpret references in these publications to the "authority having jurisdiction," or words of similar meaning, to mean the Contracting Officer. Ensure equipment, materials, installation, and workmanship are in accordance with the mandatory and advisory provisions of NFPA 70, IEEE C2 unless more stringent requirements are specified or indicated.

1.3.2 Standard Products

Provide materials and equipment that are products of manufacturers regularly engaged in the production of such products which are of equal material, design and workmanship. Provide products which have been in satisfactory commercial or industrial use for 2 years prior to bid opening. Ensure the 2-year period includes applications of equipment and materials under similar circumstances and of similar size. Ensure the product has been on sale on the commercial market through advertisements, manufacturers' catalogs, or brochures during the 2-year period. Where two or more items of the same class of equipment are required, these items must be products of a single manufacturer.

1.3.3 Ground Resistance Test Equipment

Provide combination 3-point and 4-point type ground resistance test equipment specifically designed for grounding electrode resistance and soil resistivity tests. Submit proof of current equipment calibration with test equipment product data.

1.3.4 Micro-Ohmmeter Test Equipment

Perform bond resistance tests using a micro-ohmmeter with the following characteristics:

a. Resistance range selectable and capable of measuring to 10 micro-Ohms using a minimum of 1 ampere of test current.

b. Positive and negative test leads of the 2-wire balanced type. Provide both clamp and probe type connections to allow measurements across all bonded surfaces. Provide long length balanced test lead to allow measurements from a bonding location to the nearest test well.

Submit proof of current equipment calibration with test equipment product data.

PART 2 PRODUCTS

Submit material, equipment, and fixture lists for grounding systems, including manufacturer's style or catalog numbers, specification and drawing reference numbers, warranty information, and fabrication site

information.

2.1 MATERIALS

2.1.1 Ground Rods

Provide ground rods of copper conforming to UL 467 and ANSI/NEMA GR 1. Ensure ground rods are not less than 3/4 inch in diameter and 10 feet in length.

Where ground rod length is greater than 10 feet, provide sectional type ground rods with each section 10 feet in length. Join sectional type ground rods using exothermic welding completely around both rod/coupling joints. Ensure ground rods have cone-shaped point on the end of the first section driven into the ground.

Provide ground rods and ground rod sections die-stamped near the top with the name or trademark of the manufacturer and the length of the segment in feet.

2.1.2 Ground Wires

2.1.2.1 Bare

Provide annealed bare copper, Class "B" stranded ground and bond wires in accordance with ASTM B8 for wires #4 AWG and larger and solid in accordance with ASTM B3 for wires #6 AWG and smaller. Provide conductors with 98 percent conductivity and sized wires in accordance with the requirements of NFPA 70 and NFPA 780.

2.1.2.2 Insulated

Ensure insulated conductors conform to the requirements of Section 26 05 00.00 40 COMMON WORK RESULTS FOR ELECTRICAL.

Where installed in conduit as part of a complete circuit provide conductors with green insulation for sizes #8 AWG and smaller and with green phase tape at each end and in each junction box for sizes #6 AWG and larger.

2.1.3 Connectors and Fasteners

2.1.3.1 Exothermic Welds

Ensure the molds, materials and powder charges used to make exothermic welds are the standard product of a single manufacturer and listed by the manufacturer for use on the specific type, size, quantity and configuration of conductors to which the weld is applied.

2.1.3.2 Irreversible Compression Lugs

Provide irreversible compression lug type connectors manufactured from tin-plated copper and installed using a hydraulic compression tool and die to apply correct, uniformly distributed, circumferential pressure. Ensure tools and dies are as recommended by the irreversible compression lug type connector manufacturer. Use an embossing die code or other standard method to provide visible indication that a connector has been adequately compressed onto the conductor. Apply irreversible compression lug type connectors in strict accordance with the manufacturer's written

instructions and published installation instructions. Use 2-hole lug type connectors for connections to NEMA cable pads and bus bars, and single-hole connectors otherwise.

2.1.3.3 Mechanical

Provide split bolt and clamp style mechanical type connectors manufactured from copper, listed by the manufacturer as suitable for direct burial use. Ensure mechanical type connectors are applied in strict accordance with the manufacturer's published installation instructions.

2.1.3.4 Fasteners

Provide bolts, nuts, washers, lock washers, and associated fasteners used for grounding and bonding connections manufactured of copper. Where fasteners contact dissimilar metals, apply conductive oxide-inhibiting compound.

2.1.4 Test Wells

Provide test wells that are H2O rated, precast reinforced concrete, circular, with open bottom and concrete or cast iron lid/frame. Ensure test wells have inside dimensions of not less than 12 inches in diameter by 24 inches deep. Provide test well lid with cast "GROUND" legend.

2.1.5 Conductive Corrosion Inhibiting Compounds

Provide conductive corrosion inhibiting compounds UL Listed in accordance with UL 546, listed by the manufacturer as suitable for the application, and suitable for all aluminum and copper conductor/connector applications. Ensure conductive corrosion inhibiting compounds inhibit oxidation at the conductor/connector interface and have no deleterious effect on the conductor/connector metal or EPDM, natural rubber, or polyethylene insulating materials.

2.1.6 Ground Buses

Provide solid copper ground buses conforming to ASTM B187/B187M with minimum dimensions of 0.25 inches thick, 4 inches wide, and 12 inches in length or as indicated. Ensure ground buses are equipped with two UL Recognized red 1000V rated insulated standoffs and stainless steel mounting brackets.

Provide Telecommunications Main Ground Buses and Telecommunications Ground Buses in meeting the standards of TIA-607.

Provide grounding buses with predrilled NEMA hole configuration as indicated.

PART 3 EXECUTION

3.1 INSTALLATION

Install grounding systems in accordance with NFPA 70, NFPA 780 and IEEE C2, and as indicated.

Bond exposed non-current-carrying metallic parts of electrical equipment and metallic raceway systems to ground.

Bond grounding conductors in metallic and non-metallic raceways to ground. Make ground connections at equipment and to ground rods as indicated. Interconnect all grounding media in or on the structure to provide a common ground potential. This includes lightning protection, electrical service, telecommunications system grounds, as well as underground metallic piping systems.

Bond wiring system neutrals to ground in accordance with the requirements of NFPA 70. Where ground fault protection is employed, ensure that connection of ground and neutral does not interfere with correct operation of fault protection.

Counterpoise ground systems consist of a series of ground rods with a direct buried grounding conductor loop, configured to minimize the number of dead-ends, interconnecting the individual ground rods. Provide ground rods in the locations indicated.

3.1.1 Ground Rods

Install ground rods so that the top of the rod is 4 inches above grade.

3.1.2 Conductors

Install bare or insulated conductors as indicated. Install bare conductors where not specifically identified as bare or insulated except where installed in conduit with associated phase conductors. Install insulated conductors in conduit with insulation of the same material as the associated phase conductors with which it is installed.

Provide straps/jumpers across joints subject to vibration. Install strap/jumper such that vibration will not change its electrical characteristics. Apply strap/jumper to the metallic structure on each side of the joint; do not penetrate any adjacent parts. Install straps/jumpers in areas that are accessible for maintenance. Install strap/jumper such that it does not restrict the movement of the metallic structures to which it is connected. Install strap/jumper such that it does not weaken the metallic structures to which it is attached. Do not connect two or more straps/jumpers in series.

3.1.3 Counterpoise

Install No. 4/0 AWG bare copper counterpoise grounding conductor direct buried outside of the structure drip line, within 24 to 72 inches of the structure foundation, with a minimum of 18 inches of earth cover. Install counterpoise grounding conductor in earth undisturbed by excavation, not earth fill, and do not locate beneath roof overhang, or wholly under paved areas or roadways where rainfall cannot penetrate to keep soil moist in the vicinity of the conductor.

Install ground rods vertically into the earth not less 10 feet with top of ground rod not less than 18 inches below finished grade. Bond ground rods to counterpoise grounding conductor at intervals no less than 20 linear feet nor greater than 40 linear feet of ground counterpoise cable.

3.1.4 Ground Buses

Install ground busses in accordance with manufacturer's instructions.

3.1.5 Building Grounds

Install No. 4/0 AWG bare copper ground conductor from concrete encased foundation rebar and every corner column and intermediate exterior column to counterpoise. Connect ground conductors to columns and counterpoise using exothermic welds.

Install one conductor a minimum of every 60 feet of concrete foundation perimeter. Connect ground conductors to columns and counterpoise using exothermic welds.

3.1.6 Equipment Grounding

Install ground systems for power, telecommunications, and instrumentation. Independently connect each system to the building counterpoise.

3.1.6.1 Equipment and Enclosure Bonding

Bond each metallic enclosure and all electrical equipment to ground. Make at least one copper connection from the system ground point to one or more enclosures in the area such that all enclosures and equipment provide a low-impedance path to ground when properly bonded together.

Individually and directly connect indoor substations, transformers, switchboard frames, switchgear assemblies, motors, motor control centers, air compressors, air handlers, refrigerated air dryers, generators, frames and tracks of cranes, and to the building ground. Ensure the current-carrying capacity of the grounding conductor is the same as the current-carrying capacity of the power conductors for circuits utilizing power lines size No. 2 AWG and smaller. For circuits with power wiring larger than No. 2 AWG, ensure the grounding conductor is in accordance with NFPA 70.

3.1.6.2 Bonding of Conduit and Raceway Systems

Bond all metal conduit, fittings, junction boxes, outlet boxes, armored and metal sheathed cable, and other raceways. Ensure adequate electrical contact at the joints and terminations. Ensure metallic raceway systems have electrical continuity with equipment. Individually and directly connect equipment to the building ground, independent of the raceway system.

For rigid metal conduit and terminations, ensure threaded connections are wrench-tight with no exposed threads. Ream all ends of the conduit to remove burrs and rough edges. Bond conduits entering boxes and enclosures to the box with locknuts and grounding-type bushings. Locknuts that gouge into the metal box when tightened are not acceptable.

Conduit systems that are interrupted by PVC dielectric links are bonded separately on either side of the link. Do not jumper the dielectric link.

Install flexible metal conduit with an integral grounding conductor.

3.1.6.3 Cable Tray Bonding

Bond cable tray sections together. Cable tray sections in tandem assembly are considered as having electrical continuity when these sections are bonded with the appropriate bolts. Install bond straps across expansion

joints. Bond cable trays to the building ground system.

3.1.7 Bonding Materials And Methods

Accomplish bonding of metal surfaces by welding .

3.1.7.1 Brazing

Ensure brazing solder conforms to AWS A5.8/A5.8M .

3.1.7.2 Welding

Weld using the exothermic process with procedures conforming to AWS A3.0M/A3.0, AWS B2.1/B2.1M, and manufacturer's recommendation. Where dissimilar metals are to be joined via exothermic weld, follow the weld kit manufacturer's recommendations and published instructions. Ensure connections between dissimilar metals do not produce galvanic action in accordance with MIL-STD-889.

Use welding processes of the exothermic fusion type that makes a connection without corroding or loosening. Ensure process joins all strands and does not cause the parts to be damaged or weakened. Completed connection or joint is equal or larger in size than the conductors joined and has the same current-carrying capacity as the largest conductor. Paint the buried ground connections with a bitumastic paint.

3.1.7.3 Clamping

In external locations, use clamping only where a disconnect type of connection is required. Connection device may utilize threaded fasteners. Construct device such that positive contact pressure is maintained at all times. Use machine bolts with tooth-type lockwashers.

3.1.7.4 Cleaning of Bonding Surfaces

Thoroughly clean surfaces that comprise the bond before joining. Apply an appropriate abrasive with gentle and uniform pressure to ensure a smooth and uniform surface. Do not remove excessive metal from the surface. Clean clad metals in such a manner that the cladding material is not penetrated by the cleaning process. Then clean bare metal with an appropriate solvent to remove any grease, oil, dirt, corrosion preventives, and other contaminants. Bond to the cleaned area within one hour after cleaning. Seal joint and refinish the exposed surfaces within two hours of exposure to prevent oxidation. When additional time is required, apply a corrosion preventive compound until the area can be refinished.

3.1.7.5 Protection of Finished Bonds

Protect finished bonds by painting to match the original finish after the bond is made.

3.2 FIELD QUALITY CONTROL

Perform the following tests in the presence of the Contracting Officer. Furnish test equipment and personnel and submit written results of each test. Notify the Contracting Officer at least 14 calendar working days prior to each test.

Submit written results of each test to Contracting Officer for review and approval. Document each location where test is performed, the field conditions at the time of the test, the measured results of the test, and whether the measured results "PASSED" or "FAILED" relative to specified pass/fail performance criteria.

Perform rework to correct FAILED conditions at no additional cost to the Government.

3.2.1 Bond Resistance Test

Resistance of any bond connection cannot exceed 0.5 milliohm. Rework bonds that exceed this resistance at no additional cost to the Government.

3.2.2 Ground Resistance Tests

Test grounding systems for ground resistance. Total resistance from any point on the ground network to the building counterpoise cannot exceed 50 milliohms.

Make ground resistance and counterpoise tests during dry weather, and no sooner than 48 hours after rainfall. Conduct tests using the ratio method that measures the ratio of the resistance to earth of an auxiliary test electrode to the series resistance of the electrode under test and a second auxiliary electrode. Perform measurements in accordance with IEEE 81.

3.2.3 Ground Isolation Test

Test ground systems for isolation from other ground systems.

3.2.4 Equipment Continuity Test

Test connection from electrical distribution equipment including panelboards, switchboards, transformers, substations, and motor control centers to counterpoise. Measure and record the circuit resistance between electrical equipment ground connections and the counterpoise. The circuit resistance shall not exceed 5 Ohms.

3.3 CLOSEOUT ACTIVITIES

Submit record drawings indicating the location of ground rods, mats, grids, building ground bus, supplementary grounding electrodes, steel building columns, and other metal structures connected to the grounding system.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 26 - ELECTRICAL

SECTION 26 05 71.00 40

LOW VOLTAGE OVERCURRENT PROTECTIVE DEVICES

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION
2.2 EQUIPMENT
2.2.1 Motor Controllers
2.2.1.1 Manual Motor Controllers
2.2.1.2 Magnetic Motor Controllers
2.2.1.3 Combination Motor Controllers
2.2.2 Circuit Breakers
2.2.2.1 Molded-Case Circuit Breakers
2.2.2.2 Enclosed Molded-Case Circuit Breakers
2.2.3 Fuses
2.2.4 Control Devices
2.2.4.1 Magnetic Contactors
2.2.4.2 Control-Circuit Transformers
2.2.4.3 Magnetic Control Relays
2.2.4.4 Pushbuttons and Switches
2.2.5 Finish
2.3 COMPONENTS
2.3.1 Instrument Transformers
2.3.1.1 Current Transformers
2.3.1.2 Potential Transformers
2.3.2 Enclosures
2.3.2.1 Equipment Enclosures
2.3.2.2 Remote-Control Station Enclosures
2.3.3 Time Switches
2.3.4 Protective Relays
2.3.4.1 Overcurrent Relays
2.3.4.2 Directional Overcurrent Relays
2.3.4.3 Reclosing Relays
2.3.4.4 Undervoltage Relays
2.3.5 Indicating Instruments
2.3.5.1 Ammeters
2.3.5.2 Voltmeters
2.3.5.3 Watt-Hour Meters/Wattmeters
2.3.5.4 Graphic Demand Meters
2.3.5.5 Specialty-Type Meters
2.3.6 Indicating Lights
2.3.6.1 General-Purpose Type
2.3.6.2 Switchboard Indicating Lights

PART 3 EXECUTION

3.1 INSTALLATION
3.2 FIELD QUALITY CONTROL
3.2.1 Tests

-- End of Section Table of Contents --

SECTION 26 05 71.00 40

LOW VOLTAGE OVERCURRENT PROTECTIVE DEVICES

PART 1 GENERAL

Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM applies to work specified in this section.

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

ANSI C12.1	(2014; Errata 2016) Electric Meters - Code for Electricity Metering

ASTM INTERNATIONAL (ASTM)

ASTM A240/A240M	(2020a) Standard Specification for Chromium and Chromium-Nickel Stainless Steel Plate, Sheet, and Strip for Pressure Vessels and for General Applications
ASTM D877/D877M	(2019) Standard Test Method for Dielectric Breakdown Voltage of Insulating Liquids Using Disk Electrodes

ELECTRONIC INDUSTRIES ALLIANCE (EIA)

EIA 443	(1979) NARM Standard for Solid State Relays Service

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE C37.17	(2012) Standard for Trip Devices for AC and General-Purpose DC Low-Voltage Power Circuit Breakers
IEEE C37.90	(2005; R 2011) Standard for Relays and Relay Systems Associated With Electric Power Apparatus
IEEE C57.13	(2016) Standard Requirements for Instrument Transformers
IEEE C63.2	(2009) Standard for Electromagnetic Noise and Field Strength Instrumentation, 10 Hz to 40 GHz - Specifications
IEEE C63.4	(2014) American National Standard for Methods of Measurement of Radio-Noise Emissions from Low-Voltage Electrical and

	Electronic Equipment in the Range of 9 kHz to 40 GHz

IPC - ASSOCIATION CONNECTING ELECTRONICS INDUSTRIES (IPC)

IPC D330	(1992) Design Guide Manual

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

ANSI C78.23	(1995; R 2003) American National Standard for Incandescent Lamps - Miscellaneous Types
NEMA 250	(2020) Enclosures for Electrical Equipment (1000 Volts Maximum)
NEMA AB 3	(2013) Molded Case Circuit Breakers and Their Application
NEMA FU 1	(2012) Low Voltage Cartridge Fuses
NEMA ICS 1	(2000; R 2015) Standard for Industrial Control and Systems: General Requirements
NEMA ICS 2	(2000; R 2020) Industrial Control and Systems Controllers, Contactors, and Overload Relays Rated 600 V
NEMA ICS 6	(1993; R 2016) Industrial Control and Systems: Enclosures

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National Electrical Code

UNDERWRITERS LABORATORIES (UL)

UL 20	(2018; Reprint Jan 2021) UL Standard for Safety General-Use Snap Switches
UL 50	(2015) UL Standard for Safety Enclosures for Electrical Equipment, Non-Environmental Considerations
UL 489	(2016; Rev 2019) UL Standard for Safety Molded-Case Circuit Breakers, Molded-Case Switches and Circuit-Breaker Enclosures
UL 508	(2018; Reprint Jul 2021) UL Standard for Safety Industrial Control Equipment

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Connection Diagrams; G

Fabrication Drawings; G

Control Devices; G

Protective Devices; G

SD-03 Product Data

Fuses; G

Motor Controllers; G

Instrument Transformers; G

Enclosures; G

Circuit Breakers; G

Control Devices; G

Time Switches; G

Protective Relays; G

Indicating Instruments; G

Indicating Lights; G

SD-06 Test Reports

Dielectric Tests; G

Final Test Reports; G

SD-07 Certificates

Insulating Oil; G

SD-08 Manufacturer's Instructions

Control Devices; G

Protective Devices; G

SD-10 Operation and Maintenance Data

Manual Motor Controllers; G

Magnetic Motor Controllers; G

Combination Motor Controllers; G

Circuit Breakers; G

Time Switches; G

Protective Relays; G

Indicating Instruments; G

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION

Submit connection diagrams showing the relations and connections of control devices and protective devices by showing the general physical layout of all controls, the interconnection of one system (or portion of system) with another, and internal tubing, wiring, and other devices.

Submit fabrication drawings for control devices and protective devices consisting of fabrication and assembly details performed in the factory.

2.2 EQUIPMENT

2.2.1 Motor Controllers

Conform to NEMA ICS 1, NEMA ICS 2, and UL 508 for motor controllers. Ensure controllers have thermal overload protection in each phase.

2.2.1.1 Manual Motor Controllers

Provide full-voltage, manually operated manual motor controllers for the control and protection of single-phase 60-Hz ac fractional-horsepower squirrel-cage induction motors.

Provide single-throw, single- or double-pole, three-position controllers rated at not more than 1 horsepower at 115 V and 230 V single-phase. Include a supporting base or body of electrical insulating material with enclosed switching mechanism, yoke, thermal-overload relay, and terminal connectors. Provide controllers that clearly indicate operating condition: on, off, or tripped.

Provide toggle- or key-operated-type manual motor controllers as indicated and arrange them so that they are lockable with a padlock in the "OFF" position.

Provide recessed manual motor controllers for single-speed, fractional-horsepower, squirrel-cage induction motors. Include a single controller and indicating light in a 4-inch-square wall outlet box; for flush-wiring devices, include matching corrosion-resistant steel flush cover plates. Provide surface-mounted manual motor controllers for single-speed, fractional-horsepower squirrel-cage induction motors that include a single controller and indicating light in a NEMA 250, Type 1 , general-purpose enclosure.

Provide recessed and surface-mounted manual motor controllers for two-speed, fractional-horsepower, squirrel-cage induction motors; include two controllers, two indicating lights, and a selector switch in a multiple-gang wall outlet box for flush-wiring devices, with matching corrosion-resistant steel flush cover plates. Provide surface-mounted manual motor controllers for two-speed, fractional-horsepower, squirrel-cage induction motors; include two controllers, two indicating lights, and a selector switch in a NEMA 250, Type 1 , general-purpose enclosure.

2.2.1.2 Magnetic Motor Controllers

a. Full-Voltage Controllers

Provide full-voltage, full-magnetic devices for the control and protection of single- and three-phase, 60 Hz, squirrel-cage induction motors in accordance with NEMA ICS 1, NEMA ICS 2, and UL 508 for magnetic motor controllers.

Ensure that the operating coil assembly operates satisfactorily between 85 percent and 110 percent of rated coil voltage. Provide 120 V, 60 Hz motor control circuits.

Provide the controllers with two normally open and two normally closed auxiliary contacts rated according to NEMA ICS 1 and NEMA ICS 2, in addition to the sealing-in contact for the control circuits.

Provide solderless pressure wire terminal connectors for line and load connections to the controllers.

Include three manual-reset thermal-overload devices for overcurrent protection, one in each pole of the controller. Provide thermal-overload relays of the bimetallic nonadjustable type with continuous-current ratings and service-limit current ratings. Ensure that ratings have a plus or minus 15 percent adjustment to compensate for ambient operating conditions.

Provide an externally operable manual-reset button to reestablish control power to the holding coil of the electromagnet. After the controller has tripped from overload, ensure that resetting the motor-overload device does not restart the motor.

b. Reduced-Voltage Starters

Conform to the requirements for full-voltage controllers for reduced-voltage starters, except for voltage, and to the following additional requirements:

(1) Fully protect the motor during all phases of motor starting with an overload device in each motor leg. Rate the starter contacts to withstand the switching surges during selector to full voltage. Provide a starter that contains the sensing and timing devices necessary to monitor motor operation and select the correct time for selector to full voltage.

(2) Ensure adequate ventilation of resistors and autotransformers used for starting. Ventilate solid-state starters for starting cycles as well as any follow-on restart-run cycles. Operate external control circuits or solid-state starters at a maximum of 120 V ac.

(3) For solid-state starters, provide adjustable starting torque from 0 percent to 50 percent of applied voltage, minimum. Provide autotransformer starters with a minimum of three taps above 50 percent reduced voltage.

2.2.1.3 Combination Motor Controllers

The following requirements are in addition to the requirements specified

for magnetic motor controller:

a. Provide combination motor controllers for the control and protection of single- and three-phase, 60 Hz ac squirrel-cage induction motors with branch-circuit disconnecting and protective devices in accordance with NEMA ICS 1, NEMA ICS 2, and NEMA ICS 6.

b. For combination motor controllers, include magnetic motor controllers and molded-case circuit breakers or motor circuit protectors (MCPs) in metal enclosures in accordance with NEMA 250 or motor control center draw-out assemblies with control-power transformers, selector switches, pushbuttons, and indicating lights as follows:

(1) Provide full-voltage, full-magnetic devices as specified in this section under paragraph REMOTE-CONTROL STATION ENCLOSURES for magnetic motor controllers and enclosures.

(2) Provide thermal-magnetic breakers as specified in paragraph MANUAL MOTOR CONTROLLERS for molded-case circuit breakers. Manufacturer's standard MCPs may be used in lieu of molded-case circuit breakers.

(3) Provide control-power transformers 120 V ac maximum, selector switches, pushbuttons, and pilot lights as required.

(4) Identify combination motor controllers with identification plates affixed to the front cover of the controller.

a. Nonreversing Combination Motor Controllers

The following requirements are in addition to the requirements for magnetic motor controllers:

(1) For the control and protection of single-speed squirrel-cage induction motors, include a magnetic controller with molded-case circuit breaker or MCPs with selector switch or start/stop pushbutton and indicating light in the cover of the enclosure.

(2) Provide rating of single and three-phase, single-speed, full-voltage magnetic controllers for nonplugging and nonjogging duty in accordance with NEMA ICS 1 and NEMA ICS 2.

(3) Provide wiring and connections for full-voltage, single-speed magnetic controllers in accordance with NEMA ICS 1 and NEMA ICS 2.

b. Reversing Combination Motor Controllers

The following requirements are in addition to the requirements for magnetic motor controllers:

(1) For the control and protection of single-speed squirrel-cage induction motors, include two interlocked magnetic controllers with molded-case circuit breaker or MCPs, with selector switch or forward/reverse/stop pushbutton and two indicating lights in the cover of the enclosure. Provide indicating lights to identify the forward and reverse running connection of the motor controller.

(2) Provide rating of single and three-phase, single-speed, full-voltage magnetic controllers for plug-stop, plug-reverse, or

jogging duty in accordance with NEMA ICS 1 and NEMA ICS 2.

(3) Provide wiring and connections for full-voltage, single-speed magnetic controllers in accordance with NEMA ICS 1 and NEMA ICS 2.

c. Two-Speed Combination Motor Controllers

The following requirements are in addition to the requirements for magnetic motor controllers:

(1) For the control and protection of single- and two-winding, two-speed, three-phase, squirrel-cage induction motors, include two magnetic controllers with molded-case circuit breaker or MCPs, with selector switch or fast/slow/stop pushbutton and two indicating lights in the cover of the enclosure. Provide indicating lights to identify the high- and low-speed running connection of the motor controller.

(2) Provide rating of three-phase, two-speed, full-voltage magnetic controllers for nonplugging and nonjogging duty for constant- and variable-torque motors in accordance with NEMA ICS 1 and NEMA ICS 2.

(3) Provide rating of three-phase, two-speed, full-voltage magnetic controllers for nonplugging and nonjogging duty for constant-horsepower motors in accordance with NEMA ICS 1 and NEMA ICS 2.

(4) Provide rating of three-phase, two-speed, full-voltage magnetic controllers for plug-stop, plug-reverse, or jogging duty for constant-torque, variable-torque, and constant-horsepower motors in accordance with NEMA ICS 1 and NEMA ICS 2.

2.2.2 Circuit Breakers

Provide circuit breakers that conform to UL 489 and NEMA AB 3.

2.2.2.1 Molded-Case Circuit Breakers

Provide molded-case, manually operated, trip-free circuit breakers, with inverse-time thermal-overload protection and instantaneous magnetic short-circuit protection as required. Completely enclose circuit breakers in a molded case, with a factory-sealed, calibrated sensing element to prevent tampering.

Locate thermal-magnetic tripping elements in each pole of the circuit breaker, and provide inverse-time-delay thermal-overload protection and instantaneous magnetic short-circuit protection. Provide an instantaneous magnetic tripping element that is adjustable and accessible from the front of the breaker on frame sizes larger than 100 A.

Size the breaker as required for the continuous-current rating of the circuit. Provide the breaker class as required.

Provide sufficient interrupting capacity of the panel and lighting branch circuit breakers to successfully interrupt the maximum short-circuit current imposed on the circuit at the breaker terminals. Provide circuit breaker interrupting capacities with a minimum of 10,000 A and that conform to NEMA AB 3.

Provide the common-trip-type multipole circuit breakers having a single

operating handle and a two-position on/off indication. Provide circuit breakers with temperature compensation for operation in an ambient temperature of 104 degrees F. Provide circuit breakers that have root mean square (rms) symmetrical interrupting ratings sufficient to protect the circuit being supplied. Interrupting ratings may have selective-type tripping (time delay, magnetic, thermal, or ground fault).

Provide a phenolic-composition breaker body capable of having such accessories as handle-extension, handle-locking, and padlocking devices attached where required.

For meter circuit disconnects, provide circuit breakers of the motor-circuit-protector type that meet the applicable requirements of NFPA 70.

For service disconnection, provide enclosed circuit-breakers with external handles for manual operation. Provide sheet-metal enclosures with hinged covers suitable for surface mounting.

2.2.2.2 Enclosed Molded-Case Circuit Breakers

For enclosed circuit breakers, provide thermal-magnetic, molded-case circuit breakers in surface-mounted, nonventilated enclosures conforming to NEMA 250 and UL 489.

Provide enclosed circuit breakers in nonhazardous locations as follows:

a. Contain circuit breakers installed inside clean, dry locations in NEMA Type 1, general purpose, sheet-steel enclosures.

b. Contain circuit breakers installed in unprotected outdoor locations, in NEMA Type 3R, weather-resistant sheet-steel enclosures that are splashproof, weatherproof, sleetproof, and moisture-resistant.

c. Contain circuit breakers installed in wet locations, in NEMA Type 4, watertight corrosion-resistant, sheet-steel enclosures constructed to prevent entrance of water.

d. Contain circuit breakers installed in dry, noncombustible, dust-laden atmospheres in NEMA Type 5, dusttight, corrosion-resistant sheet steel enclosures, with gaskets or their equivalent to prevent the entrance of dust.

e. Contain circuit breakers installed in industrial locations in NEMA Type 12, industrial-use, sheet-steel enclosures, constructed to prevent the entrance of dust, lint, fibers, and flyings and the seepage of oil and coolant.

f. Fabricate steel enclosures from corrosion-resistant sheet-steel, conforming to ASTM A240/A240M, 300-series, corrosion-resistant steel. Ensure that the box dimensions and thickness of the sheet steel conform to UL 50.

2.2.3 Fuses

Provide a complete set of fuses for all switches and switchgear. Ensure that fuses have a voltage rating of not less than the circuit voltage.

Make no change in continuous-current rating, interrupting rating, or

clearing or melting time of fuses unless written permission is first obtained from the Contracting Officer.

Provide nonrenewable-cartridge-type fuses for ratings 30 A, 125 V or less. Provide renewable-cartridge-type fuses for ratings above 30 A 600 V or less with time-delay dual elements, except where otherwise indicated. Ensure that fuses conform to NEMA FU 1.

Install special fuses such as extra-high interrupting-capacity fuses, fuses for welding machines, and capacitor fuses where required. Do not use plug fuses.

Label fuses showing UL class, interrupting rating, and time-delay characteristics, when applicable.

Provide porcelain fuse holders when field-mounted in a cabinet or box. Do not use fuse holders made of such materials as ebony asbestos, Bakelite, or pressed fiber for field installation.

2.2.4 Control Devices

2.2.4.1 Magnetic Contactors

Provide magnetic contactors in accordance with NEMA ICS 1 and NEMA ICS 2 as required for the control of low-voltage, 60-Hz, tungsten-lamp loads, fluorescent-lamp loads, resistance-heating loads, and the primary windings of low-voltage transformers.

Provide core-and-coil assembly that operates satisfactorily with coil voltage between 85 percent and 110 percent of its voltage rating.

Provide contactors that are designed with a normally open holding-circuit auxiliary contact for control circuits, with a rating in accordance with NEMA ICS 1 and NEMA ICS 2.

Furnish solderless pressure wire terminal connectors, or make available for line and load connections to contactors in accordance with NEMA ICS 1 and NEMA ICS 2.

Provide magnetic contactors with a rating in accordance with NEMA ICS 1 and NEMA ICS 2.

2.2.4.2 Control-Circuit Transformers

Provide control-circuit transformers within the enclosure of magnetic contactors and motor controllers when the line voltage exceeds 120 V. Provide an encapsulated dry-type, single-phase, 60-Hz transformer, with a 120 V (or 24 V) isolated secondary winding.

Do not provide a transformer with a rated primary voltage less than the rated voltage of the controller, or a rated secondary current less than the continuous-duty current of the control circuit.

Provide voltage regulation of the transformer such that, with rated primary voltage and frequency, the secondary voltage is not less than 95 percent nor more than 105 percent of rated secondary voltage.

Provide a source of supply for control-circuit transformers at the load side of the main disconnecting device. Protect the secondary winding of

the transformer and control-circuit wiring against overloads and short circuits, with fuses selected in accordance with NEMA ICS 6. Ground the secondary winding of the control-circuit transformer in accordance with NEMA ICS 6.

2.2.4.3 Magnetic Control Relays

Provide magnetic control relays for energizing and de-energizing the coils of magnetic contactors or other magnetically operated devices, in response to variations in the conditions of electric control devices in accordance with NEMA ICS 1, and NEMA ICS 2.

Ensure that the core-and-coil assembly operates satisfactorily with coil voltages between 85 percent and 110 percent of their voltage rating.

Provide relays that are designed to accommodate normally open and normally closed contacts.

Provide 120 V, 60-Hz, magnetic control relays with a continuous--contact rating of 10 A, and with current-making and -breaking ability in accordance with NEMA ICS 1 and NEMA ICS 2, two normally open and two normally closed.

2.2.4.4 Pushbuttons and Switches

a. Pushbuttons

For low-voltage ac full-voltage magnetic pushbutton controllers, provide heavy-duty, oiltight NEMA 250, Type 12 , momentary-contact devices rated 600 V, with pilot light, and with the number of buttons and the marking of identification plates as shown. Furnish pushbutton color code in accordance with NEMA ICS 6.

Provide pushbuttons that are designed with normally open, circuit-closing contacts; normally closed circuit-opening contacts; and two-circuit normally open and normally closed circuit-closing and -opening contacts. Ensure that pushbutton-contact ratings are in accordance with NEMA ICS 1 and NEMA ICS 2, with contact designation A600.

Identify pushbuttons in remote-control stations with identification plates affixed to the front cover in a prominent location. Identify the system being controlled on the identification plate.

b. Selector Switches

Provide heavy-duty, oiltight, maintained-contact selector switches for low-voltage control circuits, with the number of positions and the marking of identification plates in accordance with NEMA ICS 1 and NEMA ICS 2.

Identify selector switches in remote-control stations with engraved identification plates affixed to the front cover in a prominent location. Identify the system being controlled on the identification plate.

c. Ammeter Selector Switches

Provide rotary, multistage, snap-action-type ammeter selector switches for switchgear in accordance with UL 20. Use silver-plated contacts rated for 600 V, ac or dc. Provide a manually operated, four-position selector switch rated for 600 V, 20 A, minimum. Ensure that the switch is designed

to select the display of current readings on each bus of the main bus from a single indicating instrument. Mount the ammeter switch on the hinged front panel of the switchgear compartment, with engraved escutcheon plate. Completely isolate the switch from high-voltage circuits.

Provide a oval-type selector switch handle.

d. Voltmeter Selector Switches

Provide rotary, snap-action-type voltmeter selector switches for switchgear in accordance with UL 20. Use silver-plated contacts rated for 600 V ac or dc. Provide manually operated, four-position switches designed to select the display of voltage readings on each phase of the main bus from a single indicating instrument. Mount the voltmeter switch on the hinged front panel of the switchgear compartment, with engraved escutcheon plate. Completely isolate the switch from high-voltage circuits.

Provide a oval-type selector switch handle.

e. Miscellaneous Switches

Provide float, limit, door, pressure, proximity, and other types of switches in accordance with IPC D330 and of the types and classes indicated.

2.2.5 Finish

Protect metallic materials against corrosion. Provide equipment with the standard finish by the manufacturer when used for most indoor installations. For harsh indoor environments (any area subjected to chemical or abrasive action) and all outdoor installations, refer to Section 09 96 00 HIGH-PERFORMANCE COATINGS.

2.3 COMPONENTS

2.3.1 Instrument Transformers

Comply with the interference requirements listed below, measured in accordance with IEEE C63.2, and IEEE C63.4 for Instrument transformers.

Insulation Class kV	Basic Insulation Level kV	Nominal System Voltage kV	Preferred Test Voltage for Potential Transformers kV	Test Voltage for Current Transformers kV	Radio Influence Voltage Level, Microvolts	
					Dry Type	Oil Filled
0.6	10	----	----	0.76	250	250

1.2	30	0.208 0.416 0.832 1.04	0.132 0.264 0.528 0.66	0.76	250	250
2.5	45	2.40	1.52	1.6 7	250	250
5.0	60	4.16 4.80	2.64 3.04	3.34	250	250
8.7	75	7.20 8.32	4.57 5.28	5.77	250	250
15L or 15H	95 - 110	12.00 12.47 14.40	7.62 7.92 9.14	9.41	1000	250
25	150	23.00	14.60	15.70	2500	650
34.5	200	34.50	21.90	23.0	----	650
46	250	46.00	29.20	29.30	----	1250
69	350	69.00	43.80	44.00	----	1250
92	450	92.00	58.40	58.40	----	2500
115	550	115.00	73.40	73.40	----	2500
138	650	138.00	88.00	88.00	----	2500

2.3.1.1 Current Transformers

Ensure that current transformers conform to IEEE C57.13 for installation in metal-clad switchgear. Use a standard 3-A secondary transformer.

Provide window-type transformers.

Provide transformers that have single secondary winding.

Provide transformers that are complete with a secondary short-circuiting device.

For window-type current transformers, provide indoor, dry-type construction, with secondary current ratings as indicated with the specified burden, frequency, and accuracy.

2.3.1.2 Potential Transformers

For potential transformers, conform to IEEE C57.13 for installation in metal-clad switchgear. Use standard 120-volt secondary transformers.

Provide transformers that have single secondary winding.

Provide burden, frequency, and accuracy as required.

For disconnecting potential transformers with integral fuse mountings and

current-limiting fuses, provide indoor, dry-type two-winding construction with primary and secondary voltage ratings as required.

2.3.2 Enclosures

2.3.2.1 Equipment Enclosures

Provide enclosures for equipment in accordance with NEMA 250.

Contain equipment that is installed inside clean, dry locations in a NEMA Type 1, general-purpose sheet-steel enclosure.

Contain equipment that is installed in wet locations in a NEMA Type 4, watertight, corrosion-resistant, sheet-steel enclosure. Construct the enclosure to prevent entrance of water when tested in accordance with NEMA ICS 6 for Type 4 enclosures.

Contain equipment that is installed in industrial locations in a NEMA Type 12, industrial-use, sheet-steel enclosure. Construct the enclosure to prevent the entrance of dust, lint, fibers, and flyings and the seepage of oil and coolant.

Contain equipment that is installed in Class I, Division 1, Group A, B, C, and D, hazardous locations, in NEMA Type 7 enclosures approved for the specific flammable gas or vapor that is possibly present under normal operating conditions.

Contain equipment that is installed in Class II, Division 1, Group E, F and G, hazardous locations, in NEMA Type 9 enclosures approved for use where combustible dust is possibly present under normal operating conditions.

Fabricate sheet-steel enclosures from uncoated carbon sheet-steel of commercial quality. Ensure that the box dimensions and thickness of sheet-steel conform to UL 50.

2.3.2.2 Remote-Control Station Enclosures

Provide remote-control station enclosures for pushbuttons, selector switches, and indicating lights in accordance with NEMA ICS 6 and NEMA 250.

Contain remote-control stations installed in indoor, clean, dry locations in NEMA Type 1 general-purpose, sheet-steel enclosures. Contain recessed remote-control stations in standard wall outlet boxes with matching corrosion-resistant-steel flush cover plates.

Contain remote-control stations installed in wet locations in NEMA Type 4, watertight, corrosion-resistant, sheet-steel enclosures. Construct enclosures to prevent entrance of water when tested in accordance with NEMA ICS 6 and NEMA 250 for Type 4 enclosures.

Contain remote-control stations installed in wet locations in NEMA Type 4, watertight, cast-iron enclosures. Construct enclosures to prevent entrance of water when tested in accordance with NEMA ICS 6 and NEMA 250 for Type 4 enclosures.

Contain remote-control stations installed in industrial locations in NEMA Type 12, industrial-use, sheet-steel enclosures. Construct enclosures to prevent the entrance of dust, lint, fibers, and flyings and the seepage of

oil and coolant.

Contain remote-control stations installed in Class I, Division 1, Group A, B, C, and D, hazardous locations in NEMA Type 7 enclosures, approved for the specific flammable gas or vapor that is possibly present under normal operating conditions.

Contain remote-control stations installed in Class II, Division 1, Group E, F and G, hazardous locations in NEMA Type 9 enclosures, approved for use where combustible dust is possibly present under normal operating conditions.

Fabricate sheet-steel enclosures from uncoated carbon steel sheets of commercial quality, with box dimensions and thickness of sheet steel conforming to UL 50.

Install remote-control stations with the centerline 66 inches above the finished floor.

2.3.3 Time Switches

Provide time switches for the control of tungsten-lamp loads, fluorescent-lamp loads, resistive-heating loads, motors, and magnetically operated devices, consisting of a motor-driven time dial and switch assembly in a NEMA 250, Type 1, general-purpose enclosure.

Provide motor drives consisting of 120-V, single-phase, 60-Hz, heavy-duty, self-starting synchronous motors directly connected to the time dial through a geartrain operating mechanism. Provide a spring-wound stored-energy source of reserve power that automatically operates the mechanism for a period of at least 12 hours in case of electric power failure. Ensure that the spring automatically rewinds electrically in not more than 3 hours after electric power is restored.

Include a heavy-duty, general-purpose, precision snap-action switch conforming to UL 20 for the switch mechanism, with provisions for manual "OFF" and "ON" operation of the switch.

Provide time switches for the control of 120/240-V, two- and three-wire, single-phase, 60-Hz circuits and 120/208-V, three-phase, four-wire, 60-Hz circuits, with a continuous-current tungsten-lamp load rating of 35 A.

Provide astronomic-type time dials that automatically change settings each day, in accordance with the seasonal time changes in sunrise and sunset. Provide astronomic-type dials that have adjustable on and off trippers, for repetitive switching operations at solar time each day and at each day in the year and that make one revolution in a 24-hour period. Provide time dials that are designed to operate in the "ON" position at sunset and be fully adjustable upward in 15-minute intervals throughout each day, and that indicate the day and month of the year. Calibrate the dials in 15-minute intervals over a 24-hour period around its circumference. Provide a method to defeat the switching operation over weekends or up to 6 preselected calendar days each week.

2.3.4 Protective Relays

2.3.4.1 Overcurrent Relays

Provide a trip unit that employs a combination of discrete components and

integrated circuits to ensure the time-current protection functions as required in a modern, selectively coordinated distribution system.

Conform relays to IEEE C37.90 for overcurrent relays.

For protection against phase and ground faults, provide single-phase nondirectional, removable, induction-type overcurrent relays with built-in testing facilities designed for operation on the dc or ac control circuit indicated.

Provide ground-fault overcurrent relays with short-time inverse-time characteristics with adjustable current tap range as required.

Provide phase-fault overcurrent relays with varied inverse-time characteristics with adjustable current tap range as required. Provide attachments that indicate instantaneous trip with adjustable current range as required.

Provide solid-state, static-type trips for low-voltage power circuit breakers in accordance with EIA 443 and IEEE C37.17.

Provide complete system-selective coordination by using a combination of the following time-current curve-shaping adjustments: ampere setting; long-time delay; short-time pickup; short-time delay; instantaneous pickup; and ground fault.

Provide switchable or easily defeatable instantaneous and ground fault trips.

Make all adjustments using nonremovable, discrete-step, highly reliable switching plugs for precise settings. Provide a sealable, transparent cover over the adjustments to prevent tampering.

Furnish trip devices with three visual indicators to denote the automatic tripping mode of the breaker, including overload, short circuit, and ground fault.

Wire the trip unit to the appropriate terminals so that an optional, remote, automatic trip accessory can be used to provide the same indication.

Make available for use a series of optional, automatic trip relays for use with the trip unit to provide remote alarm and lockout circuits.

Provide all trip units with test jacks for in-service functional testing of the long-time instantaneous and ground-fault circuits using a small handheld test kit.

2.3.4.2 Directional Overcurrent Relays

Provide directional overcurrent relays in accordance with IEEE C37.90.

For protection against reverse-power faults, provide single-phase induction relays with adjustable time-delay and instantaneous trip attachments. Provide removable-type relays with inverse-time directional and overcurrent units with built-in testing facilities.

2.3.4.3 Reclosing Relays

Ensure that reclosing relays conform to IEEE C37.90.

Provide reclosing relays that reclose circuit breakers that have tripped from overcurrent. Provide a device that automatically recloses the breaker at adjustable time intervals between reclosures and then locks out the breaker in the open position if the fault persists. Ensure that if the fault disappears after any reclosure, the circuit breaker remains closed and the reclosing relay resets automatically and is ready to start a new sequence of operation.

Provide removable reclosing relays that have built-in testing facilities and that consist of a timing unit rated at 120/240 V, single-phase, ac and solenoid and contactor units with dc rating as indicated. Arrange contacts for one instantaneous reclosure and two subsequent reclosures at 15 and 45 seconds, respectively. Set the time dial for 60-second drum speed.

2.3.4.4 Undervoltage Relays

Ensure that undervoltage relays conform to IEEE C37.90.

Provide three-phase, induction-type undervoltage relays, including inverse timing with adjustable high- and low-voltage contacts and calibrated scale. Equip relays with indicating contactor and voltage switches to provide electrically separate contact circuits. Provide relays that are removable with built-in testing facilities and that are suitable for operation on 120 V ac circuits, with contacts that are suitable for operation on dc or ac control circuits.

2.3.5 Indicating Instruments

2.3.5.1 Ammeters

Provide switchboard indicating ammeters of approximately 4 1/2 inches square with 250-degree scale and recessed cases suitable for flush mounting. Furnish white dials with black figures and black pointers. Mount instruments on the hinged front panel of the switchgear compartment, completely isolated from high-voltage circuits. Provide a standard 5-ampere-type meter for a zero-to-full-scale normal movement, 60 Hz.

2.3.5.2 Voltmeters

Provide switchboard indicating voltmeters that are approximately 4 1/2 inches square with 250-degree scale and recessed cases suitable for flush mounting. Furnish white dials with black figures and black pointers. Mount instruments on the hinged front panel of the switchgear compartment, completely isolated from high-voltage circuits. Provide a standard 120-volt-type voltmeters for zero-to-full-scale normal movement, 60 Hz.

2.3.5.3 Watt-Hour Meters/Wattmeters

Provide watt-hour meters, wattmeters, and pulse initiation meters conforming to ANSI C12.1.

Provide three-phase induction-type switchboard wattmeters for use with instrument transformers with two stators, each equipped with a current and potential coil. Provide a meter rated for 5 A at 120 V and suitable for

connection to three-phase, three- and four-wire circuits. Provide the instrument complete with potential-indicating lamps, light-load and full-load adjustments, phase balance, power-factor adjustments, four-dial clock register, ratchets to prevent reverse rotation, and built-in testing facilities.

For use with demand meters or pulse recorders, provide pulse-initiating meters that are suitable for use with either mechanical or electrical pulse initiators. Ensure that the mechanical load imposed on the meter by the pulse initiator is within the limits of the pulse meter. Provide a load as constant as practical throughout the entire cycle of operation to ensure accurate meter readings. Provide a pulse-initiating meter that is capable of measuring the maximum number of pulses at which the pulse device is nominally rated. Consider the pulse-initiating meter to be operating properly when a kilowatt-hour check indicates that the demand meter kilowatt-hours are within limits of the watt-hour meter kilowatt-hours.

Locate pulse-initiating meters such that components sensitive to moisture and temperature conditions are minimized. Take precautions to protect sensitive electronic metering circuitry from electromagnetic and electrostatic induction.

Furnish removable meters with draw-out test plugs and furnish contact devices to operate remote impulse-totalizing graphic demand meters.

2.3.5.4 Graphic Demand Meters

Provide impulse-totalizing graphic demand meters conforming to ANSI C12.1.

Provide impulse-totalizing graphic demand meters that are suitable for use with switchboard watt-hour meters and include the following: a two-circuit totalizing relay, cyclometer for cumulative record of impulses, four-dial totalizing kilowatt-hour register, synchronous motor for timing mechanism, torque motor, and chart drive. Provide a positive chart-drive mechanism, consisting of chart spindles and drive sprockets, that maintains the correct chart speed for roll strip charts. Provide an instrument that records, as well as indicates, on clearly legible graph paper, the 15-minute integrated kilowatt demand of the totalized system.

Furnish the motive power for advancing the register and pen-movement mechanism with a torque motor. Provide a capillary pen containing a 1-month ink supply. Provide roll charts with a 31-day continuous record of operation capacity.

2.3.5.5 Specialty-Type Meters

Specialty-type meters are panel meters applicable to specific situations, such as pyrometers and dc parameter meters that conform to the panel layout specified. Provide meter scales that are at least 180 degrees. Do not use edgewise meters for circuit current and voltage measurements.

2.3.6 Indicating Lights

2.3.6.1 General-Purpose Type

For indicating lights, provide oiltight instrument devices with threaded base and collar for flush mounting; translucent convex lens; candelabra screw-base lampholder; and 120 V, 6 W, Type S-6 incandescent lamp in

accordance with ANSI C78.23. Provide indicating lights that are color-coded in accordance with NEMA ICS 6.

Provide indicating lights in remote-control stations when pushbuttons and selector switches are out of sight of the controller.

2.3.6.2 Switchboard Indicating Lights

For switchboard indicating lights, provide the manufacturer's standard transformer-type units 120 V input using low-voltage lamps and convex lenses of the colors indicated. Provide indicating lights that are capable of being relamped from the switchboard front. Do not use indicating lights that use resistors in series with the lamps, except in dc control circuits. Provide lights that have a press-to-test feature.

PART 3 EXECUTION

3.1 INSTALLATION

Clearly list fuse information on equipment drawings.

Install control devices and protective devices that are not factory-installed in equipment, in accordance with the manufacturer's recommendations. Field-adjust the devices. Perform operation tests on the control and protective devices. Conform requirements for installation of control and protective devices to NFPA 70, NEMA ICS 1, and NEMA ICS 2.

3.2 FIELD QUALITY CONTROL

3.2.1 Tests

Demonstrate the operation and controls of protective devices of non-factory-installed equipment.

Verify tap settings of instrumentation, potential, and current transformers.

Perform dielectric tests on insulating oil in oil circuit breakers before the breakers are energized. Test oil in accordance with ASTM D877/D877M, and provide breakdown voltage that is not less than 25,000 V. Provide manufacturer certification that the oil contains no PCB's, and affix a label to that effect on each breaker tank and on each oil drum containing the insulating oil.

Field-adjust reduced-voltage starting devices to obtain optimum operating conditions. Provide test meters and instrument transformers that conform to ANSI C12.1 and IEEE C57.13.

Do not energize control and protective devices until the results of the recorded test data have been approved by the Contracting Officer. Provide final test reports with a cover letter/sheet clearly marked with the system name, date, and the words final test reports to the Contracting Officer for approval.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 26 - ELECTRICAL

SECTION 26 09 23.00 40

LIGHTING CONTROL DEVICES

PART 1 GENERAL

1.1 REFERENCES
1.2 DEFINITIONS
1.3 SUBMITTALS
1.4 QUALITY CONTROL
1.4.1 Regulatory Requirements
1.4.2 Standard Products

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION
2.1.1 System Requirements
2.2 COMPONENTS
2.2.1 Manual Switches
2.2.2 Dimming Ballast Controls
2.2.3 Light Level Sensor
2.2.4 Incandescent Dimmer Switch
2.2.5 Time Switch
2.2.6 Photocell Switch
2.2.7 Occupancy Sensors

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Photoconductive Control Devices
3.1.2 Time Control Switches
3.1.3 Manual and Safety Switches
3.1.4 Magnetic Contactors
3.2 EQUIPMENT IDENTIFICATION
3.2.1 Manufacturer's Nameplate
3.2.2 Labels
3.3 FIELD QUALITY CONTROL
3.4 CLOSEOUT ACTIVITIES

-- End of Section Table of Contents --

SECTION 26 09 23.00 40

LIGHTING CONTROL DEVICES

PART 1 GENERAL

Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM applies to work specified in this section.

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE C2	(2023) National Electrical Safety Code
IEEE Stds Dictionary	(2009) IEEE Standards Dictionary: Glossary of Terms & Definitions

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA ICS 1	(2000; R 2015) Standard for Industrial Control and Systems: General Requirements
NEMA ICS 2	(2000; R 2020) Industrial Control and Systems Controllers, Contactors, and Overload Relays Rated 600 V
NEMA ICS 6	(1993; R 2016) Industrial Control and Systems: Enclosures

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National Electrical Code

U.S. FEDERAL COMMUNICATIONS COMMISSION (FCC)

FCC Part 15	Radio Frequency Devices (47 CFR 15)

UNDERWRITERS LABORATORIES (UL)

UL 20	(2018; Reprint Jan 2021) UL Standard for Safety General-Use Snap Switches
UL 98	(2016) UL Standard for Safety Enclosed and Dead-Front Switches
UL 773	(2016; Reprint Jul 2020) UL Standard for Safety Plug-In, Locking Type Photocontrols for Use with Area Lighting
UL 773A	(2016; Reprint Jun 2020) UL Standard for

1.2 DEFINITIONS

a. Unless otherwise specified or indicated, electrical and electronics terms used in these specifications, and on the drawings, are as defined in the IEEE Stds Dictionary.

b. DALI: Digital Addressable Lighting Interface used to transmit data to and from lighting control system input devices, end devices, and control equipment.

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Lighting System Drawings; G

SD-03 Product Data

Installation Instructions; G

Dimming Ballast Controls; G

Light Level Sensor; G

Dimmer Switch; G

Time Switch; G

Photocell Switch; G

Occupancy Sensors; G

SD-06 Test Reports

System Operation Tests

SD-10 Operation and Maintenance Data

Lighting Control System, Data Package 5

1.4 QUALITY CONTROL

1.4.1 Regulatory Requirements

In each of the publications referred to herein, consider the advisory provisions to be mandatory, as though the word, "shall" had been substituted for "should" wherever it appears. Interpret references in these publications to the "authority having jurisdiction," or words of similar meaning, to mean the Contracting Officer. Ensure equipment, materials, installation, and workmanship are in accordance with the

mandatory and advisory provisions of NFPA 70, IEEE C2 unless more stringent requirements are specified or indicated.

1.4.2 Standard Products

Provide materials and equipment that are products of manufacturers regularly engaged in the production of such products which are of equal material, design and workmanship. Provide products which have been in satisfactory commercial or industrial use for 2 years prior to bid opening. Ensure the 2-year period includes applications of equipment and materials under similar circumstances and of similar size. Ensure the product has been on sale on the commercial market through advertisements, manufacturers' catalogs, or brochures during the 2-year period. Where two or more items of the same class of equipment are required, these items must be products of a single manufacturer.

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION

Submit lighting system drawings showing luminaire configuration, control zones, and detection range of specified control devices. Ensure lighting system drawings include photometric calculations showing lighting levels in foot candles for all areas indicated. Ensure lighting calculations and photometric plans are created using industry standard light modeling software. Hand calculations will not be accepted.

b. Provide lighting control system of the centralized and addressable type that includes programmable devices. Control devices are of the digital low-voltage or wireless types and are used to create control zones which can be changed without affecting the wiring of the devices. Control zones are used to turn lights on and off or to provide light dimming capabilities.

c. Lighting control system must comply with these specifications, all applicable construction document drawings, all applicable codes, and all local authorities having jurisdiction. Lighting control system equipment includes, but is not limited to, time control switches, manual and safety switches, dimming ballasts, light level sensors, incandescent dimmer switches, lighting contactors, photocell switches, and occupancy sensors.

2.1.1 System Requirements

a. The lighting control system and lighting end devices must revert to the on position in the event of a loss of power or control signal to the system or end devices.

b. Lighting control zones consisting of one or more networked luminaires and lighting control devices must be capable of providing automatic control from sensors (occupancy and photocell) and manual control local switches.

c. Provide networked luminaires and lighting control devices that store programming in non-volatile memory such that following any loss of power the lighting control zones continue to operate according to the defined settings.

2.2 COMPONENTS

2.2.1 Manual Switches

Provide a switch mechanism consisting of a heavy-duty general-purpose precision snap-acting switch, with NEMA ICS 6 Type 1 enclosures,, single-pole, single-throw, suitable for operation on a 480Y/277 volt, 60 Hz, single-phase system. Provide with a selector switch having a minimum of three positions: ON, OFF, and AUTOMATIC. Use the automatic position when photoelectric or timer control is desired. Interface the selector switch with the lighting system magnetic contactor to control system activity.

Ensure switches conform to UL 98 as applicable. Provide a quick-make, quick-break type switch such that a screwdriver is required to open the switch door when the switch is on, with blades visible when the door is open. Coordinate terminal lugs with the wire size.

2.2.2 Dimming Ballast Controls

Provide a single slide dimming ballast control dimmer with on-off control, compatible with the ballast. Control the ballast light output over the full dimming range. Provide a dimmer ballast control which is approved by the ballast manufacturer.

2.2.3 Light Level Sensor

Wow a

Provide UL listed light level sensor capable of detecting changes in ambient lighting levels, with a dimming range of 20 percent to 100 percent, minimum. Ensure sensor is designed for use with dimming ballast and voltage system to which they are connected. Provide a sensor capable of controlling 40 electronic dimming ballasts, minimum, with a sensor light level adjustable with a set level range from 10 to 100 foot-candles, minimum. Provide a sensor with a bypass function to electrically override the sensor control.

2.2.4 Incandescent Dimmer Switch

Provide a single-pole, 600 watt, 120 volt ac, dimmer switch that conforms to UL 20. Ensure the switch is the full-range rotary on-off type with built-in electromagnetic interference filter.

2.2.5 Time Switch

Provide astronomic dial type or electronic type, arranged to turn "ON" at sunset and turn "OFF" at a predetermined time between 8:30 p.m. and 2:30 a.m. or at sunrise, automatically changing the settings each day in accordance with seasonal changes of sunset and sunrise. Provide a 120 volts rated switch, having automatically wound spring mechanism or capacitor, to maintain accurate time for a minimum of 7 hours following power failure. Provide time switch with a manual on-off bypass switch. Surface mount the housing for the time switch, inside a NEMA 1 enclosure conforming to NEMA ICS 6.

2.2.6 Photocell Switch

Ensure photocell switches conform to UL 773 or UL 773A as applicable. Provide hermetically sealed photocells that use cadmium-sulfide or silicon

diode type cells. Provide photocells that are rated at 120 volts ac, 60 Hz with single-throw contacts and designed to fail to the ON position. Provide photocells that turn on at or below 3 foot-candles and off at 4 to 10 foot-candles. Provide time delay to prevent accidental switching from transient light sources.

Provide a photocell with the following:

a. Integral to the luminaire, rated 1000W minimum.

2.2.7 Occupancy Sensors

Provide UL listed occupancy sensor complying with FCC Part 15. Design occupancy sensors and power packs to operate on the voltage indicated. Provide sensors and power packs with circuitry that only allows load switching at or near zero current crossing of supply voltage, with mounting as indicated. Provide sensor with an LED occupant detection indicator, adjustable sensitivity, and adjustable delayed-off time range of 5 minutes to 15 minutes. Provide white wall mounted sensors, and white ceiling mounted sensors. Provide ceiling mounted sensors with 360 degree coverage unless otherwise indicated.

Provide sensors with:

a. A crystal controlled ultrasonic sensor which does not cause detection interference between adjacent sensors.

b. Infrared sensors with a daylight filter, and a fresnel lens that is applicable to the controlled space.

c. Ultrasonic/Infrared Combination Sensor

(1) Occupancy detection to turn lights on requires both ultrasonic and infrared sensor detection, such that the lights remain on if either the ultrasonic or infrared sensor detects movement. Provide infrared sensor with a lens selected for indicated usage and daylight filter to prevent short wavelength infrared interference. Provide crystal controlled ultrasonic sensor frequency.

PART 3 EXECUTION

3.1 INSTALLATION

Submit installation instructions for light-sensitive, occupancy sensitive control devices in accordance with the manufacturer's recommended instructions for installation.

3.1.1 Photoconductive Control Devices

Install photoconductive control devices in accordance with the manufacturer's installation instructions.

3.1.2 Time Control Switches

Install switches with not less than four 1/4 inch bolts. Do not use sheet metal screws.

3.1.3 Manual and Safety Switches

Coordinate terminal lugs with the wire size. Securely fasten switches to the supporting structure or wall using not less than four 1/4 inch bolts. Do not use sheet metal screws.

3.1.4 Magnetic Contactors

Install magnetic contactors, mechanically held, electrically operated, conforming to NEMA ICS 1 and NEMA ICS 2, suitable for 277 volts, single phase, 60 Hz, with coil voltage of 277 volts. Provide contactors with maximum continuous ampere rating and number of poles as indicated on drawings. For contactors mounted indoors, provide enclosures conforming to NEMA ICS 6, Type 1. Provide each contactor with a spare, normally open auxiliary contact.

Coordinate terminal lugs with the wire size. Securely fasten switches to the supporting structure or wall using not less than four 1/4 inch bolts. Do not use sheet metal screws.

3.2 EQUIPMENT IDENTIFICATION

3.2.1 Manufacturer's Nameplate

Provide each item of equipment with a nameplate bearing the manufacturer's name, address, model number, and serial number securely affixed in an inconspicuous place; the nameplate of the distributing agent is not acceptable.

3.2.2 Labels

Coordinate labesl for use cases in field.

3.3 FIELD QUALITY CONTROL

Perform system operation tests in accordance with referenced standards in this section.

Demonstrate that photoconductive control devices operate satisfactorily in the presence of the Contracting Officer.

Measure and record foot-candle levels in areas indicated and compare to submitted photometric calculations. Perform all lighting measurements in the presence of the Contracting Officer. Ensure measured lighting levels are within 10% of the calculated values. Where lighting levels are determined to be deficient contractor will modify system to bring lighting levels into compliance at no additional cost to the Government.

3.4 CLOSEOUT ACTIVITIES

Submit operation and maintenance data, lighting control system, data package 5, in accordance with Section 01 78 23 OPERATION AND MAINTENANCE DATA and as specified herein. Show information for all lighting fixtures, control modules, control zones, occupancy sensors, motion sensors, light level sensors, power packs, dimming ballasts, schematic diagrams and all interconnecting control wire, conduit, and associated hardware.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 26 - ELECTRICAL

SECTION 26 20 00

INTERIOR DISTRIBUTION SYSTEM

PART 1 GENERAL

1.1 REFERENCES
1.2 DEFINITIONS
1.3 SUBMITTALS
1.4 QUALITY ASSURANCE
1.4.1 Fuses
1.4.2 Regulatory Requirements
1.4.3 Standard Products
1.4.3.1 Alternative Qualifications
1.4.3.2 Material and Equipment Manufacturing Date
1.5 MAINTENANCE
1.5.1 Electrical Systems
1.6 WARRANTY

PART 2 PRODUCTS

2.1 MATERIALS AND EQUIPMENT
2.2 CONDUIT AND FITTINGS
2.2.1 Rigid Metallic Conduit
2.2.1.1 Rigid, Threaded Zinc-Coated Steel Conduit
2.2.1.2 Rigid Aluminum Conduit
2.2.2 Rigid Nonmetallic Conduit
2.2.3 Intermediate Metal Conduit (IMC)
2.2.4 Electrical, Zinc-Coated Steel Metallic Tubing (EMT)
2.2.5 Plastic-Coated Rigid Steel and IMC Conduit
2.2.6 Flexible Metal Conduit
2.2.6.1 Liquid-Tight Flexible Metal Conduit, Steel
2.2.7 Fittings for Metal Conduit, EMT, and Flexible Metal Conduit
2.2.7.1 Fittings for Rigid Metal Conduit and IMC
2.2.7.2 Fittings for EMT
2.2.8 Fittings for Rigid Nonmetallic Conduit
2.2.9 Liquid-Tight Flexible Nonmetallic Conduit
2.3 SURFACE RACEWAY
2.3.1 Surface Metal Raceway
2.3.2 Surface Nonmetallic Raceway
2.4 BUSWAY
2.4.1 Feeder Busways
2.4.2 Plug-In Busways
2.5 CABLE TRAYS
2.5.1 Trough-Type Cable Trays
2.5.2 Ladder-Type Cable Trays
2.5.3 Channel-Type Cable Trays
2.5.4 Solid Bottom-Type Cable Trays
2.5.5 Cantilever
2.6 OPEN TELECOMMUNICATIONS CABLE SUPPORT

2.6.1 Open Top Cable Supports
2.6.2 Closed Ring Cable Supports
2.7 OUTLET BOXES AND COVERS
2.7.1 Floor Outlet Boxes
2.7.2 Outlet Boxes for Telecommunications System
2.7.3 Clock Outlet for Use in Other Than Wired Clock System
2.8 CABINETS, JUNCTION BOXES, AND PULL BOXES
2.9 WIRES AND CABLES
2.9.1 Conductors
2.9.1.1 Equipment Manufacturer Requirements
2.9.1.2 Minimum Conductor Sizes
2.9.2 Color Coding
2.9.2.1 Ground and Neutral Conductors
2.9.2.2 Ungrounded Conductors
2.9.3 Insulation
2.9.4 Bonding Conductors
2.9.4.1 Telecommunications Bonding Backbone (TBB)
2.9.4.2 Bonding Conductor for Telecommunications
2.9.5 Service Entrance Cables
2.9.6 Nonmetallic Sheathed Cable
2.9.7 Wire and Cable for 400 Hertz (Hz) Circuits
2.9.8 Mineral-Insulated, Metal-Sheathed Cable
2.9.9 Flat Conductor Cable
2.9.10 Cable Tray Cable or Power Limited Tray Cable
2.9.11 Cord Sets and Power-Supply Cords
2.10 SPLICES AND TERMINATION COMPONENTS
2.11 DEVICE PLATES
2.12 SWITCHES
2.12.1 Toggle Switches
2.12.2 Switch with Red Pilot Handle
2.12.3 Breakers Used as Switches
2.12.4 Disconnect Switches
2.13 FUSES
2.13.1 Fuseholders
2.14 RECEPTACLES
2.14.1 Split Duplex Receptacles
2.14.2 Weatherproof Receptacles
2.14.3 Ground-Fault Circuit Interrupter Receptacles
2.14.4 Tamper-Resistant Receptacles
2.15 PANELBOARDS
2.15.1 Enclosure
2.15.2 Panelboard Buses
2.15.3 Circuit Breakers
2.15.3.1 Multipole Breakers
2.15.3.2 Circuit Breaker With Ground-Fault Circuit Interrupter
2.15.4 Branch Circuit Monitoring Panelboards
2.16 ENCLOSED CIRCUIT BREAKERS
2.17 MOTOR SHORT-CIRCUIT PROTECTOR (MSCP)
2.18 TRANSFORMERS
2.18.1 Specified Transformer Efficiency
2.18.2 K-Rated Transformers
2.19 MOTORS
2.19.1 High Efficiency Single-Phase Motors
2.19.2 Premium Efficiency Polyphase and Single-Phase Motors
2.19.3 Motor Sizes
2.19.4 Wiring and Conduit
2.20 MOTOR CONTROLLERS
2.20.1 Control Wiring
2.20.2 Control Circuit Terminal Blocks

2.20.2.1 Types of Terminal Blocks
2.20.3 Control Circuits
2.20.4 Enclosures for Motor Controllers
2.20.5 Multiple-Speed Motor Controllers and Reversible Motor Controllers
2.20.6 Pushbutton Stations
2.20.7 Pilot and Indicating Lights
2.21 MANUAL MOTOR STARTERS (MOTOR RATED SWITCHES)
2.21.1 Pilot Lights
2.22 LOCKOUT REQUIREMENTS
2.23 TELECOMMUNICATIONS SYSTEM
2.24 COMMUNITY ANTENNA TELEVISION (CATV) SYSTEM
2.24.1 CATV Outlets
2.24.2 CATV Faceplates
2.24.3 Backboards
2.25 GROUNDING AND BONDING EQUIPMENT
2.25.1 Ground Rods
2.25.2 Ground Bus
2.25.3 Secondary Bonding Busbar
2.26 MANUFACTURER'S NAMEPLATE
2.27 FIELD FABRICATED NAMEPLATES
2.28 WARNING SIGNS
2.29 FIRESTOPPING MATERIALS
2.30 WIREWAYS
2.31 METERING
2.32 METER BASE ONLY
2.33 SURGE PROTECTIVE DEVICES
2.34 FACTORY APPLIED FINISH
2.35 SOURCE QUALITY CONTROL
2.35.1 Transformer Factory Tests

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Underground Service
3.1.2 Service Entrance Identification
3.1.2.1 Labels
3.1.3 Wiring Methods
3.1.3.1 Pull Wire
3.1.3.2 Flat Conductor Cable
3.1.4 Conduit Installation
3.1.4.1 Restrictions Applicable to Aluminum Conduit
3.1.4.2 Restrictions Applicable to EMT
3.1.4.3 Restrictions Applicable to Nonmetallic Conduit
3.1.4.4 Restrictions Applicable to Flexible Conduit
3.1.4.5 Underground Conduit
3.1.4.6 Conduit for Circuits Rated Greater Than 600 Volts
3.1.4.7 Conduit Installed Under Floor Slabs
3.1.4.8 Conduit Through Floor Slabs
3.1.4.9 Conduit Installed in Concrete Floor Slabs or Concrete Walls
3.1.4.10 Stub-Ups
3.1.4.11 Conduit Support
3.1.4.12 Directional Changes in Conduit Runs
3.1.4.13 Locknuts and Bushings
3.1.4.14 Flexible Connections
3.1.4.15 Telecommunications and Signal System Pathway
3.1.4.16 Community Antenna Television (CATV) System Conduits
3.1.5 Busway Installation
3.1.6 Cable Tray Installation

3.1.7 Telecommunications Cable Support Installation
3.1.8 Boxes, Outlets, and Supports
3.1.8.1 Boxes
3.1.8.1.1 Wall-Mounted Telecommunications Outlet Box
3.1.8.2 Pull Boxes
3.1.8.3 Extension Rings
3.1.9 Mounting Heights
3.1.10 Nonmetallic Sheathed Cable Installation
3.1.11 Mineral Insulated, Metal Sheathed (Type MI) Cable Installation
3.1.12 Conductor Identification
3.1.12.1 Marking Strips
3.1.13 Splices
3.1.13.1 Splices of Aluminum Conductors
3.1.14 Terminating Aluminum Conductors
3.1.14.1 Termination to Copper Bus
3.1.14.2 Termination to Aluminum Bus
3.1.15 Covers and Device Plates
3.1.16 Electrical Penetrations
3.1.17 Grounding and Bonding
3.1.17.1 Ground Rods
3.1.17.2 Grounding Connections
3.1.17.3 Ground Bus
3.1.17.4 Resistance
3.1.17.5 Telecommunications System
3.1.18 Equipment Connections
3.1.19 Elevator
3.1.20 Government-Furnished Equipment
3.1.21 Watthour Meters
3.1.22 Surge Protective Devices
3.2 FIELD FABRICATED NAMEPLATE MOUNTING
3.3 WARNING SIGN MOUNTING
3.4 FIELD APPLIED PAINTING
3.5 FIELD QUALITY CONTROL
3.5.1 Devices Subject to Manual Operation
3.5.2 600-Volt Wiring Test
3.5.3 Transformer Tests
3.5.4 Ground-Fault Receptacle Test
3.5.5 Grounding System Test
3.5.6 Watthour Meter
3.5.7 Phase Rotation Test

-- End of Section Table of Contents --

SECTION 26 20 00

INTERIOR DISTRIBUTION SYSTEM

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

ANSI C12.1	(2014; Errata 2016) Electric Meters - Code for Electricity Metering

ASTM INTERNATIONAL (ASTM)

ASTM B1	(2013) Standard Specification for Hard-Drawn Copper Wire
ASTM B8	(2011; R 2017) Standard Specification for Concentric-Lay-Stranded Copper Conductors, Hard, Medium-Hard, or Soft
ASTM D709	(2017) Standard Specification for Laminated Thermosetting Materials

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 81	(2012) Guide for Measuring Earth Resistivity, Ground Impedance, and Earth Surface Potentials of a Ground System
IEEE C2	(2023) National Electrical Safety Code
IEEE Stds Dictionary	(2009) IEEE Standards Dictionary: Glossary of Terms & Definitions

INTERNATIONAL ELECTRICAL TESTING ASSOCIATION (NETA)

NETA ATS	(2021) Standard for Acceptance Testing Specifications for Electrical Power Equipment and Systems

NATIONAL ELECTRICAL CONTRACTORS ASSOCIATION (NECA)

NECA NEIS 1	(2015) Standard for Good Workmanship in Electrical Construction

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

ANSI C12.7	(2022) Requirements for Watthour Meter Sockets

ANSI C80.1	(2020) American National Standard for Electrical Rigid Steel Conduit (ERSC)
ANSI C80.3	(2020) American National Standard for Electrical Metallic Tubing (EMT)
ANSI C80.5	(2020) American National Standard for Electrical Rigid Aluminum Conduit
NEMA 250	(2020) Enclosures for Electrical Equipment (1000 Volts Maximum)
NEMA BU 1.1	(2010) General Instructions for Proper Handling, Installation, Operation and Maintenance of Busway Rated 600 V or Less
NEMA FU 1	(2012) Low Voltage Cartridge Fuses
NEMA ICS 1	(2000; R 2015) Standard for Industrial Control and Systems: General Requirements
NEMA ICS 2	(2000; R 2020) Industrial Control and Systems Controllers, Contactors, and Overload Relays Rated 600 V
NEMA ICS 4	(2015) Application Guideline for Terminal Blocks
NEMA ICS 6	(1993; R 2016) Industrial Control and Systems: Enclosures
NEMA KS 1	(2013) Enclosed and Miscellaneous Distribution Equipment Switches (600 V Maximum)
NEMA MG 1	(2021) Motors and Generators
NEMA MG 10	(2017) Energy Management Guide for Selection and Use of Fixed Frequency Medium AC Squirrel-Cage Polyphase Induction Motors
NEMA MG 11	(1977; R 2012) Energy Management Guide for Selection and Use of Single Phase Motors
NEMA RN 1	(2005; R 2013) Polyvinyl-Chloride (PVC) Externally Coated Galvanized Rigid Steel Conduit and Intermediate Metal Conduit
NEMA ST 20	(2014) Dry-Type Transformers for General Applications
NEMA TC 2	(2020) Standard for Electrical Polyvinyl Chloride (PVC) Conduit
NEMA TC 3	(2021) Polyvinyl Chloride (PVC) Fittings for Use With Rigid PVC Conduit and Tubing
NEMA VE 2	(2018; ERTA 1-2 2018) Cable Tray

Installation Guidelines

NEMA WD 1 (1999; R 2020) Standard for General Color Requirements for Wiring Devices

NEMA WD 6 (2021) Wiring Devices Dimensions Specifications

NEMA Z535.4 (2023) Product Safety Signs and Labels

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70(2020; TIA 22-1; ERTA 1 2022)
National Electrical Code

NFPA 70E (2021) Standard for Electrical Safety in the Workplace

NFPA 780 (2023) Standard for the Installation of Lightning Protection Systems

TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)

TIA-568.1 (2020e) Commercial Building Telecommunications Infrastructure Standard

TIA-569 (2019e; Add 1 2022) Telecommunications Pathways and Spaces

TIA-607 (2019d) Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises

U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)

10 CFR 431 Energy Efficiency Program for Certain Commercial and Industrial Equipment

29 CFR 1910.147 The Control of Hazardous Energy (Lock Out/Tag Out)

29 CFR 1910.303 Electrical, General

UNDERWRITERS LABORATORIES (UL)

UL 1 (2005; Reprint Jan 2022) UL Standard for Safety Flexible Metal Conduit

UL 5 (2016; Reprint Jul 2022) UL Standard for Safety Surface Metal Raceways and Fittings

UL 5A (2015; Reprint Aug 2020) Nonmetallic Surface Raceways and Fittings

UL 6 (2022) UL Standard for Safety Electrical Rigid Metal Conduit-Steel

UL 6A (2008; Reprint Mar 2021) UL Standard for Safety Electrical Rigid Metal Conduit -

	Aluminum, Red Brass, and Stainless Steel
UL 20	(2018; Reprint May 2023) UL Standard for Safety General-Use Snap Switches
UL 44	(2018; Reprint May 2021) UL Standard for Safety Thermoset-Insulated Wires and Cables
UL 50	(2015) UL Standard for Safety Enclosures for Electrical Equipment, Non-Environmental Considerations
UL 67	(2018; Reprint Aug 2023) UL Standard for Safety Panelboards
UL 83	(2017; Reprint Mar 2020) UL Standard for Safety Thermoplastic-Insulated Wires and Cables
UL 360	(2013; Reprint Apr 2023) UL Standard for Safety Liquid-Tight Flexible Metal Conduit
UL 467	(2022) UL Standard for Safety Grounding and Bonding Equipment
UL 486A-486B	(2018; Reprint May 2021) UL Standard for Safety Wire Connectors
UL 486C	(2018; Reprint May 2021) UL Standard for Safety Splicing Wire Connectors
UL 489	(2016; Rev 2019) UL Standard for Safety Molded-Case Circuit Breakers, Molded-Case Switches and Circuit-Breaker Enclosures
UL 498	(2017; Reprint May 2023) UL Standard for Safety Attachment Plugs and Receptacles
UL 506	(2017; Reprint Jan 2022) UL Standard for Safety Specialty Transformers
UL 508	(2018; Reprint Jul 2021) UL Standard for Safety Industrial Control Equipment
UL 510	(2020; Dec 2022) UL Standard for Safety Polyvinyl Chloride, Polyethylene and Rubber Insulating Tape
UL 514A	(2013; Reprint Jun 2022) UL Standard for Safety Metallic Outlet Boxes
UL 514B	(2012; Reprint May 2020) Conduit, Tubing and Cable Fittings
UL 514C	(2014; Reprint Feb 2020) UL Standard for Safety Nonmetallic Outlet Boxes, Flush-Device Boxes, and Covers
UL 651	(2011; Reprint May 2022) UL Standard for

	Safety Schedule 40, 80, Type EB and A Rigid PVC Conduit and Fittings
UL 719	(2015; Reprint Jan 2023) UL Standard for Safety Nonmetallic-Sheathed Cables
UL 797	(2007; Reprint Apr 2023) UL Standard for Safety Electrical Metallic Tubing -- Steel
UL 817	(2015; Reprint May 2023) UL Standard for Safety Cord Sets and Power-Supply Cords
UL 854	(2020; Reprint Jan 2022) Standard for Service-Entrance Cables
UL 857	(2009; Reprint Apr 2021) UL Standard for Safety Busways
UL 869A	(2006; Reprint Jun 2020) Reference Standard for Service Equipment
UL 870	(2016; Reprint Mar 2019) UL Standard for Safety Wireways, Auxiliary Gutters, and Associated Fittings
UL 943	(2016; Reprint Feb 2018) UL Standard for Safety Ground-Fault Circuit-Interrupters
UL 984	(1996; Reprint Sep 2005) Hermetic Refrigerant Motor-Compressors
UL 1004-1	(2012; Reprint Nov 2020) UL Standard for Safety Rotating Electrical Machines - General Requirements
UL 1063	(2017; Reprint Jun 2022) UL Standard for Safety Machine-Tool Wires and Cables
UL 1242	(2006; Reprint Apr 2022) UL Standard for Safety Electrical Intermediate Metal Conduit -- Steel
UL 1449	(2021; Reprint Dec 2022) UL Standard for Safety Surge Protective Devices
UL 1561	(2011; Reprint Jun 2015) Dry-Type General Purpose and Power Transformers
UL 1660	(2019; Reprint Jan 2022) Liquid-Tight Flexible Nonmetallic Conduit
UL 2043	(2013) Fire Test for Heat and Visible Smoke Release for Discrete Products and Their Accessories Installed in Air-Handling Spaces
UL 4248-1	(2022) UL Standard for Safety Fuseholders - Part 1: General Requirements

1.2 DEFINITIONS

Unless otherwise specified or indicated, electrical and electronics terms used in these specifications, and on the drawings, are as defined in IEEE Stds Dictionary.

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Panelboards; G

Transformers; G

Busway; G

Cable Trays; G

Wireways; G

Marking Strips Drawings; G

SD-03 Product Data

Receptacles; G

Circuit Breakers; G

Switches; G

Transformers; G

Enclosed Circuit Breakers; G

Motor Controllers; G

Manual Motor Starters; G

Metering; G

Meter Base Only; G

CATV Outlets; G

Secondary Bonding Busbar; G

Surge Protective Devices; G

Cable Trays; G

SD-05 Design Data

Cable Tray Design; G

SD-06 Test Reports

600-volt Wiring Test; G

Grounding System Test; G

Transformer Tests; G

Ground-fault Receptacle Test; G

SD-07 Certificates

Fuses; G

SD-09 Manufacturer's Field Reports

Transformer Factory Tests

SD-10 Operation and Maintenance Data

Electrical Systems, Data Package 5; G

Metering, Data Package 5; G

1.4 QUALITY ASSURANCE

1.4.1 Fuses

Submit coordination data as specified in paragraph, FUSES of this section.

1.4.2 Regulatory Requirements

In each of the publications referred to herein, consider the advisory provisions to be mandatory, as though the word, "must" had been substituted for "should" wherever it appears. Interpret references in these publications to the "authority having jurisdiction," or words of similar meaning, to mean the Contracting Officer. Provide equipment, materials, installation, and workmanship in accordance with NFPA 70 unless more stringent requirements are specified or indicated. NECA NEIS 1 shall be considered the minimum standard for workmanship.

1.4.3 Standard Products

Provide materials and equipment that are products of manufacturers regularly engaged in the production of such products which are of equal material, design and workmanship and:

a. Have been in satisfactory commercial or industrial use for 2 years prior to bid opening including applications of equipment and materials under similar circumstances and of similar size.

b. Have been on sale on the commercial market through advertisements, manufacturers' catalogs, or brochures during the 2-year period.

c. Where two or more items of the same class of equipment are required, provide products of a single manufacturer; however, the component parts of the item need not be the products of the same manufacturer unless stated in this section.

1.4.3.1 Alternative Qualifications

Products having less than a 2-year field service record will be acceptable if a certified record of satisfactory field operation for not less than 6000 hours, exclusive of the manufacturers' factory or laboratory tests, is furnished.

1.4.3.2 Material and Equipment Manufacturing Date

Products manufactured more than 3 years prior to date of delivery to site are not acceptable.

1.5 MAINTENANCE

1.5.1 Electrical Systems

Submit operation and maintenance data in accordance with Section 01 78 23, OPERATION AND MAINTENANCE DATA and as specified herein. Submit operation and maintenance manuals for electrical systems that provide basic data relating to the design, operation, and maintenance of the electrical distribution system for the building. Include the following:

a. Single line diagram of the "as-built" building electrical system.

b. Schematic diagram of electrical control system (other than HVAC, covered elsewhere).

c. Manufacturers' operating and maintenance manuals on active electrical equipment.

1.6 WARRANTY

Provide equipment items supported by service organizations that are reasonably convenient to the equipment installation in order to render satisfactory service to the equipment on a regular and emergency basis during the warranty period of the contract.

PART 2 PRODUCTS

2.1 MATERIALS AND EQUIPMENT

As a minimum, meet requirements of UL, where UL standards are established for those items, and requirements of NFPA 70 for all materials, equipment, and devices.

2.2 CONDUIT AND FITTINGS

Conform to the following:

2.2.1 Rigid Metallic Conduit

2.2.1.1 Rigid, Threaded Zinc-Coated Steel Conduit

ANSI C80.1, UL 6.

2.2.1.2 Rigid Aluminum Conduit

ANSI C80.5, UL 6A.

2.2.2 Rigid Nonmetallic Conduit

PVC Type EPC-40, and EPC-80 in accordance with NEMA TC 2,UL 651.

2.2.3 Intermediate Metal Conduit (IMC)

UL 1242, zinc-coated steel only.

2.2.4 Electrical, Zinc-Coated Steel Metallic Tubing (EMT)

UL 797, ANSI C80.3.

2.2.5 Plastic-Coated Rigid Steel and IMC Conduit

NEMA RN 1, Type 40(40 mils thick).

2.2.6 Flexible Metal Conduit

UL 1, limited to 6 feet.

2.2.6.1 Liquid-Tight Flexible Metal Conduit, Steel

UL 360, limited to 6 feet.

2.2.7 Fittings for Metal Conduit, EMT, and Flexible Metal Conduit

UL 514B. Ferrous fittings: cadmium- or zinc-coated in accordance with UL 514B.

2.2.7.1 Fittings for Rigid Metal Conduit and IMC

Threaded-type. Split couplings unacceptable.

2.2.7.2 Fittings for EMT

Steel compression type.

2.2.8 Fittings for Rigid Nonmetallic Conduit

NEMA TC 3 for PVC, and UL 514B.

2.2.9 Liquid-Tight Flexible Nonmetallic Conduit

UL 1660.

2.3 SURFACE RACEWAY

2.3.1 Surface Metal Raceway

UL 5, two-piece painted steel, totally enclosed, snap-cover type. Provide multiple outlet-type raceway with grounding-type receptacle where indicated. Provide receptacles as specified herein.

2.3.2 Surface Nonmetallic Raceway

UL 5A, nonmetallic totally enclosed, snap-cover type. Provide multiple outlet-type raceway with grounding-type receptacle where indicated.

2.4 BUSWAY

NEMA BU 1.1, UL 857. Provide the following:

a. Buses: copper.

d. Busway systems: suitable for use indoors. Fixed support system.

e. Enclosures: steel.

f. Hardware: plated or otherwise protected to resist corrosion.

g. Joints: one-bolt type with through-bolts, which can be checked for tightness without de-energizing system.

h. Maximum hot spot temperature rise at any point in busway at continuous rated load: do not exceed 55 degrees C above maximum ambient temperature of 40 degrees C in any position.

i. Internal barriers to prevent movement of superheated gases.

j. Coordinate proper voltage phasing of entire bus duct system, for example where busway interfaces with transformers, switchgear, switchboards, motor control centers, and other system components.

2.4.1 Feeder Busways

Provide low-impedance busway. Provide bus bars fully covered with insulating material, except at stabs. Provide an entirely polarized busway system.

2.4.2 Plug-In Busways

Unventilated type. Provide the following:

a. Plug-in units: circuit breaker-type, switch type, equipped with high interrupting-capacity, current-limiting fuses.

b. Bus bars: covered with insulating material throughout, except at joints and other connection points.

2.5 CABLE TRAYS

NEMA VE 2. Provide the following:

Submit cable tray design, including dimensional layout, load and seismic calculations, and fill calculations. Dimensional layout includes cable spacings, cable tray splices, and supports. Fill calculations include an index of cables for each section and identification of the lb/ft, cross sectional area, and insulation voltage class for each cable.

a. Cable trays: form a wireway system.

b. Cable trays: constructed of steel that has been hot-dipped galvanized after fabrication.

c. Cable trays: include splice and end plates, dropouts, and miscellaneous hardware.

d. Edges, fittings, and hardware: finished free from burrs and sharp edges.

e. Fittings: ensure not less than load-carrying ability of straight tray sections and have manufacturer's minimum standard radius.

f. Radius of bends: as indicated.

2.5.1 Trough-Type Cable Trays

Provide size as indicated. Cable tray must be suitable for use as an equipment grounding conductor.

2.5.2 Ladder-Type Cable Trays

Provide size as indicated. Cable tray must be suitable for use as an equipment grounding conductor.

2.5.3 Channel-Type Cable Trays

Provide size as indicated. Provide size as indicated. Cable tray must be suitable for use as an equipment grounding conductor.

2.5.4 Solid Bottom-Type Cable Trays

Provide size as indicated. Provide solid covers.

2.5.5 Cantilever

Cantilever-type, center-hung cable trays may be provided at the Contractor's option in lieu of other cable tray types specified.

2.6 OPEN TELECOMMUNICATIONS CABLE SUPPORT

2.6.1 Open Top Cable Supports

Provide open top cable supports in accordance with UL 2043. Provide open top cable supports as indicated.

2.6.2 Closed Ring Cable Supports

Provide closed ring cable supports in accordance with UL 2043. Provide closed ring cable supports as indicated.

2.7 OUTLET BOXES AND COVERS

UL 514A, cadmium- or zinc-coated, if ferrous metal. UL 514C, if nonmetallic.

2.7.1 Floor Outlet Boxes

Provide the following:

a. Boxes: nonadjustable and concrete tight.

b. Telecommunications outlets: consisting of surface-mounted, aluminum or stainless steel housing with a receptacle as specified and 3/4 inch top opening.

c. Receptacle outlets: consisting of surface-mounted, aluminum or stainless steel housing with duplex-type receptacle as specified herein.

d. Provide gaskets where necessary to ensure watertight installation.

2.7.2 Outlet Boxes for Telecommunications System

Provide the following:

a. Standard type 4 inches square by 2 1/8 inches deep.

b. Outlet boxes for wall-mounted telecommunications outlets: 4 by 2 1/8 by 2 1/8 inches deep.

c. Depth of boxes: large enough to allow manufacturers' recommended conductor bend radii.

d. Outlet boxes for fiber optic telecommunication outlets: include a minimum 3/8 inch deep single or two gang plaster ring as shown and installed using a minimum one inch conduit system.

e. Outlet boxes for handicapped telecommunications station: 5 inches square by 2 7/8 inches deep deep.

2.7.3 Clock Outlet for Use in Other Than Wired Clock System

Provide the following:

a. Outlet box with plastic cover, where required, and single receptacle with clock outlet plate.

b. Receptacle: recessed sufficiently within box to allow complete insertion of standard cap, flush with plate.

c. Suitable clip or support for hanging clock: secured to top plate.

d. Material and finish of plate: as specified in paragraph DEVICE PLATES of this section.

2.8 CABINETS, JUNCTION BOXES, AND PULL BOXES

UL 50; volume greater than 100 cubic inches, NEMA Type 1 enclosure; sheet steel, hot-dip, zinc-coated. Where exposed to wet, damp, or corrosive environments, NEMA Type as indicated.

2.9 WIRES AND CABLES

Provide wires and cables in accordance applicable requirements of NFPA 70 and UL for type of insulation, jacket, and conductor specified or indicated. Do not use wires and cables manufactured more than 24 months prior to date of delivery to site.

2.9.1 Conductors

Provide the following:

a. Conductor sizes and capacities shown are based on copper, unless indicated otherwise.

b. Conductors No. 8 AWG and larger diameter: stranded.

c. Conductors No. 10 AWG and smaller diameter: solid.

d. Conductors for remote control, alarm, and signal circuits, classes 1, 2, and 3: stranded unless specifically indicated otherwise.

e. All conductors: copper.

2.9.1.1 Equipment Manufacturer Requirements

When manufacturer's equipment requires copper conductors at the terminations or requires copper conductors to be provided between components of equipment, provide copper conductors or splices, splice boxes, and other work required to satisfy manufacturer's requirements.

2.9.1.2 Minimum Conductor Sizes

Provide minimum conductor size in accordance with the following:

a. Branch circuits: No. 12 AWG.

b. Class 1 remote-control and signal circuits: No. 14 AWG.

c. Class 2 low-energy, remote-control and signal circuits: No. 16 AWG.

d. Class 3 low-energy, remote-control, alarm and signal circuits: No. 22 AWG.

2.9.2 Color Coding

Provide color coding for service, feeder, branch, control, and signaling circuit conductors.

2.9.2.1 Ground and Neutral Conductors

Provide color coding of ground and neutral conductors as follows:

a. Grounding conductors: Green.

b. Neutral conductors: White.

c. Exception, where neutrals of more than one system are installed in same raceway or box, other neutrals color coding: white with a different colored (not green) stripe for each.

2.9.2.2 Ungrounded Conductors

Provide color coding of ungrounded conductors in different voltage systems as follows:

a. 208/120 volt, three-phase

(1) Phase A - black

(2) Phase B - red

(3) Phase C - blue

b. 480/277 volt, three-phase

(1) Phase A - brown

(2) Phase B - orange

(3) Phase C - yellow

2.9.3 Insulation

Unless specified or indicated otherwise or required by NFPA 70, provide power and lighting wires rated for 600-volts, Type THWN/THHN conforming to UL 83 or Type XHHW or RHW conforming to UL 44, except that grounding wire may be type TW conforming to UL 83; remote-control and signal circuits: Type TW or TF, conforming to UL 83. Where equipment or devices require 90-degree Centigrade (C) conductors, provide only conductors with 90-degree C insulation or better.

2.9.4 Bonding Conductors

ASTM B1, solid bare copper wire for sizes No. 8 AWG and smaller diameter; ASTM B8, Class B, stranded bare copper wire for sizes No. 6 AWG and larger diameter.

2.9.4.1 Telecommunications Bonding Backbone (TBB)

Provide a copper conductor TBB in accordance with TIA-607 with No. 6 AWG minimum size, and sized at 2 kcmil per linear foot of conductor length up to a maximum size of 750 kcmil.

2.9.4.2 Bonding Conductor for Telecommunications

Provide a copper conductor Bonding Conductor for Telecommunications between the telecommunications main grounding busbar (PBB) and the electrical service ground in accordance with TIA-607. Size the bonding conductor for telecommunications the same as the TBB.

2.9.5 Service Entrance Cables

Service Entrance (SE) and Underground Service Entrance (USE) Cables, UL 854.

2.9.6 Nonmetallic Sheathed Cable

UL 719, Type NM or NMC.

2.9.7 Wire and Cable for 400 Hertz (Hz) Circuits

Insulated copper conductors.

2.9.8 Mineral-Insulated, Metal-Sheathed Cable

UL listed; NFPA 70, Type MI cable. Do not use sheathing containing asbestos fibers.

2.9.9 Flat Conductor Cable

UL listed; NFPA 70, Type FCC.

2.9.10 Cable Tray Cable or Power Limited Tray Cable

UL listed; type TC or PLTC.

2.9.11 Cord Sets and Power-Supply Cords

UL 817.

2.10 SPLICES AND TERMINATION COMPONENTS

UL 486A-486B for wire connectors and UL 510 for insulating tapes. Connectors for No. 10 AWG and smaller diameter wires: insulated, pressure-type in accordance with UL 486A-486B or UL 486C (twist-on splicing connector). Provide solderless terminal lugs on stranded conductors.

2.11 DEVICE PLATES

Provide the following:

a. UL listed, one-piece device plates for outlets to suit the devices installed.

b. For metal outlet boxes, plates on unfinished walls: zinc-coated sheet steel or cast metal having round or beveled edges.

c. For nonmetallic boxes and fittings, other suitable plates may be provided.

d. Plates on finished walls: nylon or lexan, minimum 0.03 inch wall thickness and same color as receptacle or toggle switch with which they are mounted.

e. Plates on finished walls: satin finish stainless steel or brushed-finish aluminum, minimum 0.03 inch thick.

f. Screws: machine-type with countersunk heads in color to match finish of plate.

g. Sectional type device plates are not be permitted.

h. Plates installed in wet locations: gasketed and UL listed for "wet locations."

i. Device plates in areas normally accessible to prisoners: brown or ivory finish nylon-device plates rated for high abuse. Test device plates for compliance with UL 514A and UL 514C for physical strength. Attach device plates with spanner head bolts.

2.12 SWITCHES

2.12.1 Toggle Switches

NEMA WD 1, UL 20, single pole, double pole, three-way, and four-way, totally enclosed with bodies of thermoplastic or thermoset plastic and mounting strap with grounding screw. Include the following:

a. Handles: white or ivory thermoplastic.

b. Wiring terminals: screw-type, side-wired.

c. Contacts: silver-cadmium and contact arm - one-piece copper alloy.

d. Switches: rated quiet-type ac only, 120/277 volts, with current rating and number of poles indicated.

2.12.2 Switch with Red Pilot Handle

NEMA WD 1. Provide the following:

a. Pilot lights that are integrally constructed as a part of the switch's handle.

b. Pilot light color: red and illuminate whenever the switch is closed or "on".

c. Pilot lighted switch: rated 20 amps and 120 volts or 277 volts as indicated.

d. The circuit's neutral conductor to each switch with a pilot light.

2.12.3 Breakers Used as Switches

For 120- and 277-Volt fluorescent fixtures, mark breakers "SWD" in accordance with UL 489.

2.12.4 Disconnect Switches

NEMA KS 1. Provide heavy duty-type switches where indicated, where switches are rated higher than 240 volts, and for double-throw switches. Utilize Class R fuseholders and fuses for fused switches, unless indicated otherwise. Provide horsepower rated for switches serving as the motor-disconnect means. Provide switches in NEMA as indicated per NEMA ICS 6.

2.13 FUSES

NEMA FU 1. Provide complete set of fuses for each fusible switch and control center. Coordinate time-current characteristics curves of fuses serving motors or connected in series with circuit breakers or other circuit protective devices for proper operation. Submit coordination data for approval. Provide fuses with a voltage rating not less than circuit voltage.

2.13.1 Fuseholders

Provide in accordance with UL 4248-1.

2.14 RECEPTACLES

Provide the following:

a. UL 498, general purpose specification grade, grounding-type. Residential grade receptacles are not acceptable.

b. Ratings and configurations: as indicated.

c. Bodies: white or ivory as per NEMA WD 1.

d. Face and body: thermoplastic supported on a metal mounting strap.

e. Dimensional requirements: per NEMA WD 6.

f. Screw-type, side-wired wiring terminals or of the solderless pressure type having suitable conductor-release arrangement.

g. Grounding pole connected to mounting strap.

h. The receptacle: containing triple-wipe power contacts and double or triple-wipe ground contacts.

i. Controlled receptacles: as required per ASHRAE 90.1. Provide marking for controlled receptacle per NFPA 70.

2.14.1 Split Duplex Receptacles

Provide separate terminals for each ungrounded pole. One receptacle must be controlled separately.

2.14.2 Weatherproof Receptacles

Provide receptacles, UL listed for use in "wet locations" with integral GFCI protection. Include cast metal box with gasketed, hinged, lockable and weatherproof while-in-use, polycarbonate extra-duty rated hood.

2.14.3 Ground-Fault Circuit Interrupter Receptacles

UL 943, duplex type for mounting in standard outlet box. Provide device capable of detecting current leak when the current to ground is 6 milliamperes or higher, and tripping per requirements of UL 943 for Class A ground-fault circuit interrupter devices. Provide screw-type, side-wired wiring terminals or pre-wired (pigtail) leads.

2.14.4 Tamper-Resistant Receptacles

Provide duplex receptacle with mechanical sliding shutters that prevent the insertion of small objects into its contact slots.

2.15 PANELBOARDS

Provide panelboards in accordance with the following:

a. UL 67 and UL 50 having a short-circuit current rating as indicated.

b. Panelboards for use as service disconnecting means: additionally conform to UL 869A.

c. Panelboards: circuit breaker-equipped.

d. Designed such that individual breakers can be removed without disturbing adjacent units or without loosening or removing supplemental insulation supplied as means of obtaining clearances as required by UL.

e. "Specific breaker placement" is required in panelboards to match the breaker placement indicated in the panelboard schedule on the design drawings. If it is not possible to match "specific breaker placement"

during construction, obtain Government approval prior to device installation.

f. Use of "Subfeed Breakers" is not acceptable.

g. Main breaker: "separately" mounted "above" branch breakers.

h. Where "space only" is indicated, make provisions for future installation of breakers.

i. Directories: indicate load served by each circuit in panelboard.

j. Directories: indicate source of service to panelboard (e.g., Panel PA served from Panel MDP).

k. Type directories and mount in holder behind transparent protective covering.

l. Panelboards: listed and labeled for their intended use.

m. Panelboard nameplates: provided in accordance with paragraph FIELD FABRICATED NAMEPLATES.

2.15.1 Enclosure

Provide panelboard enclosure in accordance with the following:

a. UL 50.

b. Cabinets mounted outdoors or flush-mounted: hot-dipped galvanized after fabrication.

c. Cabinets: painted in accordance with paragraph FIELD APPLIED PAINTING.

d. Outdoor cabinets: NEMA 3R raintight with conduit hubs welded to the cabinet.

e. Front edges of cabinets: form-flanged or fitted with structural shapes welded or riveted to the sheet steel, for supporting the panelboard front.

f. All cabinets: fabricated such that no part of any surface on the finished cabinet deviates from a true plane by more than 1/8 inch.

g. Holes: provided in the back of indoor surface-mounted cabinets, with outside spacers and inside stiffeners, for mounting the cabinets with a 1/2 inch clear space between the back of the cabinet and the wall surface.

h. Flush doors: mounted on hinges that expose only the hinge roll to view when the door is closed.

i. Each door: fitted with a combined catch and lock latch.

j. Keys: two provided with each lock, with all locks keyed alike.

k. Finished-head cap screws: provided for mounting the panelboard fronts on the cabinets.

2.15.2 Panelboard Buses

Support bus bars on bases independent of circuit breakers. Design main buses and back pans so that breakers may be changed without machining, drilling, or tapping. Provide isolated neutral bus in each panel for connection of circuit neutral conductors. Provide separate ground bus identified as equipment grounding bus per UL 67 for connecting grounding conductors; bond to steel cabinet.

2.15.3 Circuit Breakers

UL 489, solid state-type having a minimum short-circuit current rating equal to the short-circuit current rating of the panelboard in which the circuit breaker will be mounted. Breaker terminals: UL listed as suitable for type of conductor provided. Where indicated on the drawings, provide circuit breakers with shunt trip devices. Series rated circuit breakers and plug-in circuit breakers are unacceptable.

2.15.3.1 Multipole Breakers

Provide common trip-type with single operating handle. Design breaker such that overload in one pole automatically causes all poles to open. Maintain phase sequence throughout each panel so that any three adjacent breaker poles are connected to Phases A, B, and C, respectively.

2.15.3.2 Circuit Breaker With Ground-Fault Circuit Interrupter

UL 943 and NFPA 70. Provide with auto-monitoring (self-test) and lockout features, "push-to-test" button, visible indication of tripped condition, and ability to detect and trip when current imbalance is 6 milliamperes or higher per requirements of UL 943 for Class A ground-fault circuit interrupter devices.

2.15.4 Branch Circuit Monitoring Panelboards

Provide a microprocessor-based panelboard monitoring system having the following features:

a. ANSI C12.1 and IEC 62053-21 Class 1 energy revenue metering accuracy.

b. Direct reading metered or calculated values for up to forty-two branch circuits.

c. Monitored values at the branch circuit level for current (A), power (kW), and energy (kWh).

d. Four user-configurable alarm thresholds.

e. Communications with building automation system using Modbus RTU protocol via RS-485 cable connection.

2.16 ENCLOSED CIRCUIT BREAKERS

UL 489. Individual molded case circuit breakers with voltage and continuous current ratings, number of poles, overload trip setting, and short circuit current interrupting rating as indicated. Enclosure type as indicated.

2.17 MOTOR SHORT-CIRCUIT PROTECTOR (MSCP)

Motor short-circuit protectors, also called motor circuit protectors (MCPs): UL 508 and UL 489, and provided as shown. Provide MSCPs that consist of an adjustable instantaneous trip circuit breaker used only in conjunction with a combination motor controller which provides coordinated motor branch-circuit overload and short-circuit protection. Rate MSCPs in accordance with the requirements of NFPA 70.

2.18 TRANSFORMERS

Provide transformers in accordance with the following:

a. NEMA ST 20, general purpose, dry-type, self-cooled.

b. Provide transformers in NEMA enclosure as indicated on plans.

c. Taps for transformers 15 kVA and larger: Two 2.5 percent taps Full Capacity Above Nominal (FCAN) and four 2.5 percent taps Full Capacity Below Nominal (FCBN).

d. Transformer insulation system:

(1) 220 degrees C insulation system for transformers 15 kVA and greater, with temperature rise not exceeding 115 degrees C under full-rated load in maximum ambient of 40 degrees C.

(2) 180 degrees C insulation for transformers rated 10 kVA and less, with temperature rise not exceeding 80 degrees C under full-rated load in maximum ambient of 40 degrees C.

e. Transformer of 150 degrees C temperature rise is not acceptable.

f. Transformer of 115 degrees C temperature rise: capable of carrying continuously 115 percent of nameplate kVA without exceeding insulation rating.

g. Transformer of 80 degrees C temperature rise: capable of carrying continuously 130 percent of nameplate kVA without exceeding insulation rating.

h. Transformers: quiet type with maximum sound level at least 3 decibels less than NEMA standard level for transformer ratings indicated.

2.18.1 Specified Transformer Efficiency

Transformers, indicated and specified with: 480V primary, 80 degrees C or 115 degrees C temperature rise, kVA ratings of 37.5 to 100 for single phase or 30 to 500 for three phase, energy efficient type. The transformer is not acceptable if the calculated transformer efficiency is less than the efficiency indicated in 10 CFR 431, Subpart K.

2.18.2 K-Rated Transformers

Provide K-rated transformers for non-linear loads in accordance with the following:

a. Transformer insulation: UL recognized 220 degrees C system. Neither

the primary nor the secondary temperature is allowed to exceed 220 degrees C at any point in the coils while carrying their full rating of non-sinusoidal load.

b. Transformers are to be UL listed and labeled for K-Factor rating as indicated in accordance with UL 1561.

c. Transformers evaluated by the UL K-Factor evaluation: listed for 115 degrees C average temperature rise only.

d. Transformers with K-Factor ratings with temperature rise of 150 degrees C rise are not acceptable.

e. K-Factor rated transformers impedance: allowed range of 3 percent to 5 percent, with a minimum reactance of 2 percent to prevent excessive neutral current when supplying loads with large amounts of third harmonic.

2.19 MOTORS

Provide motors in accordance with the following:

a. NEMA MG 1.

b. Hermetic-type sealed motor compressors: Also comply with UL 984.

c. Provide the size in terms of HP, or kVA, or full-load current, or a combination of these characteristics, and other characteristics, of each motor as indicated or specified.

d. Determine specific motor characteristics to ensure provision of correctly sized starters and overload heaters.

e. Rate motors for operation on 208-volt, 3-phase circuits with a terminal voltage rating of 200 volts, and those for operation on 480-volt, 3-phase circuits with a terminal voltage rating of 460 volts.

f. Use motors designed to operate at full capacity with voltage variation of plus or minus 10 percent of motor voltage rating.

g. Unless otherwise indicated, use continuous duty type motors if rated 1 HP and above.

h. Where fuse protection is specifically recommended by the equipment manufacturer, provide fused switches in lieu of non-fused switches indicated.

2.19.1 High Efficiency Single-Phase Motors

Single-phase fractional-horsepower alternating-current motors: high efficiency types are not acceptable. In exception, for special purpose motors and motor-driven equipment with a minimum seasonal or overall efficiency rating, such as a SEER rating, provide equipment with motor to meet the overall system rating indicated.

2.19.2 Premium Efficiency Polyphase and Single-Phase Motors

Select polyphase and continuous-duty single phase motors based on high

efficiency characteristics relative to typical characteristics and applications as listed in NEMA MG 10 and NEMA MG 11. In addition, continuous rated, polyphase squirrel-cage medium induction motors must meet the requirements for premium efficiency electric motors in accordance with NEMA MG 1, including the NEMA full load efficiency ratings. In exception, for motor-driven equipment with a minimum seasonal or overall efficiency rating, such as a SEER rating, provide equipment with motor to meet the overall system rating indicated. Electronically Commutated Motors (ECM) to have an integrated controller that senses rotor position and electronically commutates the stator windings to provide synchronous rotation. The rotor must be of a permanent magnet type supported by ball bearings to increase motor efficiency and longevity. The motor must maintain 70 percent or greater efficiency for its design application. ECM motors to comply with UL 1004-1.

2.19.3 Motor Sizes

Provide size for duty to be performed, not exceeding the full-load nameplate current rating when driven equipment is operated at specified capacity under most severe conditions likely to be encountered. When motor size provided differs from size indicated or specified, make adjustments to wiring, disconnect devices, and branch circuit protection to accommodate equipment actually provided. Provide controllers for motors rated 1-hp and above with electronic phase-voltage monitors designed to protect motors from phase-loss, undervoltage, and overvoltage. Provide protection for motors from immediate restart by a time adjustable restart relay.

2.19.4 Wiring and Conduit

Provide internal wiring for components of packaged equipment as an integral part of the equipment. Provide power wiring and conduit for field-installed equipment using adjustable speed drive (ASD) manufacturer required wiring type and length, and motor control equipment forming part of motor control centers or switchgear assemblies, the conduit and wiring connecting such centers, assemblies, or other power sources to equipment as specified herein. Power wiring and conduit: conform to the requirements specified herein. Control wiring: provided under, and conform to, the requirements of the section specifying the associated equipment.

2.20 MOTOR CONTROLLERS

Provide motor controllers in accordance with the following:

a. UL 508, NEMA ICS 1, and NEMA ICS 2.

b. Provide controllers with thermal overload protection in each phase, and one spare normally open auxiliary contact, and one spare normally closed auxiliary contact.

c. Provide controllers for motors rated 1-hp 746 watts and above with electronic phase-voltage monitors designed to protect motors from phase-loss, undervoltage, and overvoltage.

d. Provide protection for motors from immediate restart by a time adjustable restart relay.

e. When used with pressure, float, or similar automatic-type or

maintained-contact switch, provide a hand/off/automatic selector switch with the controller.

f. Connections to selector switch: wired such that only normal automatic regulatory control devices are bypassed when switch is in "hand" position.

g. Safety control devices, such as low and high pressure cutouts, high temperature cutouts, and motor overload protective devices: connected in motor control circuit in "hand" and "automatic" positions.

h. Control circuit connections to hand/off/automatic selector switch or to more than one automatic regulatory control device: made in accordance with indicated or manufacturer's approved wiring diagram.

i. Provide selector switch with the means for locking in any position.

j. Provide a disconnecting means, capable of being locked in the open position, for the motor that is located in sight from the motor location and the driven machinery location. As an alternative, provide a motor controller disconnect, capable of being locked in the open position, to serve as the disconnecting means for the motor if it is in sight from the motor location and the driven machinery location.

k. Overload protective devices: provide adequate protection to motor windings; be thermal inverse-time-limit type; and include manual reset-type pushbutton on outside of motor controller case.

l. Cover of combination motor controller and manual switch or circuit breaker: interlocked with operating handle of switch or circuit breaker so that cover cannot be opened unless handle of switch or circuit breaker is in "off" position.

m. Provide controllers in hazardous locations with classifications as indicated.

2.20.1 Control Wiring

Provide control wiring in accordance with the following:

a. All control wire: stranded tinned copper switchboard wire with 600-volt flame-retardant insulation Type SIS meeting UL 44, or Type MTW meeting UL 1063, and passing the VW-1 flame tests included in those standards.

b. Hinge wire: Class K stranding.

c. Current transformer secondary leads: not smaller than No. 10 AWG.

d. Control wire minimum size: No. 14 AWG.

e. Power wiring for 480-volt circuits and below: the same type as control wiring with No. 12 AWG minimum size.

f. Provide wiring and terminal arrangement on the terminal blocks to permit the individual conductors of each external cable to be terminated on adjacent terminal points.

2.20.2 Control Circuit Terminal Blocks

Provide control circuit terminal blocks in accordance with the following:

a. NEMA ICS 4.

b. Control circuit terminal blocks for control wiring: molded or fabricated type with barriers, rated not less than 600 volts.

c. Provide terminals with removable binding, fillister or washer head screw type, or of the stud type with contact and locking nuts.

d. Terminals: not less than No. 10 in size with sufficient length and space for connecting at least two indented terminals for 10 AWG conductors to each terminal.

e. Terminal arrangement: subject to the approval of the Contracting Officer with not less than four spare terminals or 10 percent, whichever is greater, provided on each block or group of blocks.

f. Modular, pull apart, terminal blocks are acceptable provided they are of the channel or rail-mounted type.

g. Submit data showing that any proposed alternate will accommodate the specified number of wires, are of adequate current-carrying capacity, and are constructed to assure positive contact between current-carrying parts.

2.20.2.1 Types of Terminal Blocks

a. Short-Circuiting Type: Short-circuiting type terminal blocks: furnished for all current transformer secondary leads with provision for shorting together all leads from each current transformer without first opening any circuit. Terminal blocks: comply with the requirements of paragraph CONTROL CIRCUIT TERMINAL BLOCKS above.

b. Load Type: Load terminal blocks rated not less than 600 volts and of adequate capacity: provided for the conductors for NEMA Size 3 and smaller motor controllers and for other power circuits, except those for feeder tap units. Provide terminals of either the stud type with contact nuts and locking nuts or of the removable screw type, having length and space for at least two indented terminals of the size required on the conductors to be terminated. For conductors rated more than 50 amperes, provide screws with hexagonal heads. Conducting parts between connected terminals must have adequate contact surface and cross-section to operate without overheating. Provide each connected terminal with the circuit designation or wire number placed on or near the terminal in permanent contrasting color.

2.20.3 Control Circuits

Control circuits: maximum voltage of 120 volts derived from control transformer in same enclosure. Transformers: conform to UL 506, as applicable. Transformers, other than transformers in bridge circuits: provide primaries wound for voltage available and secondaries wound for correct control circuit voltage. Size transformers so that 80 percent of rated capacity equals connected load. Provide disconnect switch on primary side. For designated systems, as indicated, provide backup power supply, including transformers connected to emergency power source.

Provide for automatic switchover and alarm upon failure of primary control circuit.

2.20.4 Enclosures for Motor Controllers

NEMA ICS 6.

2.20.5 Multiple-Speed Motor Controllers and Reversible Motor Controllers

Across-the-line-type, electrically and mechanically interlocked. Multiple-speed controllers: include compelling relays and multiple-button, station-type with pilot lights for each speed.

2.20.6 Pushbutton Stations

Provide with "start/stop" momentary contacts having one normally open and one normally closed set of contacts, and red lights to indicate when motor is running. Stations: heavy duty, oil-tight design.

2.20.7 Pilot and Indicating Lights

Provide transformer, resistor, or diode type.

2.21 MANUAL MOTOR STARTERS (MOTOR RATED SWITCHES)

Single, Double, or Three pole designed for surface mounting with overload protection.

2.21.1 Pilot Lights

Provide yoke-mounted, seven element LED cluster light module.

2.22 LOCKOUT REQUIREMENTS

Provide circuit breakers, disconnecting means, and other devices that are electrical energy-isolating capable of being locked out for machines and other equipment to prevent unexpected startup or release of stored energy in accordance with 29 CFR 1910.147, NFPA 70E and 29 CFR 1910.303. Comply with requirements of Division 23, "Heating, Ventilating, and Air Conditioning (HVAC)" for mechanical isolation of machines and other equipment.

2.23 TELECOMMUNICATIONS SYSTEM

Provide system of telecommunications wire-supporting structures (pathway), including: outlet boxes, conduits with pull wires wireways, cable trays, and other accessories for telecommunications outlets and pathway in accordance with TIA-569 and as specified herein. Additional telecommunications requirements are specified in Section 27 10 00 BUILDING TELECOMMUNICATIONS CABLING SYSTEM.

2.24 COMMUNITY ANTENNA TELEVISION (CATV) SYSTEM

Additional CATV requirements are specified in Section 27 05 13.43 TELEVISION DISTRIBUTION SYSTEM.

2.24.1 CATV Outlets

Provide flush mounted, 75-ohm, F-type connector outlet rated from 5 to

1000 MHz in standard electrical outlet boxes with isolation barrier with mounting frame.

2.24.2 CATV Faceplates

Provide modular faceplates for mounting of CATV Outlets. Faceplate: include designation labels and label covers for circuit identification. Faceplate color: match outlet and switch coverplates.

2.24.3 Backboards

Coordinate CATV backboard requirements with telecommunications backboard requirements as specified in Section 27 10 00 BUILDING TELECOMMUNICATIONS CABLING.

2.25 GROUNDING AND BONDING EQUIPMENT

2.25.1 Ground Rods

UL 467. Ground rods: cone pointed copper, with minimum diameter of 3/4 inch and minimum length 10 feet. Sectional type rods may be used for rods 20 feet or longer.

2.25.2 Ground Bus

Copper ground bus: provided in the electrical equipment rooms as indicated.

2.25.3 Secondary Bonding Busbar

Provide corrosion-resistant grounding busbar suitable for indoor installation in accordance with TIA-607. Busbars: plated for reduced contact resistance. If not plated, clean the busbar prior to fastening the conductors to the busbar and apply an anti-oxidant to the contact area to control corrosion and reduce contact resistance. Provide a Primary bonding busbar (PBB) in the telecommunications entrance facility and a Secondary bonding busbar (SBB) in all other telecommunications rooms and equipment rooms. The Primary bonding busbar (PBB) and the Secondary bonding busbar (SBB): sized in accordance with the immediate application requirements and with consideration of future growth. Provide Secondary bonding busbars with the following:

a. Predrilled copper busbar provided with holes for use with standard sized lugs,

b. Minimum dimensions of 0.25 in thick by 4 in wide for the PBB and 2 in wide for SBBs with length as indicated;

c. Listed by a nationally recognized testing laboratory.

2.26 MANUFACTURER'S NAMEPLATE

Provide on each item of equipment a nameplate bearing the manufacturer's name, address, model number, and serial number securely affixed in a conspicuous place; the nameplate of the distributing agent will not be acceptable.

2.27 FIELD FABRICATED NAMEPLATES

Provide field fabricated nameplates in accordance with the following:

a. ASTM D709.

b. Provide laminated plastic nameplates for each equipment enclosure, relay, switch, and device; as specified or as indicated on the drawings.

c. Each nameplate inscription: identify the function and, when applicable, the position.

d. Nameplates: melamine plastic, 0.125 inch thick, white with black center core.

e. Surface: matte finish. Corners: square. Accurately align lettering and engrave into the core.

f. Minimum size of nameplates: one by 2.5 inches.

g. Lettering size and style: a minimum of 0.25 inch high normal block style.

2.28 WARNING SIGNS

Provide warning signs for flash protection in accordance with NFPA 70E and NEMA Z535.4 for switchboards, panelboards, industrial control panels, and motor control centers that are in other than dwelling occupancies and are likely to require examination, adjustment, servicing, or maintenance while energized. Provide field installed signs to warn qualified persons of potential electric arc flash hazards when warning signs are not provided by the manufacturer. Provide marking that is clearly visible to qualified persons before examination, adjustment, servicing, or maintenance of the equipment.

2.29 FIRESTOPPING MATERIALS

Provide firestopping around electrical penetrations in accordance with Section 07 84 00 FIRESTOPPING.

2.30 WIREWAYS

UL 870. Material: steel galvanized 16 gauge for heights and depths up to 6 by 6 inches, and 14 gauge for heights and depths up to 12 by 12 inches. Provide in length indicated, as required for the application with hinged-cover NEMA 1 enclosure per NEMA ICS 6.

2.31 METERING

ANSI C12.1. Provide a self-contained, socket-mounted, electronic programmable outdoor watthour meter. Meter: either programmed at the factory or programmed in the field. Turn field programming device over to the Contracting Officer at completion of project. Coordinate meter to system requirements. Coordinate meter, system components, and meter location to be compatible with the Activity's central advanced metering system.

a. Design: Provide watthour meter designed for use on a single-phase,

three-wire, 480/240 volt system. Include necessary KYZ pulse initiation hardware for Energy Monitoring and Control System (EMCS).

b. Class: 200; accuracy: plus or minus 1.0 percent; Finish: Class II.

c. Cover: Polycarbonate and lockable to prevent tampering and unauthorized removal.

d. Kilowatt-hour Register: five digit electronic programmable type.

e. Demand Register:

(1) Provide solid state.

(2) Meter reading multiplier: Indicate multiplier on the meter face.

(3) Demand interval length: programmed for 60 minutes with rolling demand up to six subintervals per interval.

f. Socket: ANSI C12.7. Provide NEMA Type 3R, box-mounted socket, ringless, having jaws compatible with requirements of the meter. Provide manufacturers standard enclosure color unless otherwise indicated.

2.32 METER BASE ONLY

ANSI C12.7. Provide NEMA Type 3R, box-mounted socket, ringless, having jaws compatible with requirements of a class: 200 and self contained watthour meter. Provide gray plastic closing cover and bypass links. Provide manufacturers standard enclosure color unless otherwise indicated.

2.33 SURGE PROTECTIVE DEVICES

Provide parallel type surge protective devices (SPD) which comply with UL 1449 at the service entrance, panelboards. Provide surge protectors in a NEMA enclosure per NEMA ICS 6. Do not install SPD inside a panelboard or switchboard enclosure. However, SPD may be installed in a separate compartment of a switchgear provided that it is supplied by a dedicated circuit breaker. SPD must have the same short-circuit current rating as the protected equipment and must not be installed at a point of system where the available fault current is in excess of that rating. Use Type 1 or Type 2 SPD and connect on the load side of a dedicated circuit breaker. Submit performance and characteristic curves.

Provide the following modes of protection:

FOR SINGLE PHASE AND THREE PHASE WYE CONNECTED SYSTEMS-
Phase to phase (L-L)
Each phase to neutral (L-N)
Neutral to ground (N-G)
Phase to ground (L-G)

SPDs at the service entrance: provide with a minimum surge current rating of 80,000 amperes for L-L mode minimum and 40,000 amperes for other modes (L-N, L-G, and N-G) and downstream SPDs rated 40,000 amperes for L-L mode minimum and 20,000 amperes for other modes (L-N, L-G, and N-G).

Provide SPDs per NFPA 780 for the lightning protection system.

Maximum L-N, and N-G Voltage Protection Rating:

700V for 120V, single phase system
1,000V for 120/240V, single phase system
700V for 120/240V, three phase system
700V for 208Y/120V, three phase system
1,200V for 480Y/277V, three phase system

Maximum L-G Protection Rating:
700V for 120V, single phase system
1,000V for 120/240V, single phase system
700V for 120/240V, three phase system
700V for 208Y/120V, three phase system
1,200V for 480Y/277V, three phase system

Maximum L-L Voltage Protection Rating:

1,200V for 120/240V, three phase system
1,200V for 208Y/120V, three phase system
1,800V for 480Y/277V, three phase system

Provide SPDs.

Maximum L-N, L-G, and N-G Voltage Protection Rating:

700V for 120V, single phase system
700V for 120/240V, single phase system
700V for 208Y/120V, three phase system
1,200V for 480Y/277V, three phase system

Maximum L-L Voltage Protection Rating:

1,200V for 120V, single phase system
1,200V for 120/240V, single phase system
1,200V for 208Y/120V, three phase system
1,800V for 480Y/277V, three phase system

The minimum MCOV (Maximum Continuous Operating Voltage) rating for L-N and L-G modes of operation: 120 percent of nominal voltage for 240 volts and below; 115 percent of nominal voltage above 240 volts to 480 volts.

Provide EMI/RFI filtering when required by project documents.

2.34 FACTORY APPLIED FINISH

Provide factory-applied finish on electrical equipment in accordance with the following:

a. NEMA 250 corrosion-resistance test and the additional requirements as specified herein.

b. Interior and exterior steel surfaces of equipment enclosures: thoroughly cleaned followed by a rust-inhibitive phosphatizing or equivalent treatment prior to painting.

c. Exterior surfaces: free from holes, seams, dents, weld marks, loose scale or other imperfections.

d. Interior surfaces: receive not less than one coat of

corrosion-resisting paint in accordance with the manufacturer's standard practice.

e. Exterior surfaces: primed, filled where necessary, and given not less than two coats baked enamel with semigloss finish.

f. Equipment located indoors: ANSI Light Gray, and equipment located outdoors: ANSI Dark Gray.

g. Provide manufacturer's coatings for touch-up work and as specified in paragraph FIELD APPLIED PAINTING.

2.35 SOURCE QUALITY CONTROL

2.35.1 Transformer Factory Tests

Submittal: include routine NEMA ST 20 transformer test results on each transformer and also provide the results of NEMA "design" and "prototype" tests that were made on transformers electrically and mechanically equal to those specified.

PART 3 EXECUTION

3.1 INSTALLATION

Electrical installations, including weatherproof and hazardous locations and ducts, plenums and other air-handling spaces: conform to requirements of NFPA 70 and IEEE C2 and to requirements specified herein.

3.1.1 Underground Service

Underground service conductors and associated conduit: continuous from service entrance equipment to outdoor power system connection.

3.1.2 Service Entrance Identification

Service entrance disconnect devices, switches, and enclosures: labeled and identified as such.

3.1.2.1 Labels

Wherever work results in service entrance disconnect devices in more than one enclosure, as permitted by NFPA 70, label each enclosure, new and existing, as one of several enclosures containing service entrance disconnect devices. Label, at minimum: indicate number of service disconnect devices housed by enclosure and indicate total number of enclosures that contain service disconnect devices. Provide laminated plastic labels conforming to paragraph FIELD FABRICATED NAMEPLATES. Use lettering of at least 0.25 inch in height, and engrave on black-on-white matte finish. Service entrance disconnect devices in more than one enclosure: provided only as permitted by NFPA 70.

3.1.3 Wiring Methods

Provide insulated conductors installed in rigid steel conduit, IMC, rigid nonmetallic conduit, or EMT, except where specifically indicated or specified otherwise or required by NFPA 70 to be installed otherwise. Grounding conductor: separate from electrical system neutral conductor. Provide insulated green equipment grounding conductor for circuit(s)

installed in conduit and raceways. Minimum conduit size: 1/2 inch in diameter for low voltage lighting and power circuits. Vertical distribution in multiple story buildings: made with metal conduit in fire-rated shafts, with metal conduit extending through shafts for minimum distance of 6 inches. Firestop conduit which penetrates fire-rated walls, fire-rated partitions, or fire-rated floors in accordance with Section 07 84 00 FIRESTOPPING.

3.1.3.1 Pull Wire

Install pull wires in empty conduits. Pull wire: plastic having minimum 200-pound force tensile strength. Leave minimum 36 inches of slack at each end of pull wire.

3.1.3.2 Flat Conductor Cable

Install in accordance with NFPA 70, Type FCC cable.

3.1.4 Conduit Installation

Unless indicated otherwise, conceal conduit under floor slabs and within finished walls, ceilings, and floors. Keep conduit minimum 6 inches away from parallel runs of flues and steam or hot water pipes. Install conduit parallel with or at right angles to ceilings, walls, and structural members where located above accessible ceilings and where conduit will be visible after completion of project.

3.1.4.1 Restrictions Applicable to Aluminum Conduit

a. Do not install underground or encase in concrete or masonry.

b. Do not use brass or bronze fittings.

c. Do not use when the enclosed conductors must be shielded from the effects of High-altitude Electromagnetic Pulse (HEMP).

3.1.4.2 Restrictions Applicable to EMT

a. Do not install underground.

b. Do not encase in concrete, mortar, grout, or other cementitious materials.

c. Do not use in areas subject to physical damage including but not limited to equipment rooms where moving or replacing equipment could physically damage the EMT.

d. Do not use in hazardous areas.

e. Do not use outdoors.

f. Do not use in fire pump rooms.

g. Do not use when the enclosed conductors must be shielded from the effects of High-altitude Electromagnetic Pulse (HEMP).

3.1.4.3 Restrictions Applicable to Nonmetallic Conduit

a. PVC Schedule 40.

(1) Do not use where subject to physical damage, including but not limited to, mechanical equipment rooms, electrical equipment rooms, fire pump rooms, and where restrictions are applying to both PVC Schedule 40 and PVC Schedule 80.

(2) Do not use above grade, except where allowed in this section for rising through floor slab or indicated otherwise.

b. PVC Schedule 80.

(1) Do not use where subject to physical damage, including but not limited to, hospitals, power plant, missile magazines, and other such areas.

(2) Do not use in hazardous (classified) areas.

(3) Do not use in penetrating fire-rated walls or partitions, or fire-rated floors.

-

3.1.4.4 Restrictions Applicable to Flexible Conduit

Use only as specified in paragraph FLEXIBLE CONNECTIONS. Do not use when the enclosed conductors must be shielded from the effects of High-altitude Electromagnetic Pulse (HEMP).

3.1.4.5 Underground Conduit

Plastic-coated rigid steel; plastic-coated steel IMC; PVC, Type EPC-40 Plastic coating: extend minimum 6 inches above floor.

3.1.4.6 Conduit for Circuits Rated Greater Than 600 Volts

Rigid metal conduit or IMC only.

3.1.4.7 Conduit Installed Under Floor Slabs

Conduit run under floor slab: located a minimum of 12 inches below the vapor barrier. Seal around conduits at penetrations thru vapor barrier. Use NECA NEIS 1 Table 2a (Minimum Raceway Spacing) to determine under floor slab conduit spacing unless greater spacing is required elsewhere in this section.

3.1.4.8 Conduit Through Floor Slabs

Where conduits rise through floor slabs, do not allow curved portion of bends to be visible above finished slab. Where conduit rises through slab-on grade, seal all electrical penetrations to address radon mitigation and prevent infiltration of air, insects, and vermin.

3.1.4.9 Conduit Installed in Concrete Floor Slabs or Concrete Walls

PVC, Type EPC-40, unless indicated otherwise. Locate so as not to adversely affect structural strength of slabs. Install conduit within middle one-third of concrete slab. Do not stack conduits. Space conduits horizontally not closer than three diameters, except at cabinet locations. Curved portions of bends must not be visible above finish slab. Increase slab thickness as necessary to provide minimum one inch cover over conduit. Where embedded conduits cross building expansion

joints, provide suitable watertight expansion/deflection fittings and bonding jumpers. Expansion/deflection fittings must allow horizontal and vertical movement of raceway. Conduit larger than one inch trade size: installed parallel with or at right angles to main reinforcement; when at right angles to reinforcement, install conduit close to one of supports of slab. Where nonmetallic conduit is used, convert raceway to plastic coated rigid steel or plastic coated steel IMC before rising above floor, unless specifically indicated.

3.1.4.10 Stub-Ups

Provide conduits stubbed up through concrete floor for connection to free-standing equipment with adjustable top or coupling threaded inside for plugs, set flush with finished floor. Extend conductors to equipment in rigid steel conduit, except that flexible metal conduit may be used 6 inches above floor. Where no equipment connections are made, install screwdriver-operated threaded flush plugs in conduit end.

3.1.4.11 Conduit Support

Support conduit by pipe straps, wall brackets, threaded rod conduit hangers, or ceiling trapeze. Plastic cable ties are not acceptable. Fasten by wood screws to wood; by toggle bolts on hollow masonry units; by concrete inserts or expansion bolts on concrete or brick; and by machine screws, welded threaded studs, or spring-tension clamps on steel work. Threaded C-clamps may be used on rigid steel conduit only. Do not weld conduits or pipe straps to steel structures. Do not exceed one-fourth proof test load for load applied to fasteners. Provide vibration resistant and shock-resistant fasteners attached to concrete ceiling. Do not cut main reinforcing bars for any holes cut to depth of more than 1 1/2 inches in reinforced concrete beams or to depth of more than 3/4 inch in concrete joints. Fill unused holes. In partitions of light steel construction, use sheet metal screws. In suspended-ceiling construction, run conduit above ceiling. Do not support conduit by ceiling support system. Conduit and box systems: supported independently of both (a) tie wires supporting ceiling grid system, and (b) ceiling grid system into which ceiling panels are placed. Do not share supporting means between electrical raceways and mechanical piping or ducts. Identify independent conduit support in both fire and non-fire rated assemblies per NFPA 70. Coordinate installation with above-ceiling mechanical systems to assure maximum accessibility to all systems. Spring-steel fasteners may be used for lighting branch circuit conduit supports in suspended ceilings in dry locations. Support exposed risers in wire shafts of multistory buildings by U-clamp hangers at each floor level and at 10 foot maximum intervals. Where conduit crosses building expansion joints, provide suitable watertight expansion fitting that maintains conduit electrical continuity by bonding jumpers or other means. For conduits greater than 2 1/2 inches inside diameter, provide supports to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction.

3.1.4.12 Directional Changes in Conduit Runs

Make changes in direction of runs with symmetrical bends or cast-metal fittings. Make field-made bends and offsets with hickey or conduit-bending machine. Do not install crushed or deformed conduits. Avoid trapped conduits. Prevent plaster, dirt, or trash from lodging in conduits, boxes, fittings, and equipment during construction. Free clogged conduits of obstructions.

3.1.4.13 Locknuts and Bushings

Fasten conduits to sheet metal boxes and cabinets with two locknuts where required by NFPA 70, where insulated bushings are used, and where bushings cannot be brought into firm contact with the box; otherwise, use at least minimum single locknut and bushing. Provide locknuts with sharp edges for digging into wall of metal enclosures. Install bushings on ends of conduits, and provide insulating type where required by NFPA 70.

3.1.4.14 Flexible Connections

Provide flexible steel conduit between 3 and 6 feet in length for recessed and semirecessed lighting fixtures; for equipment subject to vibration, noise transmission, or movement; and for motors. Install flexible conduit to allow 20 percent slack. Minimum flexible steel conduit size: 1/2 inch diameter. Provide liquid tight flexible nonmetallic conduit in wet and damp locations and in fire pump rooms for equipment subject to vibration, noise transmission, movement or motors. Provide separate ground conductor across flexible connections. Plastic cable ties are not acceptable as a support method.

3.1.4.15 Telecommunications and Signal System Pathway

Install telecommunications pathway in accordance with TIA-569.

a. Horizontal Pathway: Telecommunications pathways from the work area to the telecommunications room: installed and cabling length requirements in accordance with TIA-568.1. Size conduits, wireways, and cable trays in accordance with TIA-569 and as indicated.

b. Backbone Pathway: Telecommunication pathways from the telecommunications entrance facility to telecommunications rooms, and, telecommunications equipment rooms (backbone cabling): installed in accordance with TIA-569. Size conduits, wireways, and cable trays for telecommunications risers in accordance with TIA-569 and as indicated.

3.1.4.16 Community Antenna Television (CATV) System Conduits

Install a system of CATV wire-supporting structures (pathway), including: outlet boxes, conduits with pull wires wireways, cable trays, and other accessories for CATV outlets and pathway in accordance with TIA-569..

3.1.5 Busway Installation

Comply at minimum with NFPA 70. Install busways parallel with or at right angles to ceilings, walls, and structural members. Support busways at 5 foot maximum intervals, and brace to prevent lateral movement. Provide fixed type hinges on risers; spring-type are unacceptable. Provide flanges where busway makes penetrations through walls and floors, and seal to maintain smoke and fire ratings. Provide waterproof curb where busway riser passes through floor. Seal gaps with fire-rated foam and caulk. Provide expansion joints, but only where bus duct crosses building expansion joints. Provide supports to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction.

3.1.6 Cable Tray Installation

Install and ground in accordance with NFPA 70. In addition, install and ground telecommunications cable tray in accordance with TIA-569, and TIA-607. Install cable trays parallel with or at right angles to ceilings, walls, and structural members. Cable tray and tray supports must not partially nor completely obstruct access to the room. Support in accordance with NEMA VE 2 and with manufacturer recommendations but at not more than 6 foot intervals. Coat contact surfaces of aluminum connections with an antioxidant compound prior to assembly. Adjacent cable tray sections: bonded together by connector plates of an identical type as the cable tray sections. For grounding of cable tray system provide No. 2 AWG bare copper wire throughout cable tray system, and bond to each section, except use No. 1/0 aluminum wire if cable tray is aluminum. Terminate cable trays 10 inches from both sides of smoke and fire partitions. Install conductors run through smoke and fire partitions in 4 inch rigid steel conduits with grounding bushings, extending 12 inches beyond each side of partitions. Seal conduit on both ends to maintain smoke and fire ratings of partitions. Firestop penetrations in accordance with Section 07 84 00, FIRESTOPPING. Provide supports to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction.

3.1.7 Telecommunications Cable Support Installation

Install open top and closed ring cable supports on 4 ft to 5 ft centers to adequately support and distribute the cable’s weight. Use these types of supports to support a maximum of 50 0.25 in diameter cables. Install suspended cables with at least 3 in of clear vertical space above the ceiling tiles and support channels (T-bars). Open top and closed ring cable supports: suspended from or attached to the structural ceiling or walls with hardware or other installation aids specifically designed to support their weight.

3.1.8 Boxes, Outlets, and Supports

Provide boxes in wiring and raceway systems wherever required for pulling of wires, making connections, and mounting of devices or fixtures. Boxes for metallic raceways: cast-metal, hub-type when located in wet locations, when surface mounted on outside of exterior surfaces, and when specifically indicated. Boxes in other locations: sheet steel, except that aluminum boxes may be used with aluminum conduit, and nonmetallic boxes may be used with nonmetallic sheathed cable conduit system. Provide each box with volume required by NFPA 70 for number of conductors enclosed in box. Boxes for mounting lighting fixtures: minimum 4 inches square, or octagonal, except that smaller boxes may be installed as required by fixture configurations, as approved. Boxes for use in masonry-block or tile walls: square-cornered, tile-type, or standard boxes having square-cornered, tile-type covers. Provide gaskets for cast-metal boxes installed in wet locations and boxes installed flush with outside of exterior surfaces. Provide separate boxes for flush or recessed fixtures when required by fixture terminal operating temperature; provide readily removable fixtures for access to boxes unless ceiling access panels are provided. Support boxes and pendants for surface-mounted fixtures on suspended ceilings independently of ceiling supports. Fasten boxes and supports with wood screws on wood, with bolts and expansion shields on concrete or brick, with toggle bolts on hollow masonry units, and with machine screws or welded studs on steel. Threaded studs driven in by powder charge and provided with lock washers and nuts or nail-type nylon

anchors may be used in lieu of wood screws, expansion shields, or machine screws. In open overhead spaces, cast boxes threaded to raceways need not be separately supported except where used for fixture support; support sheet metal boxes directly from building structure or by bar hangers. Where bar hangers are used, attach bar to raceways on opposite sides of box, and support raceway with approved-type fastener maximum 24 inches from box. When penetrating reinforced concrete members, avoid cutting reinforcing steel.

3.1.8.1 Boxes

Boxes for use with raceway systems: minimum 1 1/2 inches deep, except where shallower boxes required by structural conditions are approved. Boxes for other than lighting fixture outlets: minimum 4 inches square, except that 4 by 2 inch boxes may be used where only one raceway enters outlet.

3.1.8.1.1 Wall-Mounted Telecommunications Outlet Box

Provide double gang electrical boxes, minimum standard size 4-11/16 inches square and 2-1/8 inches deep with plaster ring for connection of single gang faceplate. Design outlet box for recess mounting with the faceplate flush with the wall surface, at the same height as the electrical outlets.

3.1.8.2 Pull Boxes

Construct of at least minimum size required by NFPA 70 of code-gauge aluminum or galvanized sheet steel, and compatible with nonmetallic raceway systems, except where cast-metal boxes are required in locations specified herein. Provide boxes with screw-fastened covers. Where several feeders pass through common pull box, tag feeders to indicate clearly electrical characteristics, circuit number, and panel designation.

3.1.8.3 Extension Rings

Extension rings are not permitted for new construction. Use only on existing boxes in concealed conduit systems where wall is furred out for new finish.

3.1.9 Mounting Heights

Mount panelboards, enclosed circuit breakers, motor controller and disconnecting switches so height of center of grip of the operating handle of the switch or circuit breaker at its highest position is maximum 79 inches above floor or working platform or as allowed in Section 404.8 per NFPA 70. Mount lighting switches and handicapped telecommunications stations 48 inches above finished floor. Mount receptacles and telecommunications outlets 18 inches above finished floor, unless otherwise indicated. Wall-mounted telecommunications outlets: mounted at height as indicated. Mount other devices as indicated. Measure mounting heights of wiring devices and outlets in non-hazardous areas to center of device or outlet. Measure mounting heights of receptacle outlet boxes in the hazardous area to the bottom of the outlet box.

3.1.10 Nonmetallic Sheathed Cable Installation

Where possible, install cables concealed behind ceiling or wall finish. Thread cables through holes bored on approximate centerline of wood members; notching of end surfaces is not permitted. Provide sleeves

through concrete or masonry for threading cables. Install exposed cables parallel to or at right angles to walls or structural members. Protect exposed nonmetallic sheathed cables less than 4 feet above floors from mechanical injury by installation in conduit or tubing. When cable is used in metal stud construction, insert plastic stud grommets in studs at each point through which cable passes, prior to installation of cable.

3.1.11 Mineral Insulated, Metal Sheathed (Type MI) Cable Installation

Mineral-insulated, metal-sheathed cable system, Type MI, may be used in lieu of exposed conduit and wiring. Conductor sizes: not less than those indicated for the conduit installation. Fasten cables within 12 inches of each turn or offset and at 33 inches maximum intervals. Make cable terminations in accordance with NFPA 70 and cable manufacturer's recommendations. Terminate single-conductor cables of a circuit, having capacities of more than 50 amperes, in a single box or cabinet opening. Color code individual conductors in all outlets and cabinets.

3.1.12 Conductor Identification

Provide conductor identification within each enclosure where tap, splice, or termination is made. For conductors No. 6 AWG and smaller diameter, provide color coding by factory-applied, color-impregnated insulation. For conductors No. 4 AWG and larger diameter, provide color coding by plastic-coated, self-sticking markers; colored nylon cable ties and plates; or heat shrink-type sleeves. Identify control circuit terminations in accordance with manufacturer's recommendations. Provide telecommunications system conductor identification as specified in Section 27 10 00 BUILDING TELECOMMUNICATIONS CABLING SYSTEMS.

3.1.12.1 Marking Strips

Provide marking strips for identification of power distribution, control, data, and communications cables in accordance with the following:

a. Provide white or other light-colored plastic marking strips, fastened by screws to each terminal block, for wire designations.

b. Use permanent ink for the wire numbers

c. Provide reversible marking strips to permit marking both sides, or provide two marking strips with each block.

d. Size marking strips to accommodate the two sets of wire numbers.

e. Assign a device designation in accordance with NEMA ICS 1 to each device to which a connection is made. Mark each device terminal to which a connection is made with a distinct terminal marking corresponding to the wire designation used on the Contractor's schematic and connection diagrams.

f. The wire (terminal point) designations used on the Contractor's wiring diagrams and printed on terminal block marking strips may be according to the Contractor's standard practice; however, provide additional wire and cable designations for identification of remote (external) circuits for the Government's wire designations.

g. Prints of the marking strips drawings submitted for approval will be so marked and returned to the Contractor for addition of the

designations to the terminal strips and tracings, along with any rearrangement of points required.

3.1.13 Splices

Make splices in accessible locations. Make splices in conductors No. 10 AWG and smaller diameter with insulated, pressure-type connector. Make splices in conductors No. 8 AWG and larger diameter with solderless connector, and cover with insulation material equivalent to conductor insulation.

3.1.13.1 Splices of Aluminum Conductors

Make with solderless circumferential compression-type, aluminum-bodied connectors UL listed for AL/CU. Remove surface oxides from aluminum conductors by wire brushing and immediately apply oxide-inhibiting joint compound and insert in connector. After joint is made, wipe away excess joint compound, and insulate splice.

3.1.14 Terminating Aluminum Conductors

3.1.14.1 Termination to Copper Bus

Terminate aluminum conductors to copper bus either by: (a) inline splicing a copper pigtail, of ampacity at least that of aluminum conductor, or (b) utilizing circumferential, compression-type, aluminum-bodied terminal lug UL listed for AL/CU, and steel Belleville cadmium-plated hardened steel spring washers, flat washers, bolts, and nuts. Carefully install Belleville spring washers with crown up toward nut or bolt head, with concave side of Belleville bearing on heavy-duty, wide series flat washer of larger diameter than Belleville. Tighten nuts sufficiently to flatten Belleville, and leave in position. Lubricate hardware with joint compound prior to making connection. Wire brush and apply joint compound to conductor prior to inserting in lug.

3.1.14.2 Termination to Aluminum Bus

Terminate aluminum conductors to aluminum bus by using aluminum nuts, bolts, washers, and compression lugs. Wire brush and apply joint compound to conductor prior to inserting in lug. Lubricate hardware with joint compound prior to making connection. When bus contact surface is unplated, scratch-brush and coat with joint compound, without grit.

3.1.15 Covers and Device Plates

Install with edges in continuous contact with finished wall surfaces without use of mats or similar devices. Plaster fillings are not permitted. Install plates with alignment tolerance of 1/16 inch. Use of sectional-type device plates are not permitted. Provide gasket for plates installed in wet locations.

3.1.16 Electrical Penetrations

Seal openings around electrical penetrations through fire resistance-rated walls, partitions, floors, or ceilings in accordance with Section 07 84 00 FIRESTOPPING.

3.1.17 Grounding and Bonding

Provide in accordance with NFPA 70 and NFPA 780. Ground exposed, non-current-carrying metallic parts of electrical equipment, metallic raceway systems, grounding conductor in metallic and nonmetallic raceways, telecommunications system grounds, grounding conductor of nonmetallic sheathed cables, and neutral conductor of wiring systems. Make ground connection at main service equipment, and extend grounding conductor to point of entrance of metallic water service. Make connection to water pipe by suitable ground clamp or lug connection to plugged tee. If flanged pipes are encountered, make connection with lug bolted to street side of flanged connection. Supplement metallic water service grounding system with additional made electrode in compliance with NFPA 70. Make ground connection to driven ground rods on exterior of building. Bond additional driven rods together with a minimum of 4 AWG soft bare copper wire buried to a depth of at least 12 inches. Interconnect all grounding media in or on the structure to provide a common ground potential. This includes lightning protection, electrical service, telecommunications system grounds, as well as underground metallic piping systems. Make interconnection to the gas line on the customer's side of the meter. Use main size lightning conductors for interconnecting these grounding systems to the lightning protection system. In addition to the requirements specified herein, provide telecommunications grounding in accordance with TIA-607. Where ground fault protection is employed, ensure that connection of ground and neutral does not interfere with correct operation of fault protection.

3.1.17.1 Ground Rods

Provide ground rods and measure the resistance to ground using the fall-of-potential method described in IEEE 81. Do not exceed 25 ohms under normally dry conditions for the maximum resistance of a driven ground. In high-ground-resistance, UL listed chemically charged ground rods may be used. If the resultant resistance exceeds 25 ohms measured not less than 48 hours after rainfall, notify the Contracting Officer who will decide on the number of ground rods to add.

3.1.17.2 Grounding Connections

Make grounding connections which are buried or otherwise normally inaccessible, excepting specifically those connections for which access for periodic testing is required, by exothermic weld or high compression connector.

a. Make exothermic welds strictly in accordance with the weld manufacturer's written recommendations. Welds which are "puffed up" or which show convex surfaces indicating improper cleaning are not acceptable. Mechanical connectors are not required at exothermic welds.

b. Make high compression connections using a hydraulic or electric compression tool to provide the correct circumferential pressure. Provide tools and dies as recommended by the manufacturer. Use an embossing die code or other standard method to provide visible indication that a connector has been adequately compressed on the ground wire.

3.1.17.3 Ground Bus

Provide a copper ground bus in the electrical equipment rooms as indicated. Noncurrent-carrying metal parts of transformer neutrals and other electrical equipment: effectively grounded by bonding to the ground bus. Bond the ground bus to both the entrance ground, and to a ground rod or rods as specified above having the upper ends terminating approximately 4 inches above the floor. Make connections and splices of the brazed, welded, bolted, or pressure-connector type, except use pressure connectors or bolted connections for connections to removable equipment. For raised floor equipment rooms in computer and data processing centers, provide a minimum of four, one at each corner, ground buses connected to the building grounding system. Use bolted connections in lieu of thermoweld, so they can be changed as required by additions and alterations.

3.1.17.4 Resistance

Maximum resistance-to-ground of grounding system: do not exceed 25 ohms under dry conditions. Where resistance obtained exceeds 25 ohms, contact Contracting Officer for further instructions.

3.1.17.5 Telecommunications System

Provide telecommunications grounding in accordance with the following:

a. Telecommunications Grounding Busbars: Provide a Primary bonding busbar (PBB) in the telecommunications entrance facility. Install the PBB as close to the electrical service entrance grounding connection as practicable. Provide a Secondary bonding busbar (SBB) in all other telecommunications rooms and telecommunications equipment rooms. Install the SBB as close to the telecommunications room panelboard as practicable, when equipped. Where a panelboard for telecommunications equipment is not installed in the telecommunications room, locate the SBB near the backbone cabling and associated terminations. In addition, locate the SBB to provide for the shortest and straightest routing of the grounding conductors. Where a panelboard for telecommunications equipment is located within the same room or space as a SBB, bond that panelboard's alternating current equipment ground (ACEG) bus (when equipped) or the panelboard enclosure to the SBB. Install Secondary bonding busbars to maintain clearances as required by NFPA 70 and insulated from its support. A minimum of 2 inches separation from the wall is recommended to allow access to the rear of the busbar and adjust the mounting height to accommodate overhead or underfloor cable routing.

b. Telecommunications Bonding Conductors: Provide main telecommunications service equipment ground consisting of separate bonding conductor for telecommunications, between the PBB and readily accessible grounding connection of the electrical service. Grounding and bonding conductors should not be placed in ferrous metallic conduit. If it is necessary to place grounding and bonding conductors in ferrous metallic conduit that exceeds 3 feet in length, bond the conductors to each end of the conduit using a grounding bushing or a No. 6 AWG conductor, minimum.

c. Telecommunications Grounding Connections: Telecommunications grounding connections to the PBB or SBB: utilize listed compression two-hole lugs, exothermic welding, suitable and equivalent one hole non-twisting lugs, or other irreversible compression type

connections. Bond all metallic pathways, cabinets, and racks for telecommunications cabling and interconnecting hardware located within the same room or space as the PBB or SBB to the PBB or SBB respectively. In a metal frame (structural steel) building, where the steel framework is readily accessible within the room; bond each PBB to the vertical steel metal frame using a minimum No. 6 AWG conductor. Where the metal frame is external to the room and readily accessible, bond the metal frame to the SBB or PBB with a minimum No. 6 AWG conductor. When practicable because of shorter distances and, where horizontal steel members are permanently electrically bonded to vertical column members, the SBB may be bonded to these horizontal members in lieu of the vertical column members. All connectors used for bonding to the metal frame of a building must be listed for the intended purpose.

3.1.18 Equipment Connections

Provide power wiring for the connection of motors and control equipment under this section of the specification. Except as otherwise specifically noted or specified, automatic control wiring, control devices, and protective devices within the control circuitry are not included in this section of the specifications and are provided under the section specifying the associated equipment.

3.1.19 Elevator

Provide circuit to line terminals of elevator controller, and disconnect switch on line side of controller, outlet for control power, outlet receptacle and work light at midheight of elevator shaft, and work light and outlet receptacle in elevator pit.

3.1.20 Government-Furnished Equipment

Contractor make connections to Government-furnished equipment to make equipment operate as intended, including providing miscellaneous items such as plugs, receptacles, wire, cable, conduit, flexible conduit, and outlet boxes or fittings.

3.1.21 Watthour Meters

ANSI C12.1.

3.1.22 Surge Protective Devices

Connect the surge protective devices in parallel to the power source, keeping the conductors as short and straight as practically possible. Maximum allowed lead length is 3 feet avoiding 90 degree bends. Do not locate surge protective devices inside a panelboard or switchboard enclosure.

3.2 FIELD FABRICATED NAMEPLATE MOUNTING

Provide number, location, and letter designation of nameplates as indicated. Fasten nameplates to the device with a minimum of two sheet-metal screws or two rivets. Provide nameplate on all equipment in access controlled spaces and areas.

3.3 WARNING SIGN MOUNTING

Provide the number of signs required to be readable from each accessible

side. Space the signs in accordance with NFPA 70E.

3.4 FIELD APPLIED PAINTING

Paint electrical equipment as required to match finish of adjacent surfaces or to meet the indicated or specified safety criteria. Painting: as specified in Section 09 90 00 PAINTS AND COATINGS.

3.5 FIELD QUALITY CONTROL

Furnish test equipment and personnel and submit written copies of test results. Give Contracting Officer 5 working days notice prior to each test. Where applicable, test electrical equipment in accordance with NETA ATS.

3.5.1 Devices Subject to Manual Operation

Operate each device subject to manual operation at least five times, demonstrating satisfactory operation each time.

3.5.2 600-Volt Wiring Test

Test wiring rated 600 volt and less to verify that no short circuits or accidental grounds exist. Perform insulation resistance tests on wiring No. 6 AWG and larger diameter using instrument which applies voltage of 1,000 volts DC for 600 volt rated wiring and 500 volts DC for 300 volt rated wiring per NETA ATS to provide direct reading of resistance. All existing wiring to be reused must also be tested.

3.5.3 Transformer Tests

Perform the standard, not optional, tests in accordance with the Inspection and Test Procedures for transformers, dry type, air-cooled, 600 volt and below; as specified in NETA ATS. Measure primary and secondary voltages for proper tap settings. Tests need not be performed by a recognized independent testing firm or independent electrical consulting firm.

3.5.4 Ground-Fault Receptacle Test

Test ground-fault receptacles with a "load" (such as a plug in light) to verify that the "line" and "load" leads are not reversed. Press the TEST button and then the RESET button to verify by LED status that the device is a self-test model as specified in UL 943.

3.5.5 Grounding System Test

Test grounding system to ensure continuity, and that resistance to ground is not excessive. Test each ground rod for resistance to ground before making connections to rod; tie grounding system together and test for resistance to ground. Make resistance measurements in dry weather, not earlier than 48 hours after rainfall. Submit written results of each test to Contracting Officer, and indicate location of rods as well as resistance and soil conditions at time measurements were made.

3.5.6 Watthour Meter

a. Visual and mechanical inspection

(1) Examine for broken parts, shipping damage, and tightness of

connections.

(2) Verify that meter type, scales, and connections are in accordance with approved shop drawings.

b. Electrical tests

(1) Determine accuracy of meter.

(2) Calibrate watthour meters to one-half percent.

(3) Verify that correct multiplier has been placed on face of meter, where applicable.

3.5.7 Phase Rotation Test

Perform phase rotation test to ensure proper rotation of service power prior to operation of new or reinstalled equipment using a phase rotation meter. Follow the meter manual directions performing the test.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 26 - ELECTRICAL

SECTION 26 24 16.00 40

PANELBOARDS

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 QUALITY CONTROL
1.3.1 Regulatory Requirements
1.3.2 Standard Products

PART 2 PRODUCTS

2.1 PANELBOARDS
2.2 COMPONENTS
2.2.1 Enclosure
2.2.2 Panelboard Buses
2.2.2.1 Panelboard Neutrals for Non-Linear Loads
2.2.3 Circuit Breakers
2.2.3.1 Multipole Breakers
2.2.3.2 Circuit Breaker With Ground-Fault Circuit Interrupter
2.2.3.3 Circuit Breakers for HVAC Equipment
2.2.3.4 Arc-Fault Circuit Interrupters
2.2.4 Directory Card and Holder
2.2.5 Filtered Panelboards
2.2.5.1 General
2.2.5.2 RF Shielding
2.2.5.3 Circuit Breaker Actuators
2.2.5.4 Terminals
2.2.5.5 Attenuation
2.2.5.6 Current
2.2.5.7 Voltage
2.2.5.8 Circuit Breakers
2.2.5.9 RF Filters
2.2.5.10 Filter Discharge Unit
2.2.6 Surge Protective Devices
2.2.7 Precautionary Label
2.3 TESTS, INSPECTIONS, AND VERIFICATIONS

PART 3 EXECUTION

3.1 INSTALLATION
3.2 FIELD QUALITY CONTROL
3.3 CLOSEOUT ACTIVITIES

-- End of Section Table of Contents --

SECTION 26 24 16.00 40

PANELBOARDS

PART 1 GENERAL

Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM applies to work specified in this section.

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ASTM INTERNATIONAL (ASTM)

ASTM D1535	(2014; R 2018) Standard Practice for Specifying Color by the Munsell System

ELECTRONIC COMPONENTS INDUSTRY ASSOCIATION (ECIA)

ECIA RS-416	(1974; R 1981) Filters for Radio Interference
ECIA/IS 46	(1987) Test Procedure for Resistance to Soldering (Vapor Phase Technique) for Surface Mount Devices

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE C2	(2023) National Electrical Safety Code

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA 250	(2020) Enclosures for Electrical Equipment (1000 Volts Maximum)
NEMA AB 3	(2013) Molded Case Circuit Breakers and Their Application
NEMA ICS 6	(1993; R 2016) Industrial Control and Systems: Enclosures
NEMA PB 1	(2011) Panelboards

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National Electrical Code
NFPA 70E	(2021) Standard for Electrical Safety in the Workplace

U.S. DEPARTMENT OF DEFENSE (DOD)

MIL-HDBK 232	(1987; Rev A; Notice 1 1988; Notice 2 2000; Notice 3 2014) Red/Black Engineering - Installation Guidelines

U.S. GENERAL SERVICES ADMINISTRATION (GSA)

FED-STD-595	(Rev C; Notice 1) Colors Used in Government Procurement

UNDERWRITERS LABORATORIES (UL)

UL 50	(2015) UL Standard for Safety Enclosures for Electrical Equipment, Non-Environmental Considerations
UL 67	(2018; Reprint Jul 2020) UL Standard for Safety Panelboards
UL 489	(2016; Rev 2019) UL Standard for Safety Molded-Case Circuit Breakers, Molded-Case Switches and Circuit-Breaker Enclosures
UL 869A	(2006; Reprint Jun 2020) Reference Standard for Service Equipment
UL 943	(2016; Reprint Feb 2018) UL Standard for Safety Ground-Fault Circuit-Interrupters
UL 1449	(2021) UL Standard for Safety Surge Protective Devices
UL 1699	(2017; Reprint Feb 2022) UL Standard for Safety Arc-Fault Circuit-Interrupters

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-03 Product Data

Panelboards; G

Filtered Panelboards; G

SD-06 Test Reports

Acceptance Tests; G

SD-08 Manufacturer's Instructions

Manufacturer's Instructions

1.3 QUALITY CONTROL

1.3.1 Regulatory Requirements

In each of the publications referred to herein, consider the advisory provisions to be mandatory, as though the word, "shall" had been substituted for "should" wherever it appears. Interpret references in these publications to the "authority having jurisdiction," or words of similar meaning, to mean the Contracting Officer. Ensure equipment, materials, installation, and workmanship are in accordance with the mandatory and advisory provisions of NFPA 70, IEEE C2 unless more stringent requirements are specified or indicated.

1.3.2 Standard Products

Provide materials and equipment that are products of manufacturers regularly engaged in the production of such products which are of equal material, design and workmanship. Provide products which have been in satisfactory commercial or industrial use for 2 years prior to bid opening. Ensure the 2-year period includes applications of equipment and materials under similar circumstances and of similar size. Ensure the product has been on sale on the commercial market through advertisements, manufacturers' catalogs, or brochures during the 2-year period. Where two or more items of the same class of equipment are required, these items must be products of a single manufacturer.

Products manufactured more than 3 years prior to date of delivery to site are not to be used, unless specified otherwise.

PART 2 PRODUCTS

2.1 PANELBOARDS

Provide panelboards in accordance with NEMA PB 1, UL 67, and UL 50. Ensure panelboards for use as service equipment are also in accordance with UL 869A. Ensure panelboards have current rating, number of phases, and number of wires as indicated or specified herein. Ensure panelboards are rated for 120/208-volt, three-phase or 277/480-volt, three-phase, 60-hertz. Ensure each panelboard, as a complete unit, has a short-circuit current rating equal to or greater than the integrated equipment rating indicated, but in no case less than 10,000 amperes symmetrical.

Provide panelboards with bolt-on circuit breakers only. Use of plug-in style breaker is not permitted. Ensure panelboards are designed such that individual breakers can be removed without disturbing adjacent units or without loosening or removing supplemental insulation supplied as means of obtaining required clearance. Provide main lugs or main circuit breakers mounted "above" branch breakers with current ratings as indicated. Use of sub-feed breakers is not acceptable unless specifically indicated otherwise. Where "space only" is indicated, make provisions for future installation of breakers.

Submit detail drawings and manufacturer's standard product data for panelboards. Detail drawings consist of fabrication and assembly drawings for all parts of the work in sufficient detail to verify conformity with all requirements. Ensure drawings for panelboards indicate details of bus layout, overall physical features, dimensions, ratings, service requirements, and weights of equipment.

2.2 COMPONENTS

2.2.1 Enclosure

Ensure panelboard enclosures are NEMA 250, Type 1 as indicated and in accordance with UL 50 and NEMA PB 1.

Provide flush-mounted panelboard cabinets as indicated. Ensure cabinets are constructed of 12 gauge sheet steel and hot-dipped galvanized after fabrication. Ensure front of cabinet is form-flanged or fitted with structural shapes welded or riveted to the sheet steel for supporting the panelboard front. Provide panelboard cabinets fabricated such that no part of any surface on the finished cabinet deviates from a true plane by more than 1/8 inch. Provide holes in the back of indoor surface-mounted cabinets, with outside spacers and inside stiffeners, for mounting the cabinets with a 1/2 inch clear space between the back of the cabinet and the wall surface.

Provide front cover with center door for access to circuit breakers. Provide side gutters in enclosure measuring minimum 5.75 inches for routing of wiring. Where panelboards are installed flush with the walls, ensure that the hinged front can be opened without damage to the adjacent wall surfaces. Ensure circuit breaker access doors are equipped with pin-tumbler cylinder locks. Ensure all locks provided, including locks for hinged covers, are identically keyed and properly tagged. Provide two keys for each enclosure.

Finish panelboards with baked enamel. Finish color is ASTM D1535 No. 61 gray conforming to FED-STD-595.

2.2.2 Panelboard Buses

Provide copper buses of the rating indicated, with main lugs or main circuit breaker. Provide all panelboards for use on grounded ac systems with a separate grounding bus in accordance with UL 67 bonded to the panelboard enclosure. Ensure grounding bus is a solid bus bar of rectangular cross section equipped with binding screws for the connection of equipment grounding conductors. In addition to equipment grounding bus, provide second "isolated" ground bus, where indicated. Provide three-phase, four-wire and single-phase, three-wire panelboards with an isolated full-capacity bus providing spaces for single-pole circuit breaker switches and spaces indicated as spare.

Provide bus bar connections to the branch circuit breakers that are the "distributed phase" or "phase sequence" type. Ensure single-phase, three-wire panelboard busing is such that when any two adjacent single-pole breakers are connected to opposite phases, two-pole breakers can be installed in any location. Ensure that three-phase, four-wire panelboard busing is such that when any three adjacent single-pole breakers are individually connected to each of the three different phases, two- or three-pole breakers can be installed at any location. Ensure current-carrying parts of the bus assembly are plated.

Support bus bars on bases independent of circuit breakers. Design main buses and back pans so that breakers may be changed without machining, drilling, or tapping.

2.2.2.1 Panelboard Neutrals for Non-Linear Loads

Where indicated, provide panelboard specifically listed for use on non-linear loads. Ensure panelboards are heat rise tested in accordance with UL 67, except with the neutral assembly installed and carrying 200 percent of the phase bus current during testing. Two neutral assemblies paralleled together with cable is not acceptable. Ensure panel is marked "SUITABLE FOR NON-LINEAR LOADS" with field fabricated nameplate and provide a neutral label with instructions for wiring of panelboard.

2.2.3 Circuit Breakers

Provide circuit breakers that conform to UL 489 and NEMA AB 3 and as specified in Section 26 05 71.00 40 LOW VOLTAGE OVERCORRECT PROTECTIVE DEVICES with frame a trip ratings as indicated.

Provide bolt-on type, molded-case, manually operated, trip-free circuit breakers, with inverse-time thermal-overload protection and instantaneous magnetic short-circuit protection. Completely enclose circuit breakers in a molded case, with a factory-sealed, calibrated sensing element to prevent tampering. Plug-in type, tandem, and half-size circuit breakers are not permitted.

Provide sufficient interrupting capacity of the panel and lighting branch circuit breakers to successfully interrupt the maximum short-circuit current imposed on the circuit at the breaker terminals. Provide circuit breaker interrupting capacities with a minimum of 10,000 A and that conform to NEMA AB 3. Series rating of circuit breakers or overcurrent protective devices to achieve indicated interrupt rating is not permitted.

Provide the common-trip-type multipole circuit breakers having a single operating handle and a two-position on/off indication. Provide circuit breakers with temperature compensation for operation in an ambient temperature of 104 degrees F. Provide circuit breakers that have root mean square (rms) symmetrical interrupting ratings sufficient to protect the circuit being supplied. Interrupting ratings may have selective-type tripping (time delay, magnetic, thermal, or ground fault).

Provide a phenolic-composition breaker body capable of having such accessories as handle-extension, handle-locking, and padlocking devices attached where required to meet lock-out/tag-out requirements of NFPA 70E.

Provide shunt trips where indicated.

When multiple wires per phase are specified, furnish the circuit breakers with connectors made to accommodate multiple wires.

Ensure circuit breaker spaces called out on the drawings are complete with mounting hardware to permit ready installation of the circuit breakers.

2.2.3.1 Multipole Breakers

Provide common trip-type with single operating handle. Design breaker such that overload in one pole automatically causes all poles to open. Maintain phase sequence throughout each panel so that any three adjacent breaker poles are connected to Phases A, B, and C, respectively.

2.2.3.2 Circuit Breaker With Ground-Fault Circuit Interrupter

UL 943 and NFPA 70. Provide with "push-to-test" button, visible indication of tripped condition, and ability to detect and trip on current imbalance of 6 milliamperes or greater per requirements of UL 943 for Class A ground-fault circuit interrupter. Tripping of a branch circuit breaker containing ground fault circuit interruption is not to disturb the feeder circuit to the panelboard.

2.2.3.3 Circuit Breakers for HVAC Equipment

Provide circuit breakers for HVAC equipment having motors (group or individual) marked for use with HACR type and UL listed as HACR type.

2.2.3.4 Arc-Fault Circuit Interrupters

UL 489, UL 1699 and NFPA 70. Molded case circuit breakers: rated as indicated. Two pole arc-fault circuit-interrupters: rated 120/240 volts. Provide with "push-to-test" button.

2.2.4 Directory Card and Holder

Provide a directory card on the inside of hinged fronts and doors in a metal frame, with spaces for circuit numbers and load supplied. Where hinged fronts or doors are not required, provide the directory card in a metal frame mounted on the left-hand side of the front trim. Ensure the directory card includes type written designations identifying each branch circuit with its respective and numbered circuit breaker.

2.2.5 Filtered Panelboards

2.2.5.1 General

Design panelboards for the distribution, control, and protection of electrical circuits, providing filtering and shielding performance and, when specified, conforming to MIL-HDBK 232.

Provide panelboard cabinet with 12-gauge steel minimum, corrosion-resistant finish and four external mounting brackets welded to the case. Provide code-gauge steel front door and trim, with ASTM D1535 No. 61 gray finish, equipped with directory, holder, adjustable trim clamps, hinges, self-latching catch, tumbler lock and key and bears the UL label. Provide a red diagonal strip across the outside surface of door and trim.

2.2.5.2 RF Shielding

Ensure circuit breaker and filter compartments are completely radio-frequency (RF) shielded and in compliance with specified shielding requirements with front door open. Ensure case seams are continuous inert gas welded. Fit removable circuit breaker actuator faceplate and the filter compartment cover with corrosion-resistant RF gasketing material. Install in place with suitable fasteners having a maximum spacing of 3 inches on center. Mount RF filter units to the internal shield wall with similar RF gasketing to ensure RF shielding integrity.

2.2.5.3 Circuit Breaker Actuators

Design circuit breaker operating mechanisms to maintain RF shielding

effectiveness without limit to time or number of operations.

2.2.5.4 Terminals

Ensure filter terminals are high-temperature alumina ceramic, continuously brazed to filter case. Do not use soft solder. Provide ceramic terminals that incorporate a permanently attached flexible lead, with a suitable electric lug. Make incoming service connections to the filter lead at a UL-approved, flame-retardant standoff insulator, mounted in the filter compartment.

2.2.5.5 Attenuation

Ensure each filter provides a minimum insertion loss of 100 dB over the frequency range of 14 kilohertz (kHz) to 10 gigahertz (GHz) . Ensure each filter provides a full rated load insertion loss of 100 dB in the frequency range 14 kHz to 20 megahertz (MHz), to 14 kHz as measured by a Government-approved laboratory.

2.2.5.6 Current

Ensure each filter unit is capable of carrying its full rated current continuously without heat rise exceeding 122 degrees F above ambient temperature. Ensure each filter is capable of withstanding a 100 -percent overload for 30 seconds without damage.

2.2.5.7 Voltage

Ensure each filter unit is capable of continuous operation at its full rated voltage and withstanding an initial voltage test of twice its rated voltage without damage.

2.2.5.8 Circuit Breakers

Ensure circuit breakers are rated a minimum 10,000 amperes asymmetrical ac interrupting capacity, 5,000 amperes dc, and are in accordance with UL 489.

2.2.5.9 RF Filters

Design RF filter units to suppress and reduce the amplitude of undesired RF energy conducted by power service lines. Design RF filter units in compliance with the applicable requirements of ECIA RS-416.

Provide filter cases made of steel, 16-gaugeminimum, corrosion-resistant finish with a blue lacquer over zinc chromate primer. Use conductive grounding surfaces that are either plated or made of corrosion-resistant steel. Use continuous inert gas welds for hermetic seams; do not use soft solder. Firmly mount internal components to withstand applicable shock and vibration test requirements without damage.

Ensure internal components are fully impregnated and immersed in the fluid to obtain the full benefit of cooling by convection flow through the liquid medium to filter case. Completely fill filter case with the fluid. Ensure fluid conforms to UL nonflammable classification.

2.2.5.10 Filter Discharge Unit

Provide a filter discharge unit for three-filtered circuits on the panelboard. Install in accordance with NFPA 70. Ensure unit meets

applicable requirements of ECIA/IS 46

2.2.6 Surge Protective Devices

Provide parallel type surge protective devices (SPD) which comply with UL 1449 at the service entrance and panelboards. Provide surge protectors in a NEMA 1 enclosure per NEMA ICS 6. Use Type 1 or Type 2 SPD and connect on the load side of a dedicated circuit breaker. Ensure SPDs are of the Metal Oxide Varistor (MOV) type and rated have fault current rating equal to or greater than the rating of the device to be protected. Where internal fuses are used, ensure fuses will allow maximum rated surge to pass without operating fuse.

Provide SPDs that are factory installed and integrated with the equipment to be protected. Ensure factory installed SPDs are supplied through a dedicated circuit breaker or are directly connected to the bus with no wire between bus bare and SPD.

Provide the following modes of protection:

FOR SINGLE PHASE AND THREE PHASE WYE CONNECTED SYSTEMS-
Phase to phase (L-L)
Each phase to neutral (L-N)
Neutral to ground (N-G)
Phase to ground (L-G)

SPDs at the service entrance: provide with a minimum surge current rating of 80,000 amperes for L-L mode minimum and 40,000 amperes for other modes (L-N, L-G, and N-G) and downstream SPDs rated 40,000 amperes for L-L mode minimum and 20,000 amperes for other modes (L-N, L-G, and N-G).

Provide SPDs per NFPA 780 for the lightning protection system.

Maximum L-N, L-G, and N-G Voltage Protection Rating:

600V for 120V, single phase system
600V for 120/240V, single phase system
600V for 208Y/120V, three phase system
1,200V for 480Y/277V, three phase system

Maximum L-L Voltage Protection Rating:

1,200V for 120V, single phase system
1,200V for 208Y/120V, three phase system
1,200V for 480Y/277V, three phase system

The minimum MCOV (Maximum Continuous Operating Voltage) rating for L-N and L-G modes of operation: 120% of nominal voltage for 240 volts and below; 115% of nominal voltage above 240 volts to 480 volts.

Provide EMI/RFI filtering when required by project documents.

2.2.7 Precautionary Label

To ensure persons are aware of immediate or potential hazard in the application, installation, use, or maintenance of panelboards, conspicuously mark each panelboard on the trim or dead front shield with the text (or equivalent) **DANGER** symbol. If the panel is supplied with a door, ensure the label is visible when the door is in the open position.

2.3 TESTS, INSPECTIONS, AND VERIFICATIONS

Provide panelboards in compliance with UL 67.

PART 3 EXECUTION

3.1 INSTALLATION

Install panelboards in accordance with the manufacturer's instructions. Fully align and mount panels so that the height of the top operating handle does not exceed 72inches above the finished floor.

Ensure directory-card information is typewritten in capital letters to indicate loads served by each circuit and is mounted in holders behind protective covering.

3.2 FIELD QUALITY CONTROL

Do not energize panelboards until the recorded test data has been submitted to and approved by the Contracting Officer.

Provide test equipment, labor, and personnel as required to perform the acceptance tests as specified. Record and submit test data. Include the location and identification of panelboards and megohm readings versus time.

Conduct continuity tests using a dc device with bell . Document results as pass-fail.

Conduct continuity and insulation tests on the panelboards after the installation has been completed and before the panelboard is energized. Document results as pass-fail.

Conduct insulation tests on 480-volt panelboards using a 1,000-volt insulation-resistance test set. Record readings every minute until three equal and consecutive readings have been obtained. Ensure resistance between phase conductors and between phase conductors and ground is not less than 50 megohms.

Conduct insulation tests on panelboards rated 300 volts or less using a 500-volt minimum insulation-resistance test set. Record readings after 1 minute and until the reading is constant for 15 seconds. Ensure resistance between phase conductors and between phase conductors and ground is not less than 25 megohms.

Conduct phase-rotation tests on all panelboards using a phase-rotation indicating instrument. Perform phase rotation of electrical connections to connected equipment in a clockwise direction, facing the source.

3.3 CLOSEOUT ACTIVITIES

Submit manufacturer's instructions for panelboards including special provisions required to install equipment components and system packages. Provide special notices details impedances, hazards and safety precautions.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 26 - ELECTRICAL

SECTION 26 32 15.00

ENGINE-GENERATOR SET STATIONARY 15-2500 KW, WITH AUXILIARIES

PART 1 GENERAL

1.1 REFERENCES
1.2 RELATED MATERIALS
1.3 SUBMITTALS
1.4 QUALITY ASSURANCE
1.4.1 Conformance to Codes and Standards
1.4.2 Site Welding
1.4.3 Vibration Limitation
1.4.4 Torsional Analysis
1.4.5 Performance Data
1.4.6 Experience
1.4.7 Field Engineer
1.4.8 Detailed Drawings
1.4.9 Auxiliary Systems Engine-Generator Set and Auxiliary Equipment Drawing Requirements
1.4.10 Auxiliary Systems Drawing Requirements
1.4.11 Vibration Isolation System Certification
1.4.12 Fuel System Certification
1.5 DELIVERY, STORAGE, AND HANDLING
1.6 EXTRA MATERIALS
1.7 MAINTENANCE SERVICES
1.7.1 Operation Manual
1.7.2 Maintenance Manual
1.7.3 Assembled Operation and Maintenance Manuals

PART 2 PRODUCTS

2.1 SYSTEM REQUIREMENTS
2.1.1 Engine-Generator Parameter Schedule
2.1.2 Rated Output Capacity
2.1.2.1 Engine Emission Limits
2.1.2.2 Performance Class
2.1.3 Power Ratings
2.1.4 Transient Response
2.1.5 Reliability and Durability
2.1.6 Engine-Generator Set Enclosure
2.1.7 Vibration Isolation
2.1.8 Harmonic Requirements
2.1.9 Starting Time Requirements
2.2 NAMEPLATES
2.2.1 Materials
2.2.2 Control Devices and Operation Indicators
2.2.3 Equipment
2.3 SAFETY DEVICES
2.4 MATERIALS AND EQUIPMENT

2.4.1 Circuit Breakers, Low Voltage
2.4.2 Filter Elements
2.4.3 Instrument Transformers
2.4.4 Revenue Metering
2.4.5 Pipe (Fuel/Lube-Oil, Compressed Air, Coolant, and Exhaust)
2.4.5.1 Flanges and Flanged Fittings
2.4.5.2 Pipe Welding Fittings
2.4.5.3 Threaded Fittings
2.4.5.4 Valves
2.4.5.5 Gaskets
2.4.6 Pipe Hangers
2.4.7 Electrical Enclosures
2.4.7.1 Switchboards
2.4.7.2 Panelboards
2.4.8 Electric Motors
2.4.9 Motor Controllers
2.5 ENGINE
2.5.1 Sub-base Mounting
2.5.2 Assembly
2.5.3 Turbocharger
2.5.4 Intercooler
2.5.5 Crankcase Protection
2.5.6 Miscellaneous Engine Accessories
2.5.7 Intercooler
2.6 FUEL SYSTEM
2.6.1 Pumps
2.6.1.1 Main Pump
2.6.1.2 Auxiliary Fuel Pump
2.6.2 Fuel Filter
2.6.3 Relief/Bypass Valve
2.6.4 Integral Main Fuel Storage Tank
2.6.4.1 Fuel Transfer Pump
2.6.4.2 Capacity
2.6.4.3 Local Fuel Fill
2.6.4.4 Fuel Level Controls
2.6.4.5 Arrangement
2.6.5 Day Tank
2.6.5.1 Capacity, Prime
2.6.5.2 Capacity, Standby
2.6.5.3 Drain Line
2.6.5.4 Local Fuel Fill
2.6.5.5 Fuel Level Controls
2.6.5.6 Fuel Oil Solenoid Valve
2.6.5.7 Arrangement
2.6.6 Fuel Oil Cooler
2.7 LUBRICATION
2.7.1 Lube-Oil Filter
2.7.2 Lube-Oil Sensors
2.7.3 Precirculation Pump
2.8 COOLING SYSTEM
2.8.1 Coolant Pumps
2.8.2 Heat Exchanger
2.8.2.1 Fin-Tube-Type Heat Exchanger (Radiator)
2.8.2.2 Shell and U-Tube Type Heat Exchanger
2.8.3 Expansion Tank
2.8.4 Thermostatic Control Valve
2.8.5 Ductwork
2.8.6 Temperature Sensors
2.9 SOUND LIMITATIONS

2.10 AIR INTAKE EQUIPMENT
2.11 EXHAUST SYSTEM
2.11.1 Flexible Sections and Expansion Joints
2.11.2 Exhaust Muffler
2.11.3 Exhaust Piping
2.12 PYROMETER
2.13 EMISSIONS
2.14 STARTING SYSTEM
2.14.1 Controls
2.14.2 Capacity
2.14.3 Electrical Starting
2.14.3.1 Battery
2.14.3.2 Battery Charger
2.14.4 Storage Batteries
2.14.5 Starting Aids
2.14.5.1 Glow Plugs
2.14.5.2 Jacket-Coolant Heaters
2.14.5.2.1 Prime Rated Sets
2.14.5.2.2 Standby Rated Sets
2.14.5.3 Lubricating-Oil Heaters
2.15 GOVERNOR
2.16 GENERATOR
2.16.1 Current Balance
2.16.2 Voltage Balance
2.16.3 Waveform
2.17 EXCITER
2.17.1 Electromagnetic Interference (EMI) Suppression
2.18 VOLTAGE REGULATOR
2.19 GENERATOR ISOLATION AND PROTECTION
2.19.1 Switchboards
2.19.2 Devices
2.20 SAFETY SYSTEM
2.20.1 Audible Signal
2.20.2 Visual Signal
2.20.3 Alarms and Action Logic
2.20.3.1 Shutdown
2.20.3.2 Problem
2.20.4 Safety Indications and Shutdowns
2.20.5 Time-Delay on Alarms
2.21 SYNCHRONIZING PANEL
2.22 PANELS
2.22.1 Enclosures
2.22.2 Analog
2.22.3 Electronic
2.22.4 Parameter Display
2.23 SURGE PROTECTION
2.24 MANUAL ENGINE-GENERATOR-SET SYSTEM OPERATION
2.25 STATION BATTERY SYSTEM
2.25.1 Battery Charger
2.26 BASE
2.27 THERMAL INSULATION
2.28 PAINTING AND FINISHING
2.29 FACTORY INSPECTION AND TESTS
2.29.1 Factory Inspection
2.29.2 Factory Tests

PART 3 EXECUTION

3.1 EXAMINATION

3.2 GENERAL INSTALLATION
3.3 PIPING INSTALLATION
3.3.1 Support
3.3.1.1 Ceiling and Roof
3.3.1.2 Wall
3.3.2 Flanged Joints
3.3.3 Cleaning
3.3.4 Pipe Sleeves
3.4 ELECTRICAL INSTALLATION
3.5 FIELD PAINTING
3.6 ONSITE INSPECTION AND TESTS
3.6.1 Test Conditions
3.6.1.1 Data
3.6.1.2 Power Factor
3.6.1.3 Contractor Supplied Items
3.6.1.4 Instruments
3.6.1.5 Sequence
3.6.2 Construction Tests
3.6.2.1 Piping Test
3.6.2.2 Electrical Equipment Tests
3.6.3 Inspections
3.6.4 Engine Tests
3.6.5 Generator Tests
3.6.5.1 Routine Tests
3.6.5.2 Design Tests
3.6.6 Assembled Engine-Generator Set Tests
3.6.6.1 Initial Stabilization Readings
3.6.6.2 Regulator Range Test
3.6.6.3 Frequency Range Test
3.6.6.4 Transient Response Test
3.6.7 Pre-operational Tests
3.6.7.1 Protective Relays
3.6.7.2 Insulation Test
3.6.7.3 Engine-Generator Connection Coupling Test
3.6.8 Safety Run Test
3.6.9 Performance Tests
3.6.9.1 Continuous Engine Load Run Test
3.6.9.2 Voltage and Frequency Droop Test
3.6.9.3 Voltage Regulator Range Test
3.6.9.4 Governor Adjustment Range Test
3.6.9.5 Frequency and Voltage Stability and Transient Response
3.6.10 Parallel Operation Test
3.6.10.1 Combinations
3.6.10.2 Multiple Combinations
3.6.11 Parallel Operation Test (Commercial Source)
3.6.12 Automatic Operation Tests
3.6.13 Automatic Operation Tests for Stand-Alone Operation
3.7 GROUNDING
3.7.1 Grounding Electrodes
3.7.2 Engine-Generator Set Grounding
3.7.3 Connections
3.7.4 Grounding and Bonding Equipment
3.8 START-UP ENGINEER
3.9 PREREQUISITES FOR FUNCTIONAL ACCEPTANCE TESTING
3.9.1 Generator Sets
3.9.2 Preliminary Operations
3.9.3 Preliminary Assembled Operation and Maintenance Manuals
3.9.4 Functional Acceptance Test Procedure
3.9.5 Test Equipment

3.10 FIELD QUALITY CONTROL
3.10.1 Acceptance Checks and Tests
3.10.1.1 Circuit Breakers - Low Voltage Insulated Case/Molded Case
3.10.1.2 Current Transformers
3.10.1.3 Metering and Instrumentation
3.10.1.4 Battery Systems
3.10.1.5 Engine-Generator Set
3.10.1.6 Grounding System
3.10.2 Functional Acceptance Tests
3.11 DEMONSTRATION
3.11.1 Instructor's Qualification Resume
3.11.2 Training Plan
3.11.2.1 Operating Personnel Training
3.11.2.2 Maintenance Personnel Training
3.12 ONSITE TRAINING
3.13 INSTALLATION
3.14 FINAL TESTING AND INSPECTION
3.15 MANUFACTURER'S FIELD SERVICE
3.16 POSTED DATA AND INSTRUCTIONS
3.17 ACCEPTANCE

-- End of Section Table of Contents --

SECTION 26 32 15.00

ENGINE-GENERATOR SET STATIONARY 15-2500 KW, WITH AUXILIARIES

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN SOCIETY OF MECHANICAL ENGINEERS (ASME)

ASME B16.1	(2020) Gray Iron Pipe Flanges and Flanged Fittings Classes 25, 125, and 250
ASME B16.3	(2021) Malleable Iron Threaded Fittings, Classes 150 and 300
ASME B16.5	(2020) Pipe Flanges and Flanged Fittings NPS 1/2 Through NPS 24 Metric/Inch Standard
ASME B16.9	(2018) Factory-Made Wrought Buttwelding Fittings
ASME B16.11	(2016) Forged Fittings, Socket-Welding and Threaded
ASME B16.21	(2021) Nonmetallic Flat Gaskets for Pipe Flanges
ASME B31.1	(2020) Power Piping
ASME B31.3	(2020) Process Piping
ASME BPVC SEC IX	(2017; Errata 2018) BPVC Section IX-Welding, Brazing and Fusing Qualifications
ASME BPVC SEC VIII D1	(2019) BPVC Section VIII-Rules for Construction of Pressure Vessels Division 1

ASTM INTERNATIONAL (ASTM)

ASTM A53/A53M	(2022) Standard Specification for Pipe, Steel, Black and Hot-Dipped, Zinc-Coated, Welded and Seamless
ASTM A106/A106M	(2019a) Standard Specification for Seamless Carbon Steel Pipe for High-Temperature Service
ASTM A126	(2004; R 2019) Standard Specification for Gray Iron Castings for Valves, Flanges, and Pipe Fittings

ASTM A181/A181M	(2014; R 2020) Standard Specification for Carbon Steel Forgings, for General-Purpose Piping
ASTM A193/A193M	(2020) Standard Specification for Alloy-Steel and Stainless Steel Bolting Materials for High-Temperature Service and Other Special Purpose Applications
ASTM A194/A194M	(2022) Standard Specification for Carbon Steel, Alloy Steel, and Stainless Steel Nuts for Bolts for High-Pressure or High-Temperature Service, or Both
ASTM A234/A234M	(2019) Standard Specification for Piping Fittings of Wrought Carbon Steel and Alloy Steel for Moderate and High Temperature Service
ASTM B395/B395M	(2018) Standard Specification for U-Bend Seamless Copper and Copper Alloy Heat Exchanger and Condenser Tubes
ASTM D975	(2020) Standard Specification for Diesel Fuel Oils

ELECTRICAL GENERATING SYSTEMS ASSOCIATION (EGSA)

EGSA 101P	(1995) Performance Standard for Engine Driven Generator Sets

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 1	(2000; R 2011) General Principles for Temperature Limits in the Rating of Electric Equipment and for the Evaluation of Electrical Insulation
IEEE 43	(2013) Recommended Practice for Testing Insulation Resistance of Rotating Machinery
IEEE 81	(2012) Guide for Measuring Earth Resistivity, Ground Impedance, and Earth Surface Potentials of a Ground System
IEEE 100	(2000; Archived) The Authoritative Dictionary of IEEE Standards Terms
IEEE 115	(2019) Guide for Test Procedures for Synchronous Machines: Part I Acceptance and Performance Testing; Part II Test Procedures and Parameter Determination for Dynamic Analysis
IEEE 120	(1989; R 2007) Master Test Guide for Electrical Measurements in Power Circuits
IEEE 519	(2022) Standard for Harmonic Control in

Electrical Power Systems

IEEE C2	(2023) National Electrical Safety Code
IEEE C50.12	(2005; R 2010) Standard for Salient Pole 50 HZ and 60 Hz Synchronous Generators and Generation/Motors for Hydraulic Turbine Applications Rated 5 MVA and above
IEEE C57.13	(2016) Standard Requirements for Instrument Transformers
IEEE C57.13.1	(2006; R 2012) Guide for Field Testing of Relaying Current Transformers

INTERNATIONAL ELECTRICAL TESTING ASSOCIATION (NETA)

NETA ATS	(2021) Standard for Acceptance Testing Specifications for Electrical Power Equipment and Systems

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

ISO 3046	(2002, 2006, 2009, 2001) Reciprocating Internal Combustion Engines - Performance--Part 1, 3, 4, 5, 6
ISO 8528	(1993; R 2018) Reciprocating Internal Combustion Engine Driven Alternating Current Generator Sets--Part 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13

MANUFACTURERS STANDARDIZATION SOCIETY OF THE VALVE AND FITTINGS INDUSTRY (MSS)

MSS SP-58	(2018) Pipe Hangers and Supports - Materials, Design and Manufacture, Selection, Application, and Installation
MSS SP-70	(2011) Gray Iron Gate Valves, Flanged and Threaded Ends
MSS SP-71	(2018) Gray Iron Swing Check Valves, Flanged and Threaded Ends
MSS SP-80	(2019) Bronze Gate, Globe, Angle and Check Valves
MSS SP-85	(2011) Gray Iron Globe & Angle Valves Flanged and Threaded Ends

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA ICS 2	(2000; R 2020) Industrial Control and Systems Controllers, Contactors, and Overload Relays Rated 600 V
NEMA ICS 6	(1993; R 2016) Industrial Control and Systems: Enclosures

NEMA MG 1	(2021) Motors and Generators
NEMA PB 1	(2011) Panelboards
NEMA PB 2	(2011) Deadfront Distribution Switchboards
NEMA/ANSI C12.11	(2006; R 2019) Instrument Transformers for Revenue Metering, 10 kV BIL through 350 kV BIL (0.6 kV NSV through 69 kV NSV)

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 30	(2021; TIA 20-1; TIA 20-2; TIA 21-3) Flammable and Combustible Liquids Code
NFPA 37	(2021) Standard for the Installation and Use of Stationary Combustion Engines and Gas Turbines
NFPA 54	(2021) National Fuel Gas Code
NFPA 58	(2020; TIA 20-1; TIA 20-2; TIA 20-3) Liquefied Petroleum Gas Code
NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National Electrical Code
NFPA 99	(2021; TIA 20-1) Health Care Facilities Code
NFPA 110	(2022) Standard for Emergency and Standby Power Systems

SOCIETY OF AUTOMOTIVE ENGINEERS INTERNATIONAL (SAE)

SAE ARP892	(1965; R 1994) DC Starter-Generator, Engine
SAE J537	(2016) Storage Batteries

U.S. DEPARTMENT OF DEFENSE (DOD)

MIL-DTL-16884	(2017; Rev P) Fuel, Naval Distillate
MIL-STD-461	(2015; Rev G) Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment

U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)

40 CFR 60	Standards of Performance for New Stationary Sources

UNDERWRITERS LABORATORIES (UL)

UL 142	(2006; Reprint Jan 2021) UL Standard for Safety Steel Aboveground Tanks for Flammable and Combustible Liquids

UL 429	(2013; Reprint Mar 2021) Electrically Operated Valves
UL 467	(2022) UL Standard for Safety Grounding and Bonding Equipment
UL 489	(2016; Rev 2019) UL Standard for Safety Molded-Case Circuit Breakers, Molded-Case Switches and Circuit-Breaker Enclosures
UL 891	(2019) UL Standard for Safety Switchboards
UL 1236	(2015; Reprint Feb 2021) UL Standard for Safety Battery Chargers for Charging Engine-Starter Batteries
UL 1437	(2006) Electrical Analog Instruments - Panel Board Types

1.2 RELATED MATERIALS

Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM applies to this section, except as modified herein.

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Engine-Generator Set and Auxiliary Equipment; G

Auxiliary Systems; G

Detailed Drawings; G

Acceptance; G

SD-03 Product Data

Harmonic Requirements; G

Emissions; G

filters; G

special tools; G

Remote Alarm Annunciator; G

Engine-Generator Parameter Schedule

Heat Exchanger

Generator

Manufacturer's Catalog

Site Welding

Spare Parts

Onsite Training

Vibration-Isolation

Posted Data and Instructions; G

Instructions; G

Experience

Field Engineer

General Installation

Exciter

SD-05 Design Data

Performance Criteria

Sound Limitations; G

Integral Main Fuel Storage Tank

Day Tank

Power Factor

Heat Exchanger

Time-Delay on Alarms

Cooling System

Vibration Isolation

Battery Charger

Capacity Calculations for Engine-Generator Set; G

SD-06 Test Reports

Performance Tests

Factory Inspection and Tests

Factory Tests

Onsite Inspection and Tests; G

Functional Acceptance Tests; G

Maintenance Procedures; G

Operation and Maintenance Manuals; G

Inspections; G

Functional Acceptance Test Procedure; G

SD-07 Certificates

Cooling System

Vibration Isolation

Prototype Test

Reliability and Durability

Fuel System Certification; G

Start-Up Engineer; G

Instructor's Qualification Resume; G

Engine Emission Limits; G

Sound Limitations

Site Visit

Current Balance

Materials and Equipment

Factory Inspection and Tests

SD-09 Manufacturer's Field Reports

Engine Tests; G

Generator Tests; G

Assembled Engine-Generator Set Tests; G

SD-10 Operation and Maintenance Data

Preliminary Assembled Operation and Maintenance Manuals; G

Submit in accordance with Section 01 78 23 OPERATION AND MAINTENANCE DATA and the paragraph ASSEMBLED OPERATION AND MAINTENANCE MANUALS.

SD-11 Closeout Submittals

Posted Data and Instructions; G

Training Plan; G

1.4 QUALITY ASSURANCE

1.4.1 Conformance to Codes and Standards

Where equipment is specified to conform to requirements of any code or standard such as UL, NEMA, etc., the design, fabrication and installation must also conform to the code.

1.4.2 Site Welding

Weld structural members in accordance with Section 05 05 23.16 STRUCTURAL WELDING. For all other welding, qualify procedures and welders in accordance with ASME BPVC SEC IX.

a. Welding procedures qualified by others, and welders and welding operators qualified by a previously qualified employer may be accepted as permitted by ASME B31.1.

b. Submit a copy of qualifying procedures and a list of names and identification symbols of qualified welders and welding operators.

c. Submit a letter listing the welder qualifying procedures for each welder, complete with supporting data such as test procedures used, what was tested to, and a list of the names of all welders and their identification symbols.

d. Perform welder qualification tests for each welder whose qualifications are not in compliance with the referenced standards. Notify the Contracting Officer 24 hours in advance of qualification tests which must be performed at the work site, if practical.

e. The welder or welding operator must apply the personally assigned symbol near each weld made as a permanent record.

1.4.3 Vibration Limitation

Limit the maximum engine-generator set vibration in the horizontal, vertical, and axial directions to 6 mils (peak-peak RMS), with an overall velocity limit of 0.95 inches/second RMS, at rated speed for all loads through 110 percent of rated speed. The engine-generator set must be provided with vibration isolation in accordance with the manufacturer's standard recommendation. Where the vibration isolation system does not secure the base to the structure floor or unit foundation, provide seismic restraints in accordance with the seismic parameters specified.

1.4.4 Torsional Analysis

Submit torsional analysis including prototype testing or calculations which certify and demonstrate that no damaging or dangerous torsional vibrations will occur when the prime mover is connected to the generator, at synchronous speeds, plus/minus 10 percent.

1.4.5 Performance Data

Submit vibration isolation system performance data for the range of frequencies generated by the engine-generator set during operation from no load to full load and the maximum vibration transmitted to the floor. Also submit a description of seismic qualification of the engine-generator mounting, base, and vibration isolation.

1.4.6 Experience

Each component manufacturer must have a minimum of 3 years' experience in the manufacture, assembly and sale of components used with stationary engine-generator sets for commercial and industrial use. The engine-generator set manufacturer/assembler must have a minimum of 3 years' experience in the manufacture, assembly and sale of stationary engine-generator sets for commercial and industrial use. Submit a statement showing and verifying these requirements.

1.4.7 Field Engineer

The engine-generator set manufacturer or assembler must furnish a qualified field engineer to supervise the complete installation of the engine-generator set, assist in the performance of the onsite tests, and instruct personnel as to the operational and maintenance features of the equipment. The field engineer must have attended the engine generator manufacturer's training courses on installation and operation and maintenance of engine generator sets. Submit a letter listing the qualifications, schools, formal training, and experience of the field engineer.

1.4.8 Detailed Drawings

Submit detailed drawings showing the following:

a. Base-mounted equipment, complete with base and attachments, including anchor bolt template and recommended clearances for maintenance and operation.

b. Starting system.

c. Fuel system.

d. Cooling system.

e. Exhaust system.

f. Electric wiring of relays, breakers, programmable controllers, and switches including single line and wiring diagrams.

g. Lubrication system, including piping, pumps, strainers, filters, heat exchangers for lube oil and turbocharger cooling, electric heater, controls and wiring.

h. Location, type, and description of vibration isolation devices for all applications.

i. The safety system, including wiring schematics.

j. One-line schematic and wiring diagrams of the generator, exciter, regulator, governor, and instrumentation.

k. Panel layouts.

l. Mounting and support for each panel and major piece of electrical equipment.

m. Engine-generator set rigging points and lifting instructions.

1.4.9 Auxiliary Systems Engine-Generator Set and Auxiliary Equipment Drawing Requirements

Submit drawings pertaining to the engine-generator set and auxiliary equipment, including but not limited to the following:

a. Certified outline, general arrangement (setting plan), and anchor bolt details. Show total weight and center of gravity of assembled equipment on the steel sub-base.

b. Detailed elementary, schematic wiring, and interconnection diagrams of the engine starting system, jacket coolant heating system, engine protective devices, engine alarm devices, engine speed governor system, generator and excitation system, and other integral devices.

c. Detailed elementary, schematic wiring; and interconnection diagrams of the fuel system, starting battery system, engine-generator control panel, generator circuit breaker, and remote alarm annunciator.

d. Dimensional drawings or catalog cuts of exhaust silencers, radiator, fuel day tanks, fuel oil cooler, valves and pumps, intake filters, vibration isolators, and other auxiliary equipment not integral with the engine-generator set.

1.4.10 Auxiliary Systems Drawing Requirements

Submit drawings showing floor plan arrangement of exhaust, air intake, fuel oil cooler, and jacket coolant water systems including arrangement of piping and pipe sizes.

1.4.11 Vibration Isolation System Certification

Submit certification from the manufacturer that the vibration isolation system will reduce the vibration to the limits specified in the paragraph VIBRATION ISOLATION.

1.4.12 Fuel System Certification

When the fuel system requires a fuel oil cooler as described in the paragraph FUEL OIL COOLER, submit certification from the engine manufacturer that the fuel system design is satisfactory.

1.5 DELIVERY, STORAGE, AND HANDLING

Properly protect materials and equipment, in accordance with the manufacturers recommended storage procedures,before, during, and after installation. Protect stored items from the weather and contamination. During installation, cap piping and similar openings to keep out dirt and other foreign matter.

Deliver equipment on pallets or blocking wrapped in heavy-duty plastic, sealed to protect parts and assemblies from moisture and dirt. Protect and prepare batteries for shipment as recommended by the battery manufacturer. Store auxiliary equipment at the site in covered enclosures, protected from atmospheric moisture, dirt, and ground water.

1.6 EXTRA MATERIALS

Provide two sets of special tools and two sets of filters required for maintenance. Special tools are those that only the manufacturer provides, for special purposes, or to reach otherwise inaccessible parts. One handset must be provided for each electronic governor when required to indicate and/or change governor response settings. Furnish 4 liters one gallon of identical paint used on engine-generator set in manufacturer's sealed container with each engine-generator set.

Wrenches and tools specifically designed and required to work on the new equipment, which are not commercially available as standard mechanic's tools, must be furnished to the Contracting Officer.

Provide proposed operating instructions for the engine-generator set and auxiliary equipment laminated between matte-surface thermoplastic sheets and suitable for placement adjacent to corresponding equipment. After approval, install operating instructions where directed.

1.7 MAINTENANCE SERVICES

Submit the operation and maintenance manuals and have them approved prior to commencing onsite tests.

1.7.1 Operation Manual

Provide three copies of the manufacturer's standard operation manual . Sections must be separated by heavy plastic dividers with tabs which identify the material in the section. Fold drawings with the title block visible, and placed in 8-1/2 by 11 inch plastic pockets with reinforced holes. The manual must include:

a. Step-by-step procedures for system startup, operation, and shutdown;

b. Drawings, diagrams, and single-line schematics to illustrate and define the electrical, mechanical, and hydraulic systems with their controls, alarms, and safety systems;

c. Procedures for interface and interaction with related systems to include automatic transfer switches, fire alarm/suppression systems, and load shedding systems.

1.7.2 Maintenance Manual

Provide three copies of the manufacturer's standard maintenance manual. Separate each section by a heavy plastic divider with tabs. Fold drawings with the title block visible, and placed in plastic pockets with reinforced holes. The manual must include:

a. Procedures for each routine maintenance item.Procedures for troubleshooting.Factory-service, take-down overhaul, and repair service manuals, with parts lists.

b. The manufacturer's recommended maintenance schedule.

c. A component list which includes the manufacturer's name, address, type or style, model or serial number, rating, and catalog number for the major components.

d. A list of spare parts for each piece of equipment and a complete list of materials and supplies needed for operation.

1.7.3 Assembled Operation and Maintenance Manuals

The contents of the assembled operation and maintenance manuals must include the manufacturer's O&M information required by the paragraph SD-10, OPERATION AND MAINTENANCE DATA .

a. Manuals must be in separate books or volumes, assembled and bound securely in durable, hard covered, water resistant binder, and indexed by major assembly and components in sequential order.

b. A table of contents (index) must be made part of the assembled O&M. The manual must be assembled in the order noted in table of contents.

c. The cover sheet or binder on each volume of the manuals must be identified and marked with the words, "Operation and Maintenance Manual."

PART 2 PRODUCTS

2.1 SYSTEM REQUIREMENTS

a. Provide and install each engine-generator set complete and totally functional, with all necessary ancillary equipment to include: air filtration; starting system; generator controls, protection, and isolation; instrumentation; lubrication; fuel system; cooling system; and engine exhaust system. Each engine-generator set must satisfy the requirements specified in the Engine-Generator Parameter Schedule. Submit certification that the engine-generator set and cooling system function properly in the ambient temperatures specified.

b. Provide each engine-generator set consisting of one engine, one generator, and one exciter mounted, assembled, and aligned on one base; and all other necessary ancillary equipment which may be mounted separately. Assemble sets having a capacity of 750 kW or smaller and attach to the base prior to shipping. Sets over 750 kW capacity may be shipped in sections. Provide set components that are environmentally suitable for the locations shown and that are the manufacturer's standard product offered in catalogs for commercial or industrial use. Provide a generator strip heater for moisture control when the generator is not operating. Identify any nonstandard products or components and the reason for their use.

2.1.1 Engine-Generator Parameter Schedule

Engine-Generator Set and Auxiliary Equipment Capacity Calculations for Engine-Generator Set shall be provided by manufacturer.

2.1.2 Rated Output Capacity

Provide each engine-generator-set with power equal to the sum of service load plus the machine's efficiency loss and associated ancillary equipment loads. Rated output capacity must also consider engine and/or generator oversizing required to meet requirements in paragraph Engine-Generator Parameter Schedule.

The engine must meet the specified maximum BMEP requirements at rated speed as calculated in accordance with the calculations in the

engine-generator parameter schedule. The engine capacity must be based on the following:

a. Engine burning diesel fuel conforming to MIL-DTL-16884 at an ambient temperature of 85 degrees F. For stationary engines operated in the United States, diesel fuel requirements are found in 40 CFR 60 Subpart IIII.

b. Engine cooled by a radiator fan mechanically driven by the engine or remote with a motor driven fan.

c. Engine cooled by coolant mixture of water and ethylene glycol, 50 percent by volume of each.

2.1.2.1 Engine Emission Limits

Engine must be certified by the manufacturer to meet applicable EPA emission standards found in 40 CFR 60 Subpart IIII. In addition, engine must meet any applicable state or local emission requirements (ex: California SCAQMD).

2.1.2.2 Performance Class

The voltage and frequency behavior of the generator set must be in accordance with ISO 8528 operating limit values for performance Cof the class to which it belongs.

2.1.3 Power Ratings

Power ratings must be in accordance with EGSA 101P.

2.1.4 Transient Response

The engine-generator set governor and voltage regulator must cause the engine-generator set to respond to the maximum step load changes such that output voltage and frequency recover to and stabilize within the operational bandwidth within the transient recovery time. The engine-generator set must respond to maximum step load changes such that the maximum voltage and frequency deviations from bandwidth are not exceeded.

2.1.5 Reliability and Durability

Provide prime engine-generator sets that have both an engine and a generator capable of delivering the specified power on a prime basis with an anticipated mean time between overhauls of not less than 10,000 hours operating with a 70 percent load factor. Cite two like engines and two like generators that have performed satisfactorily in a stationary power plant, independent from the physical location of the manufacturer's and assembler's facilities. The engine and generators should have been in operation for a minimum of 8000 actual hours at a minimum load of 70 percent of the rated output capacity. During two consecutive years of service, the units should not have experienced any failure resulting in a downtime in excess of 72 hours. Provide engines that are the same model, speed, bore, stroke, number and configuration of cylinders and rated output capacity. Provide generators that are the same model, speed, pitch, cooling, exciter, voltage regulator and rated output capacity.

Submit a reliability and durability certification letter from the

manufacturer and assembler to prove that existing facilities are and have been successfully utilizing the same components proposed to meet this specification, in similar service. Certification may be based on components, i.e. engines used with different models of generators and generators used with different engines, and does not exclude annual technological improvements made by a manufacturer in the basic standard-model component on which experience was obtained, provided parts interchangeability has not been substantially affected and the current standard model meets the performance requirements specified. Provide a list with the name of the installations, completion dates, and name and telephone number of a point of contact.

2.1.6 Engine-Generator Set Enclosure

Provide engine-generator set enclosures that are corrosion resistant and fully weather resistant. The enclosure must contain all set components and provide ventilation to permit operation at Service Load under secured conditions. Provide access doors to controls and equipment requiring periodic maintenance or adjustment. Provide removable panels for access to components requiring periodic replacement. The enclosure must be capable of being removed without disassembly of the engine-generator set or removal of components other than the exhaust system. The enclosure must reduce the noise of the generator set to within the limits specified in the paragraph SOUND LIMITATIONS.

2.1.7 Vibration Isolation

Provide an engine-generator set with a vibration isolation system in accordance with the manufacturer's standard recommendation. Submit vibration isolation system performance data for the range of frequencies generated by the engine-generator set during operation from no load to full load and the maximum vibration transmitted to the floor plus description of seismic qualification of the engine-generator mounting, base, and vibration isolation. Submit torsional analysis including prototype testing or and calculations which certify and demonstrate that no damaging or dangerous torsional vibrations will occur when the prime mover is connected to the generator, at synchronous speeds, plus 10 percent. Design and qualify vibration isolation systems as an integral part of the base and mounting system in accordance with the seismic parameters specified. Where the vibration isolation system does not secure the base to the structure floor or unit foundation, provide seismic restraints in accordance with the seismic parameters specified.

2.1.8 Harmonic Requirements

Non-linear loads to be served by each engine-generator set are as indicated. The maximum linear load demand (kVA at PF) when non-linear loads will also be in use is as indicated.

2.1.9 Starting Time Requirements

Upon receipt of a signal to start, each engine generator set will start, reach rated frequency and voltage and be ready to assume load within the time specified. For standby sets used in emergency power applications, each engine generator set will start, reach rated frequency and voltage, and power will be supplied to the load terminals of the automatic transfer switch within the starting time specified.

2.2 NAMEPLATES

Provide the manufacturer's name, type or style, model or serial number and rating on a plate secured to the equipment for each major component of this specification. Provide plates and tags sized so that inscription is readily legible to operating or maintenance personnel and securely mounted to or attached in proximity of their identified controls or equipment. Lettering must be normal block lettering, a minimum of 0.25 inch high. As a minimum, provide nameplates for:

Engines	Relays
Generators	Transformers (CT & PT)
Regulators	Day tanks
Pumps and pump motors	Governors
Generator Breaker	Air Starting System
Economizers	Heat exchangers (other than base mounted)

Where the following equipment is not provided as a standard component by the engine generator set manufacturer, the nameplate information may be provided in the maintenance manual in lieu of nameplates.

Battery charger	Heaters
Switchboards	Exhaust mufflers
Switchgear	Silencers
Battery	Exciters

2.2.1 Materials

Construct ID plates and tags of 16 gage minimum thickness bronze or stainless steel sheet metal engraved or stamped with inscription. Construct plates and tags not exposed to the weather or high operational temperature of the engine of laminated plastic, 0.125 inch thick, matte white finish with black center core, with lettering accurately aligned and engraved into the core.

2.2.2 Control Devices and Operation Indicators

Provide ID plates or tags for control devices and operation indicators, including valves, off-on switches, visual alarm annunciators, gages and thermometers, that are required for operation and maintenance of provided mechanical systems. Plates or tags must be minimum of 0.5 inch high and 2 inches long and must indicate component system and component function.

2.2.3 Equipment

Provide ID plates of a minimum size of high and 5 inches long on provided equipment indicating the following information:

a. Manufacturer's name, address, type and model number, serial number,

and certificate of compliance with applicable EPA mission standards;

b. Contract number and accepted date;

c. Capacity or size;

d. System in which installed; and

e. System which it controls.

2.3 SAFETY DEVICES

Exposed moving parts, parts that produce high operating temperatures, parts which may be electrically energized, and parts that may be a hazard to operating personnel must be insulated, fully enclosed, guarded, or fitted with other types of safety devices. Install safety devices such that proper operation of the equipment is not impaired.

2.4 MATERIALS AND EQUIPMENT

Submit certification stating that where materials or equipment are specified to comply with requirements of UL, written proof of such compliance has been obtained. The label or listing of the specified agency, or a written certificate from an approved, nationally recognized testing organization equipped to perform such services, stating that the items have been tested and conform to the requirements and testing methods of the specified agency are acceptable as proof.

2.4.1 Circuit Breakers, Low Voltage

UL 489.

2.4.2 Filter Elements

Provide the manufacturer's standard fuel-oil, lubricating-oil, and combustion-air filter elements.

2.4.3 Instrument Transformers

NEMA/ANSI C12.11.

2.4.4 Revenue Metering

IEEE C57.13.

2.4.5 Pipe (Fuel/Lube-Oil, Compressed Air, Coolant, and Exhaust)

ASTM A53/A53M, or ASTM A106/A106M steel pipe. Pipe smaller than 2 inches must be Schedule 80. Pipe 2 inches and larger must be Schedule 40.

2.4.5.1 Flanges and Flanged Fittings

ASTM A181/A181M, Class 60, or ASME B16.5, Grade 1, Class 150.

2.4.5.2 Pipe Welding Fittings

ASTM A234/A234M, Grade WPB or WPC, Class 150 or ASME B16.11, 3000 lb.

2.4.5.3 Threaded Fittings

ASME B16.3, Class 150.

2.4.5.4 Valves

MSS SP-80, Class 150.

2.4.5.5 Gaskets

Manufacturer's standard.

2.4.6 Pipe Hangers

MSS SP-58.

2.4.7 Electrical Enclosures

NEMA ICS 6.

2.4.7.1 Switchboards

NEMA PB 2.

2.4.7.2 Panelboards

NEMA PB 1.

2.4.8 Electric Motors

Provide electric motors that conform to the requirements of NEMA MG 1. Motors must have sealed ball bearings and a maximum speed of 1800 rpm. Motors used indoors must have drip-proof frames; enclose those that are used outside. Alternating current motors larger than 1/2 Hp must be of the squirrel-cage induction type for operation on 208 volts or higher, 60 Hz, and three-phase power. Alternating current motors 1/2 Hp or smaller, must be suitable for operation on 120 volts, 60 Hz, and single-phase power. Direct current motors must be suitable for operation on 125 volts.

2.4.9 Motor Controllers

Provide motor controllers and starters that conform to the requirements of NFPA 70 and NEMA ICS 2.

2.5 ENGINE

Each engine must operate on No. 2-D diesel fuel conforming to ASTM D975, must be designed for stationary applications and must be complete with ancillaries. The engine must be a standard production model shown in the manufacturer's catalog describing and depicting each engine-generator set and all ancillary equipment in sufficient detail to demonstrate complete specification compliance. The engine must be naturally aspirated, supercharged, or turbocharged. The engine must be 2- or 4-stroke-cycle and compression-ignition type. The engine must be vertical in-line, V- or opposed-piston type, with a solid cast block or individually cast cylinders. The engine must have a minimum of two cylinders. Opposed-piston type engines must have more than four cylinders. Each block must have a coolant drain port. Equip each engine with an over-speed sensor.

ISO 3046. Diesel engines must be four-cycle naturally aspirated, or turbocharged, or turbocharged and intercooled; vertical in-line or vertical Vee type; designed for stationary service. Engines must be capable of immediate acceleration from rest to normal speed without intermediate idle/warm up period or pre-lubrication to provide essential electrical power. Two-cycle engines are not acceptable.

2.5.1 Sub-base Mounting

Mount each engine-generator set on a structural steel sub-base sized to support the engine, generator, and necessary accessories, auxiliaries and control equipment to produce a complete self-contained unit as standard with the manufacturer. Design the structural sub-base to properly support the equipment and maintain proper alignment of the engine-generator set in the specified seismic zone. In addition, provide sub-base with both lifting rings and jacking pads properly located to facilitate shipping and installation of the unit. Factory align engine and generator on the sub-base and securely bolt into place in accordance with the manufacturer's standard practice. Crankshaft must have rigid coupling for connection to the generator.

2.5.2 Assembly

Completely shop assemble each engine-generator set on its structural steel sub-base. Paint entire unit with manufacturer's standard paints and colors. After factory tests and before shipping, thoroughly clean and retouch painting as necessary to provide complete protection.

2.5.3 Turbocharger

If required by the manufacturer to meet the engine-generator set rating, provide turbine type driven by exhaust gas from engine cylinders, and direct connected to the blower supplying air to the engine intake manifold.

2.5.4 Intercooler

Provide manufacturer's standard intercooler for engine size specified.

2.5.5 Crankcase Protection

2.5.6 Miscellaneous Engine Accessories

Provide the following engine accessories where the manufacturer's standard design permits:

a. Piping on engine to inlet and outlet connections, including nonstandard companion flanges.

b. Structural steel sub-base and vibration isolators, foundation bolts, nuts, and pipe sleeves.

c. Level jack screws or shims, as required.

d. Rails, chocks, and shims for installation of sub-base on the foundation.

e. Removable guard, around fan. Support guard, on engine sub-base, to suit manufacturer's standard.

2.5.7 Intercooler

Provide manufacturer's standard intercooler for engine size specified.

2.6 FUEL SYSTEM

Provide fuel system conforming to the requirements of NFPA 30 and NFPA 37 and containing the following elements.

2.6.1 Pumps

Fuel transfer pumps may be mounted on the day tank. Pumps must be horizontal, positive displacement. Direct-connect pump to motor through a flexible coupling. Equip each pump with a bypass relief valve, if not provided with an internal relief valve. Provide motor and controller in accordance with the paragraphs ELECTRIC MOTORS and MOTOR CONTROLLERS, respectively.

2.6.1.1 Main Pump

Provide engines with an engine driven pump. The pump must supply fuel at a minimum rate sufficient to provide the amount of fuel required to meet the performance indicated within the parameter schedule. Base the fuel flow rate on meeting the load requirements and all necessary recirculation.

2.6.1.2 Auxiliary Fuel Pump

Provide auxiliary fuel pumps to maintain the required engine fuel pressure, if either required by the installation or indicated on the drawings. The auxiliary pump must be driven by a dc electric motor powered by the starting/station batteries. Automatically actuate the auxiliary pump by a pressure-detecting device.

2.6.2 Fuel Filter

Provide a minimum of one full-flow fuel filter for each engine. The filter must be readily accessible and capable of being changed without disconnecting the piping or disturbing other components. Mark the inlet and outlet connections of the filter.

Provide intake filter assemblies for each engine of the oil bath or dry type, as standard with the manufacturer. Filters must be capable of removing a minimum of 92 percent of dirt and abrasive 3 microns and larger from intake air. Size filters to suit engine requirements at 100 percent of rated full load. Design unit for field access for maintenance purposes.

2.6.3 Relief/Bypass Valve

Provide a relief/bypass valve to regulate pressure in the fuel supply line, return excess fuel to a return line and prevent the build-up of excessive pressure in the fuel system.

2.6.4 Integral Main Fuel Storage Tank

Provide each engine with an integral main fuel tank. Each tank must be factory installed and provided as an integral part of the generator manufacturer's product. Provide each tank with connections for fuel supply line, fuel return line, local fuel fill port, gauge, vent line, and

float switch assembly. Provide a fuel return line cooler as recommended by the manufacturer and assembler. The temperature of the fuel returning to the tank must be below the flash point of the fuel. Mount the tank within the enclosure for each engine-generator set provided with weatherproof enclosures. The fuel fill line must be accessible without opening the enclosure.

a. All Tanks: UL 142. Provide integral in skid double wall (110 percent containment) fuel tanks with a capacity as indicated. Epoxy coat day tanks inside and prime and paint outside. Construct tanks of not less than 3/16 inch steel plate with welded joints and necessary stiffeners on exterior of tank. Provide a braced structural steel framework support. Weld tank top tight. Provide 4 1/2 inch square inspection port with a 2 inch NPT fill connection and spill box. Provide proper normal and emergency venting for the primary tank and emergency venting only for the secondary tank / containment basin in accordance with UL 142 requirements. Provide an overflow or return line between the fuel day tank and storage tank in accordance with NFPA 37.

b. Float Switches for Day Tanks: Provide tank-top mounted or external float cage, single-pole, single-throw type designed for use on fuel oil tanks. Arrange high level float switches to close on rise of liquid level, and low level float switches to close on fall of liquid level. Mount float cage units with isolating and drain valves. Contacts must be suitable for the station battery voltage.

(1) Critical low level float switch which must activate at 5 percent of normal liquid level must shut engine off.

(2) Low-low level float switch which must activate alarm at 30 percent of normal liquid level.

(3) Low level float switch which must open the fuel oil solenoid valve and start the fuel transfer pump at 75 percent of normal liquid level.

(4) High level float switch which must close the fuel oil solenoid valve and stop the fuel transfer pump at 90 percent of normal liquid level.

(5) Critical high level float switch which must activate alarm at 95 percent of normal liquid level.

c. Leak Detector Switch for All Tanks: Actuates when fuel is detected in containment basin, stops fuel transfer pump, and closes the fuel oil solenoid valve.

d. Control Panel for All Tanks: Provide NEMA ICS 6, Type 1, enclosed control panel for each day tank. Control panel must include the following accessories.

(1) Power available LED (green).

(2) Critical low fuel alarm contacts for shut down of engine.

(3) Low-low level fuel alarm LED.

(4) Low-low level fuel alarm contracts for remote annunciator.

(5) Critical high level fuel alarm LED.

(6) Leak detecting alarm LED.

(7) Alarm horn.

e. Tank Gages for All Tanks: Provide buoyant force type gages for fuel tanks with dial indicator not less than 4 inches in size and arranged for top mounting. Calibrate each reading dial or scale for its specific tank to read from empty to full, with intermediate points of 1/4, 1/2, and 3/4.

f. Integral Base Tanks Used as Primary Tank: Provide a 2 inch opening at the tank fill port, fitted an overfill prevention valve (OPV). Additionally, the fill opening must be perpendicular to the tank in order to allow operation of the OPV. Integral base tank must be sized and configured such that the filling and venting nozzles are outside the generator cabinet for ease of accessibility, inspection, and maintenance. Level gage must be in the line of sight from the fill port.

g. Integral Base Tanks Located Inside Buildings. The tank vents must discharge outside the building in accordance with NFPA 30 and NFPA 37. The fill pipe must terminate outside the building. The fill pipe connection point must be housed in a sealed spill box. High level alarms or level gauges used as overfill protection mechanisms must annunciate at the fill connection point. Provide an overfill prevention valve (OPV) at the tank with a check valve mounted on the fill line in the spill box. The fill connection point must be labeled with tank contents and capacity.

2.6.4.1 Fuel Transfer Pump

Fuel transfer pumps may be mounted on the day tank. Pump must be horizontal, positive displacement. Direct-connect pump to motor through a flexible coupling. Equip each pump with a bypass relief valve, if not provided with an internal relief valve. Provide motor and controller in accordance with the paragraphs ELECTRIC MOTORS and MOTOR CONTROLLERS, respectively.

2.6.4.2 Capacity

Each tank must have capacity to supply fuel to the engine for an uninterrupted 4-hour period at 100 percent rated load without being refilled.

2.6.4.3 Local Fuel Fill

Each local fuel fill port on the day tank must have a screw-on cap.

2.6.4.4 Fuel Level Controls

Provide tanks with a float-switch assembly to perform the following functions:

a. Activate the "Low Fuel Level" alarm at 70 percent of the rated tank

capacity.

b. Activate the "Overfill Fuel Level" alarm at 95 percent of the rated tank capacity.

2.6.4.5 Arrangement

Integral tanks may allow gravity flow into the engine. Gravity flow tanks and any tank that allows a fuel level above the fuel injectors must have an internal or external factory installed valve located as near as possible to the shell of the tank. The valve must close when the engine is not operating. Provide integral day tanks with any necessary pumps to supply fuel to the engine as recommended by the generator set manufacturer. The fuel supply line from the tank to the manufacturer's standard engine connection must be welded pipe.

2.6.5 Day Tank

Provide engine with integral day tank. Submit calculations for the capacity of each day tank, including allowances for recirculated fuel, usable tank capacity, and duration of fuel supply. Provide connections for fuel supply line, fuel return line, fuel overflow line, local fuel fill port, gauge, vent line, drain line, and float switch assembly for control for each day tank. Provide a fuel return line cooler as recommended by the manufacturer and assembler. The temperature of the fuel returning to the day tank must be below the flash point of the fuel. Install a temperature sensing device in the fuel supply line, fuel overflow line, local fuel fill port, gauge, vent line, drain line, and float switch assembly for control. Mount the day tank within the enclosure for each engine-generator set with weatherproof enclosures. The fuel fill line must be accessible without opening the enclosure.

2.6.5.1 Capacity, Prime

Provide day tank with the capacity to supply fuel to the engine for an uninterrupted 8-hour period at 100 percent rated load without being refilled, plus any fuel which may be returned to the main fuel storage tank. Submit calculations for the capacity of each day tank, including allowances for recirculated fuel, usable tank capacity, and duration of fuel supply. The calculation of the capacity of each day tank must incorporate the requirement to stop the supply of fuel into the day tank at a "High" level mark of 90 percent of the ultimate volume of the tank.

2.6.5.2 Capacity, Standby

Provide day tank with the capacity to supply fuel to the engine for an uninterrupted 4-hour period at 100 percent rated load without being refilled, plus any fuel which may be returned to the main fuel storage tank. Submit calculations for the capacity of each day tank, including allowances for recirculated fuel, usable tank capacity, and duration of fuel supply. The calculation of the capacity of each day tank must incorporate the requirement to stop the supply of fuel into the day tank at 90 percent of the ultimate volume of the tank.

2.6.5.3 Drain Line

Each day tank drain line must be accessible and equipped with a shutoff valve. Arrange self-supporting day tanks to allow drainage into a 12 inch tall bucket.

2.6.5.4 Local Fuel Fill

Each local fuel fill port on the day tank must have a screw-on cap.

2.6.5.5 Fuel Level Controls

Provide day tank with a float-switch assembly to perform the following functions:

a. Start the supply of fuel into the day tank when the fuel level is at the "Low" level mark, 75 percent of the rated tank capacity.

b. Stop the supply of fuel into the day tank when the fuel level is at 90 percent of the rated tank capacity.

c. Activate the "Overfill Fuel Level" alarm at 95 percent of the rated tank capacity.

d. Activate the "Low Fuel Level" alarm at 70 percent of the rated tank capacity.

e. Activate the automatic fuel supply shut-off valve located on the fill line of the day tank and shut down the fuel pump which supplies fuel to the day tank at 95 percent of the rated tank capacity. Stop the flow of fuel before any fuel can be forced into the fuel overflow line.

2.6.5.6 Fuel Oil Solenoid Valve

UL 429. Provide electric solenoid type control valve for each day tank. Solenoid must be rated for starting battery voltage. Valve body must have a minimum working pressure rating of 150 psig at 200 degrees F. Valve must be capable of passing 0 to 10 gpm of fuel oil. Valves must be two-way, direct acting, normally closed (open when energized, closed when de-energized), with stainless steel body and resilient seat material. Solenoid enclosures must be NEMA ICS 6, Type 1. Body connections must be same size as connecting piping. Valve must be in line before the fuel pump.

2.6.5.7 Arrangement

Integral day tanks may allow gravity flow into the engine. Provide gravity flow tanks with an internal or external valve located as near as possible to the shell of the tank. The valve must close when the engine is not operating. Provide integral day tanks with any necessary pumps to supply fuel to the engine as recommended by the generator set manufacturer. Arrange the overflow connection and the fuel supply line for integral day tanks which do not rely upon gravity flow so that the highest possible fuel level is below the fuel injectors. The fuel supply line from the day tank to the manufacturer's standard engine connection must be welded pipe.

2.6.6 Fuel Oil Cooler

Provide an air cooled fuel oil cooler if the temperature of the fuel returned to the tank from the engine will cause overheating of the tank fuel above the maximum fuel temperature allowed by the engine manufacturer when operating at maximum rated generator power output and low fuel level in the tank. The fuel oil cooler must be furnished by the engine

manufacturer for the application and the installation must be complete including piping and power requirements.

2.7 LUBRICATION

Provide engine with a separate lube-oil system conforming to NFPA 30 and NFPA 37. Pressurize each system by engine-driven pumps. Regulate system pressure as recommended by the engine manufacturer. Provide a pressure relief valve on the crankcase for closed systems. Vent the crankcase in accordance with the manufacturer's recommendation. Do not vent the crankcase to the engine exhaust system. Crankcase breathers, if provided on engines installed in buildings or enclosures, must be piped to vent to the outside. The system must be readily accessible for service such as draining, refilling, etc. Each system must permit addition of oil and have oil-level indication with the set operating. The system must utilize an oil cooler as recommended by the engine manufacturer.

2.7.1 Lube-Oil Filter

Provide one full-flow filter for each pump. The filter must be readily accessible and capable of being changed without disconnecting the piping or disturbing other components. Mark inlet and outlet connections.

2.7.2 Lube-Oil Sensors

Equip each engine with lube-oil pressure sensors located downstream of the filters and provide signals for required indication and alarms. Submit two complete sets of filters, required for maintenance, supplied in a suitable storage box. Provide these filters in addition to filters replaced after testing.

2.7.3 Precirculation Pump

Provide a motor-driven precirculation pump powered by the station battery, complete with motor starter, if recommended by the engine manufacturer.

2.8 COOLING SYSTEM

Provide each engine with its own cooling system to operate automatically while its engine is running. The cooling system coolant must use a combination of water and ethylene-glycol sufficient for freeze protection at the minimum winter outdoor temperature specified. The maximum temperature rise of the coolant across each engine must not exceed that recommended below. Submit a letter which certifies that the engine-generator set and cooling system function properly in the ambient temperature specified.

2.8.1 Coolant Pumps

Provide centrifugal coolant pumps. Each engine must have an engine-driven primary pump. Provide secondary pumps that are electric motor driven and have automatic controllers. Control raw-water circulating pump by manual-off-automatic controllers and must be engine driven.

2.8.2 Heat Exchanger

Provide heat exchanger with the size and capacity to limit the maximum allowable temperature rise in the coolant across the engine to that recommended and submitted for the maximum summer outdoor design

temperature and site elevation. Submit manufacturer's data to quantify heat rejected to the space with the engine generator set at rated capacity. Provide heat exchangers that are corrosion resistant, suitable for service in ambient conditions of application.

2.8.2.1 Fin-Tube-Type Heat Exchanger (Radiator)

Heat exchanger may be factory coated with corrosion resistant film, provided that corrective measures are taken to restore the heat rejection capability of the radiator to the initial design requirement via over sizing, or other compensating methods. Provide internal surfaces that are compatible with liquid fluid coolant used. Materials and coolant are subject to approval by the Contracting Officer. Provide heat exchangers that are pressure type incorporating a pressure valve, vacuum valve and a cap. Design caps for pressure relief prior to removal. Provide heat exchanger and cooling system that is capable of withstanding a minimum pressure of 7 psi and protect with a strong grille or screen guard. Provide heat exchanger with at least two tapped holes; equip one tapped hole with a drain cock, and plug the rest.

Provide for each engine-generator set, as standard with the manufacturer.

a. Design Conditions: Each radiator unit must have ample capacity to remove not less than the total Btu per hour of heat rejected by its respective engine at 100 percent full-rated load to the jacket water, fuel oil, and lubricating oil system, and intercooler. Radiator capacity must be rated at optimum temperature of coolant leaving the engine and intercooler as recommended by the engine manufacturer. Pressure drop through the radiator must not exceed 6 psi when circulating the maximum required coolant flow. Radiator air velocity must be a maximum of 1500 feet per minute.

b. Engine Mounted Radiator Construction: Radiator fan must direct airflow from the engine outward through the radiator. Fan must be V-belt driven directly from the engine crankshaft. Fan static capacity must be adjusted to suit the ductwork furnished. Cooling section must have a tube and fin-type core consisting of copper or copper base alloy tubes with nonferrous fins. Select engine-driven fans for quiet vibration-free operation. Make provision for coolant expansion either by self-contained expansion tanks or separately mounted expansion tanks, as standard with the manufacturer. Provide suitable guards for each fan and drive.

c. Remote Radiator Construction: Provide radiators as described above, except radiators must be remotely piped and provided with electric motor driven fan. Drive must be multiple V-belt or reduction gears. Expansion tanks must be separately mounted. Air flow must be vertical or horizontal as indicated. Interlock fan with engine operation such that fan must operate when engine operates when recommended by engine manufacturer. Provide controls and control devices complete which must cycle fan on and off based upon coolant temperature. Provide motors and controllers in accordance with the paragraphs ELECTRIC MOTORS and MOTOR CONTROLLERS, respectively. Motors, controllers, contactors, and disconnects must conform to Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM.

d. Coolant solution must be a mixture of clean water and ethylene glycol, 50 percent by volume each. Provide an anti-freeze solution tester suitable for the mixture.

Field installed jacket coolant water piping must conform to the following:

a. Piping: Provide seamless steel pipe, Schedule 40, conforming to ASTM A53/A53M, Grade A.

b. Fittings and Flanges: Fittings, 1 1/2 inches or smaller, must be malleable iron conforming to ASME B16.3 for Class 300 threaded type. Fittings, 2 inches and larger, must be steel butt welding conforming to ASME B16.9. Utilize either ASME B16.1 or Class A of ASTM A126 for Class 125 cast-iron flanged fittings. Flanges must be Class 150 slip-on forged steel welding flanges in accordance with ASME B16.5, with material in accordance with ASTM A181/A181M, Grade I. Provide flat face flanges for connecting to Class 125 standard cast-iron valves, fittings, and equipment connections.

c. Valves

(1) Gate Valves: For valves, 1 1/2 inches and smaller, provide double disk, rising stem, inside screw, union bonnet type, Class 125 bronze material conforming to MSS SP-80. For valves, 2 inches and larger, provide double-disk, parallel seat type, hydraulic-rated, Class 125, outside screw and yoke type with flanged ends and bronze trim conforming to MSS SP-70. Provide stem packing of material compatible with the system coolant.

(2) Globe Valves: For valves, 1 1/2 inches and smaller, provide rising stem, inside screw, union bonnet type, Class 125 bronze valves conforming to MSS SP-80. For valves, 2 inches and larger, provide Class 125 cast iron, flanged ends, bronze trim globe valves conforming to MSS SP-85. Valves must have renewable composition or cast iron discs compatible with the system coolant.

(3) Check Valves: MSS SP-71 or MSS SP-80, swing check type.

d. Hangers and Supports: MSS SP-58.

e. Piping Sleeves: Provide where piping passes through masonry or concrete walls, floors, roofs, and partitions. Place sleeves during construction. Unless indicated otherwise, pipe sleeves must comply with following requirements: Sleeves in outside walls below and above grade, in floor, or in roof slabs, must be standard weight zinc coated steel pipe. Sleeves in partitions must be zinc coated sheet steel having a nominal weight of not less than 0.90 pound per square foot. Space between piping insulation and the sleeve must be not less than 0.25 inch. Sleeves must be held securely in proper position and location during construction. Sleeves must be of sufficient length to pass through entire thickness of walls, partitions, or slabs. Sleeves in floor slabs must extend 2 inches above the finished floor. Space between the pipe and the sleeve must be firmly packed with insulation and caulked at both ends of the sleeve with plastic waterproof cement.

2.8.2.2 Shell and U-Tube Type Heat Exchanger

Provide multiple pass shell, U-tube type heat exchanger. Exchanger must operate with low temperature water in the shell and high temperature water in the tubes. Provide exchangers that are constructed in accordance with ASME BPVC SEC VIII D1 and certified with ASME stamp secured to the unit. Provide U-tube bundles that are completely removable for cleaning and tube

replacement and free to expand with the shell. Construct shells of seamless steel pipe or welded steel. Tubes must be cupronickel or inhibited admiralty, constructed in accordance with ASTM B395/B395M, suitable for the temperatures and pressures specified. Tubes less than 3/4 inch unless otherwise indicated are not acceptable. Design shell side and tube side for 150 psig working pressure and factory tested at 300 psig. Locate high and low temperature water and pressure relief connections in accordance with the manufacturers standard practice. Water connections larger than 3 inches must be ASME Class 150 flanged. Water pressure loss through clean tubes must be as recommended by the engine manufacturer. Minimum water velocity through tubes must be 1 fps and assure turbulent flow. Provide one or more pressure relief valves for each heat exchanger in accordance with ASME BPVC SEC VIII D1. The aggregate relieving capacity of the relief valves must be not less than that required by the above code. Install discharge from the valves indicated. Install the relief valves on the heat exchanger shell. Install a drain connection with 3/4 inch hose bib at the lowest point in the system near the heat exchanger. Install additional drain connection with threaded cap or plug wherever required for thorough draining of the system.

2.8.3 Expansion Tank

The cooling system must include an air expansion tank which will accommodate the expanded water of the system generated within the normal operating temperature range, limiting the pressure increase at all components in the system to the maximum allowable pressure at those components. The tank must be suitable for operating temperature of 250 degrees F and a working pressure of 125 psi. Provide welded steel tank , tested and stamped in accordance with ASME BPVC SEC VIII D1 for the stated working pressure. Do not use a bladder type tank. Support the tank by steel legs or bases for vertical or steel saddles for horizontal installation.

2.8.4 Thermostatic Control Valve

Provide a modulating type, thermostatic control valve in the coolant system to maintain the coolant temperature range submitted in paragraph SUBMITTALS.

2.8.5 Ductwork

Provide ductwork as specified in mechanical documents and specs, except use a flexible connection to connect the duct to the engine radiator. Material for the connection must be wire-reinforced glass. Provide airtight connection.

2.8.6 Temperature Sensors

Equip each engine with coolant temperature sensors. Provide temperature sensors with signals for pre-high and high indication and alarms.

2.9 SOUND LIMITATIONS

Submit sound power level data for the packaged unit operating at 100 percent load in a free field environment. The data should demonstrate compliance with the sound limitation requirements of this specification. Submit certification from the manufacturer stating that the sound emissions meet the specification. Do not exceed the following sound pressure levels in any of the indicated frequencies when measured in a

free field at a radial distance of 22.9 feet 7 meters at 45 degrees apart in all directions when operating at 100 percent load.

2.10 AIR INTAKE EQUIPMENT

Locate filters and silencers in locations that are convenient for servicing. Provide high-frequency filter type silencers and locate in the air intake system as recommended by the engine manufacturer. Provide silencer to reduce the noise level at the air intake so that the indicated pressure levels specified in paragraph SOUND LIMITATIONS will not be exceeded. A combined filter-silencer unit meeting requirements for the separate filter and silencer items may be provided. Provide rubber expansion elements in air-intake lines.

Provide intake filter assemblies for each engine of the oil bath or dry type, as standard with the manufacturer. Filters must be capable of removing a minimum of 92 percent of dirt and abrasive 3 microns and larger from intake air. Size filters to suit engine requirements at 100 percent of rated full load. Design unit for field access for maintenance purposes.

2.11 EXHAUST SYSTEM

Provide a separate and complete system for each engine. Support piping to minimize vibration. Where a V-type engine is provided, use a V-type connector, with necessary flexible sections and hardware, to connect the engine exhaust outlets.

2.11.1 Flexible Sections and Expansion Joints

Provide a flexible section at each engine and an expansion joint at each muffler. Provide flexible sections and expansion joints that have flanged connections. Provide flexible sections made of convoluted seamless tube without joints or packing. Provide bellows type expansion joints. Provide stainless steel expansion and flexible elements suitable for engine exhaust gas at the maximum exhaust temperature that is specified by the engine manufacturer. Provide expansion and flexible elements that are capable of absorbing vibration from the engine and compensation for thermal expansion and contraction.

2.11.2 Exhaust Muffler

Provide a chamber type exhaust muffler. Provide welded steel muffler designed for outside horizontal mounting. Provide eyebolts, lugs, flanges, or other items as necessary for support in the location and position indicated. Do not exceed the engine manufacturer's recommended pressure drop. Outside mufflers must be zinc coated or painted with high temperature 400 degrees F resisting paint. The muffler and exhaust piping together must reduce the noise level to less than the maximum acceptable level listed for sound limitations in paragraph SOUND LIMITATIONS. Provide muffler with a drain valve, nipple, and cap at the low-point of the muffler.

A critical class silencer must be provided for each engine which will reduce the exhaust sound spectrum by the following listed values at a 75 foot radius from the outlet, with generator set loaded to rated capacity and clear weather. Inlet and outlet connections must be flanged.

Octave Band Center Frequency (Hertz)								
Minimum Silencer Attenuation Decibels	63	125	250	500	1000	2000	4000	8000

2.11.3 Exhaust Piping

Slope horizontal sections of exhaust piping downward away from the engine to a drip leg for collection of condensate with drain valve and cap. Changes in direction must be long radius. Insulate exhaust piping, mufflers and silencers installed inside any building in accordance with paragraph THERMAL INSULATION and covered to protect personnel. Provide vertical exhaust piping with a hinged, gravity-operated, self-closing, rain cover.

Field installed exhaust piping must conform to the following:

a. Exhaust Piping: Provide flanges for connections to engines, exhaust mufflers, and flexible connections. Provide steel pipe conforming to ASTM A53/A53M for each engine complete with necessary fittings, flanges, gaskets, bolts, and nuts. Exhaust piping must be Schedule 40 pipe for 12 inches and smaller, standard weight for sizes 14 inches through 24 inches, and 0.25 inch wall thickness for sizes larger than 24 inches. Flanges must be Class 150 slip-on forged steel welding flanges in accordance with ASME B16.5, with material in accordance with ASTM A181/A181M, Grade I. Fittings must be butt welding conforming to ASTM A234/A234M, with wall thickness same as adjoining piping. Fittings must be of same material and wall thickness as pipe. Built-up miter welded fittings may be used. Miter angles of each individual section must not exceed 22.5 degrees total and not more than 11.25 degrees relative to the axis of the pipe at any one cut. Gaskets for exhaust piping must be of high temperature asbestos-free material suitable for the service and must be ASME B16.21, composition ring, 0.0625 inch thick. Bolting material for exhaust flanges must be alloy-steel bolt-studs conforming to ASTM A193/A193M, Grade B7 bolts and alloy-steel nuts conforming to ASTM A194/A194M, Grade 7. Bolts must be of sufficient length to obtain full bearing on the nuts and must project not more than two full threads beyond the nut. Provide stainless steel counterbalance type rain caps at termination of each exhaust pipe.

b. Expansion (Flexible) Joints: Provide sections of multiple corrugated stainless steel expansion joints in the engine exhaust piping for each engine to absorb expansion strains and vibration transmitted to the piping. Flexible joints must be suitable for operation at 200 degrees F above normal exhaust gas temperature at 100 percent load, 10,000 cycles, minimum. Joints must be flanged and located between engine exhaust manifold and exhaust piping, must be the same size as exhaust piping size, and must be designed and constructed for engine exhaust service.

c. Hangers and Supports: MSS SP-58.

d. Piping Sleeves: Provide where piping passes through masonry or concrete walls, floors, roofs, and partitions. Sleeves must be placed during construction. Unless indicated otherwise, pipe sleeves must

comply with following requirements: sleeves in outside walls below and above grade, in floor, or in roof slabs, must be standard weight zinc coated steel pipe. Sleeves in partitions must be zinc coated sheet steel having a nominal weight of not less than 0.90 pound per square foot. Space between piping insulation and the sleeve must not be less than 0.25 inch. Sleeves must be held securely in proper position and location during construction. Sleeves must be sufficient length to pass through entire thickness of walls, partitions, or slabs. Sleeves in floor slabs must extend 2 inches above the finished floor. Space between the pipe and the sleeve must be firmly packed with insulation and caulked at both ends of the sleeve with plastic waterproof cement.

e. Piping Insulation: Provide exhaust piping insulation in accordance with Section 23 07 00 THERMAL INSULATION FOR MECHANICAL SYSTEMS.

2.12 PYROMETER

Provide a pyrometer, multi-point selector switch, and individual thermocouples with calibrated leads to show the temperature of the combined exhaust. For a supercharged engine, provide additional points, thermocouples and leads to show the temperature in the turbocharger exhaust gas outlet and combustion air discharge passages. Graduated scale length less than 6 inches is not acceptable. Provide double pole selector switch with an "off" position, one set of points for each thermocouple, and suitable indicating dial. Calibrate the pyrometer, thermocouples, leads and compensating devices to show true exhaust temperature within plus or minus 1 percent above the highest temperature encountered at 110 percent load conditions.

2.13 EMISSIONS

The finished installation must comply with Federal, state, and local regulations and restrictions regarding the limits of emissions. Submit certification from the engine manufacturer stating that the engine exhaust emissions meet the federal, state, and local regulations and restrictions specified. At a minimum this certification must include emission factors for criteria pollutants including nitrogen oxides, carbon monoxide, particulate matter, sulfur dioxide, non-methane hydrocarbon, and for hazardous air pollutants (HAPs).

2.14 STARTING SYSTEM

Provide starting system for standby engine generator sets used in emergency applications in accordance with NFPA 99 and NFPA 110and as follows.

2.14.1 Controls

Provide an engine control switch with functions including: run/start (manual), off/reset, and, automatic mode. Provide start-stop logic for adjustable cycle cranking and cool-down operation. Arrange the logic for manual starting and fully automatic starting in accordance with paragraph AUTOMATIC ENGINE-GENERATOR-SET SYSTEM OPERATION. Provide electrical starting systems with an adjustable cranking limit device to limit cranking periods from 1 second up to the maximum duration.

2.14.2 Capacity

Provide starting system with sufficient capacity, at the maximum outdoor summer temperature specified to crank the engine without damage or overheating. The system must provide a minimum of three cranking periods with 15 second intervals between cranks. Each cranking period must have a maximum duration of 15 seconds. Starting must be accomplished using an adequately sized dc starter system with a positive shift solenoid to engage the starter motor and to crank the engine continuously for 60 seconds without overheating.

2.14.3 Electrical Starting

Manufacturers recommended dc system, utilizing a negative circuit ground. Starting motors must be in accordance with SAE ARP892.

2.14.3.1 Battery

Provide a starting battery system including the battery, battery rack, intercell connectors, spacers, automatic battery charger with overcurrent protection, metering and relaying. Provide battery in accordance with SAE J537. Size critical system components (rack, protection, etc.) to withstand the seismic acceleration forces specified. Provide lead-acid battery with sufficient capacity, at the minimum outdoor and maximum outdoor temperature specified, to provide the specified cranking periods. Valve-regulated lead-acid batteries are not acceptable.

Provide maintenance free, sealed, lead-acid, SAE Type D engine starting batteries. Batteries must have sufficient capacity to provide 60 seconds of continuous cranking of the engine in an ambient temperature of 120 degrees F.

2.14.3.2 Battery Charger

Provide a current-limiting battery charger, conforming to UL 1236, that automatically recharges the batteries. Submit battery charger sizing calculations. The charger must be capable of an equalize charging rate which is manually adjustable in a continuous range and a floating charge rate for maintaining the batteries at fully charged condition. Provide an ammeter to indicate charging rate. Provide a voltmeter to indicate charging voltage. Provide a timer for the equalize charging-rate setting. A battery is considered to be fully depleted when the output voltage falls to a value which will not operate the engine generator set and its components.

Provide 120 volt ac, enclosed, automatic equalizing, dual-rate, solid-state, constant voltage type battery charger with automatic ac line compensation. DC output must be voltage regulated and current limited. Charger must have two ranges, float and equalize, and must provide continuous taper charging. The charger must have a continuous output rating of not less than 10 amperes and must be sized to recharge the engine starting batteries in a minimum of 8 hours while providing the control power needs of the engine-generator set. Enclosure must be NEMA ICS 6, Type 1. The following accessories must be included:

a. DC ammeter

b. DC voltmeter

c. Equalize light

d. AC on light

e. Low voltage light

f. High voltage light

g. Equalize test button/switch

h. AC circuit breaker

i. Low dc voltage alarm relay

j. High dc voltage alarm relay

k. Current failure relay

l. AC power failure relay

2.14.4 Storage Batteries

Provide storage batteries of suitable rating and capacity to supply and maintain power for the remote alarm annunciator for a period of 90 minutes minimum without the voltage applied falling below 87.5 percent of normal. Provide a 120 volt ac automatic battery charger.

2.14.5 Starting Aids

Provide one or more of other following methods to assist engine starting.

2.14.5.1 Glow Plugs

Design glow plugs to provide sufficient heat for combustion of fuel within the cylinders to guarantee starting at an ambient temperature of -25 degrees F.

2.14.5.2 Jacket-Coolant Heaters

Mount a thermostatically controlled electric heater in the engine coolant jacketing to automatically maintain the coolant within plus or minus 3 degrees F of the control temperature. The heater must operate independently of engine operation so that starting times are minimized. Power for the heaters must be 120 volts ac. Include necessary equipment, piping, controls, wiring, and accessories.

2.14.5.2.1 Prime Rated Sets

The control temperature must be the higher of the manufacturer's recommended temperature or the minimum coolant inlet temperature of the engine recommended in paragraph SUBMITTALS.

2.14.5.2.2 Standby Rated Sets

The control temperature must be the temperature recommended by the engine manufacturer to meet the starting time specified at the minimum winter outdoor temperature.

2.14.5.3 Lubricating-Oil Heaters

Mount a thermostatically controlled electric heater in the engine lubricating-oil system to automatically maintain the oil temperature within plus or minus 3 degrees F of the control temperature. The heater must operate independently of engine operation so that starting times are minimized. Power for the heaters must be 120 volts ac.

2.15 GOVERNOR

Provide a forward acting type engine speed governor system. Steady-state frequency band and frequency regulation (droop) must be in accordance with the operating limit values of the performance class specified in the paragraph PERFORMANCE CLASS.

Provide engine with a governor which maintains the frequency within a bandwidth of the rated frequency, over a steady-state load range of zero to 100 percent of rated output capacity. Configure the governor for safe manual adjustment of the speed/frequency during operation of the engine-generator set, without special tools, from 90 to 110 percent of the rated speed/frequency, over a steady state load range of 0 to 100 percent or rated capacity. Submit two complete sets of special tools required for maintenance (except for electronic governor handset). Special tools are those that only the manufacturer provides, for special purposes, or to reach otherwise inaccessible parts. Provide a suitable tool box for tools. Provide one handset for each electronic governor when required to indicate and/or change governor response settings. Maintain the midpoint of the frequency bandwidth at the same value for steady-state loads over the range of zero to 100 percent of rated output capacity for isochronous governors.

2.16 GENERATOR

Provide synchronous type, one or two bearing, generator conforming to the performance criteria in NEMA MG 1, equipped with winding terminal housings in accordance with NEMA MG 1, equipped with an amortisseur winding, and directly connected to the engine. Submit calculations of the engine and generator output power capability, including efficiency and parasitic load data. Provide Class H insulation.

a. Select NEMA MG 1, Part 16, standby duty, and temperature rise of 130 degrees C for engine-generator sets which are expected to operate for less than 300 hours per year. Select NEMA MG 1, Part 22, continuous duty, and temperature rise of 105 degrees C for engine-generator sets expected to operate 300 hours or greater per year or rated 300 kW and above.

b. Select 2/3 pitch design option for engine-generator sets rated 300 kW and above.

c. Select 10-12 lead re-connectable for engine-generator sets rated 300 kW to 800 kW.

d. For applications requiring high SCR loading or in harsh environments laden with salts and chemicals, select vacuum pressure impregnation (VPI) insulated coils. When engine-generator sets are rated 800 kW and larger, also select form wound coils.

e. Provide salient-pole type, ac, brushless-excited, revolving field,

air-cooled, self-ventilated, coupled type, synchronous generator conforming to NEMA MG 1, Part 16, and IEEE C50.12. Generator must be rated for standby duty at 100 percent of the power rating of the engine-generator set as specified in paragraph ENGINE-GENERATOR SET RATINGS AND PERFORMANCE. Temperature rise of each of the various parts of the generator must not exceed 130 degrees C as measured by resistance, based on a maximum ambient temperature of 40 degrees C. Winding insulation must be Class H.

f. Stator: Stator windings must be with VPI insulated coils.

g. Rotor: The rotor must have connected amortisseur windings.

h. Generator Space Heater: Provide 120 volt ac heaters. Heater capacity must be as recommended by the generator manufacturer to aid in keeping the generator insulation dry.

i. Grounding: Provide non-corrosive steel grounding pads located at two opposite mounting legs.

j. Filters: Provide manufacturer's standard generator cooling air filter assembly.

k. Design generator to protect against mechanical, electrical and thermal damage due to vibration, 25 percent overspeeds, or voltages and temperatures at a rated output capacity of 110 percent for prime applications and 100 percent for standby applications.

l. Provide generator ancillary equipment meeting the short circuit requirements of NEMA MG 1. Select drip-proof guarded option for generators without weatherproof enclosures.

m. Submit manufacturer's standard data for each generator (prototype data at the specified rating or above is acceptable), listing the following information:

(1) Direct-Axis sub-transient reactance (per unit).

(2) The generator kW rating and short circuit current capacity (both symmetric and asymmetric).

2.16.1 Current Balance

At 100 percent rated output capacity, and load impedance equal for each of the 3 phases, the permissible current difference between any 2 phases must not exceed 2 percent of the largest current on either of the 2 phases. Submit certification stating that the flywheel has been statically and dynamically balanced and is capable of being rotated at 125 percent of rated speed without vibration or damage.

2.16.2 Voltage Balance

At any balanced load between 75 and 100 percent of rated output capacity, the difference in line-to-neutral voltage among the 3 phases must not exceed 1 percent of the average line-to-neutral voltage. For a single phase load condition, consisting of 25 percent load at unity power factor placed between any phase and neutral with no load on the other 2 phases, the maximum simultaneous difference in line-to-neutral voltage between the phases must not exceed 3 percent of rated line to neutral voltage. The

single-phase load requirement must be valid utilizing normal exciter and regulator control. The interpretation of the 25 percent load for single phase load conditions means 25 percent of rated current at rated phase voltage and unity power factor.

2.16.3 Waveform

The deviation factor of the line-to-line voltage at zero load and at balanced rated output capacity must not exceed 10 percent. The RMS of all harmonics must be less than 5.0 percent and that of any one harmonic less than 3.0 percent of the fundamental at rated output capacity. Design and configure engine-generator to meet the total harmonic distortion limits of IEEE 519.

2.17 EXCITER

Provide brushless generator exciter. Provide semiconductor rectifiers that have a minimum safety factor of 300 percent for peak inverse voltage and forward current ratings for all operating conditions, including 110 percent generator output at 104 degrees F ambient. The exciter and regulator in combination must maintain generator-output voltage within the limits specified.

Provide a brushless excitation system consisting of an exciter and rotating rectifier assembly integral with the generator and a voltage regulator. Insulation class for parts integral with the generator must be as specified in paragraph GENERATOR. System must provide a minimum short circuit of 300 percent rated engine-generator set current for at least 10 seconds. Steady state voltage regulation must be in accordance with the operating limit values of the performance class specified in the paragraph PERFORMANCE CLASS.

a. Exciter and Rotating Rectifier Assembly: Rectifiers must be provided with surge voltage protection.

b. Permanent Magnet Generator: Provide a voltage spike suppression device for permanent magnet generator (PMG) excitation systems.

c. Voltage Regulator: Voltage regulator must be solid state or digital, automatic, three-phase sensing, volts per hertz type regulator. Regulator must receive its input power from a PMG. Voltage variation for any 40 degree C change over the operating temperature range must be less than plus or minus 1.0 percent. Operating temperature must be minus 40 degree C to plus 70 degree C. Voltage adjust range must be plus to minus 5.0 percent of nominal. Inherent regulator features must include over excitation shutdown.

2.17.1 Electromagnetic Interference (EMI) Suppression

Provide as an integral part of the generator and excitation system, EMI suppression complying with MIL-STD-461.

2.18 VOLTAGE REGULATOR

Provide a solid-state voltage regulator, separate from the exciter, for each generator. Maintain the voltage within a bandwidth of the rated voltage, over a steady-state load range of zero to 100 percent of rated output capacity. Configure regulator for safe manual adjustment of the engine-generator voltage output without special tools, during operation,

from 90 to 110 percent of the rated voltage over the steady state load range of 0 to 100 percent of rated output capacity. Regulation drift exceeding plus or minus 0.5 percent for an ambient temperature change of 68 degrees F is not acceptable. Reactive droop compensation or reactive differential compensation must load share the reactive load proportionally between sets during parallel operation. Provide voltage regulator with a maximum droop of 2 percent of rated voltage over a load range from 0 to 100 percent of rated output capacity and automatically maintain the generator output voltage within the specified operational bandwidth.

2.19 GENERATOR ISOLATION AND PROTECTION

Provide necessary devices for electrical protection and isolation of each engine-generator set and its ancillary equipment. The generator circuit breaker (IEEE Device 52) ratings must be consistent with the generator rated voltage and frequency, with continuous, short circuit withstand, and interrupting current ratings to match the generator capacity. Provide electrically operated generator circuit breaker. Mount a set of surge capacitors at the generator terminals. Provide monitoring and control devices as specified in paragraph GENERATOR PANEL.

The generator circuit breaker must comply with UL 489 requirements for molded case, adjustable thermal magnetic trip type circuit breaker. The circuit breaker continuous current rating must be adequate for the power rating of the engine-generator set and the circuit breaker must be rated to withstand the short circuit current provided by the generator set. Provide circuit breaker in a NEMA ICS 6, Type 1 enclosure mounted on the engine-generator set.

2.19.1 Switchboards

Provide free-standing, metal-enclosed, general purpose, 3-phase, 4-wire, 600 volt rated, with neutral bus and continuous ground bus, switchboards conforming to NEMA PB 2 and UL 891. Neutral bus and ground bus capacity must be as shown. Provide panelboards conforming to NEMA PB 1. Provide enclosure designs, construction, materials and coatings suitable for the application and environment. Bus continuous current rating must be at least equal to the generator rating and correspond to the UL listed current ratings specified for panelboards and switchboards. Current withstand (short circuit rating) must be equal to the breaker interrupting rating. Provide copper buses.

2.19.2 Devices

Furnish with respective pieces of equipment. Motors, controllers, contactors, and disconnects must conform to Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Provide electrical connections under Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Provide controllers and contactors with maximum of 120-volt control circuits, and auxiliary contacts for use with controls furnished. When motors and equipment furnished are larger than size indicated, the cost of providing additional electrical service and related work must be included under this section.

2.20 SAFETY SYSTEM

Provide and install devices, wiring, remote panels, and local panels, etc., as a complete system to automatically activate the appropriate

signals and initiate the appropriate actions. Provide a safety system with a self-test method to verify its operability. Provide alarm signals that have manual acknowledgment and reset devices. The alarm signal systems must reactivate for new signals after acknowledgment is given to any signal. Configure the systems so that loss of any monitoring device will be dealt with as an alarm on that system element.

2.20.1 Audible Signal

Provide audible alarm signal sound at a frequency of 70 Hz at a volume of 75 dB at 10 feet. The sound must be continuously activated upon alarm and silenced upon acknowledgment. Locate signal devices as shown.

2.20.2 Visual Signal

The visual alarm signal must be a panel light. The light must be normally off, activated to be blinking upon alarm. The light must change to continuously lit upon acknowledgement. If automatic shutdown occurs, the display must maintain activated status to indicate the cause of failure and must not be reset until cause of alarm has been cleared and/or restored to normal condition. Shutdown alarms must be red; all other alarms must be amber.

2.20.3 Alarms and Action Logic

2.20.3.1 Shutdown

Accomplish simultaneous activation of the audible signal, activation of the visual signal, stopping the engine, and opening the generator main circuit breakers.

2.20.3.2 Problem

Accomplish activation of the visual signal.

2.20.4 Safety Indications and Shutdowns
Provide a local alarm panel with the following shutdown and alarm functions in accordance with NFPA 99 mounted either on or adjacent to the engine generator set.

A remote alarm panel is required for audible alarms, e.g., in the control room.

Indicator Function (at battery voltage)	NFPA 99 Level 1 CV S RA	NFPA 110 Level 1 CV S RA	NFPA 110 Level 2 CV S RA
Overcrank	X X X	X X X	X X O
Low water temperature	X NA X	X NA X	X NA O
High engine temperature pre-alarm	X NA X	X NA X	O NA NA
High engine temperature	X X X	X X X	X X O

Indicator Function (at battery voltage)	NFPA 99 Level 1 CV S RA	NFPA 110 Level 1 CV S RA	NFPA 110 Level 2 CV S RA
Low lube oil pressure pre-alarm	X NA X	NA NA NA	NA NA NA
Low lube oil pressure	X X X	X X X	X X O
Overspeed	X X X	X X X	X X O
Low fuel main tank	X NA X	X NA X	O NA O
Low coolant level	X O X	X O X	X O X
EPS supplying load	X NA NA	X NA NA	O NA NA
Control switch not in automatic position	X NA X	X NA X	X NA X
High battery voltage	X NA NA	X NA NA	O NA NA
Low cranking voltage	X NA X	X NA X	O NA NA
Low voltage in battery	X NA NA	X NA NA	O NA NA
Battery charger ac failure	X NA NA	X NA NA	O NA NA
Lamp test	X NA NA	X NA NA	X NA NA
Contacts for local and remote common alarm	X NA X	X NA X	X NA X
Audible alarm silencing switch	NA NA X	NA NA X	NA NA O
Low starting air pressure	X NA NA	X NA NA	O NA NA
Low starting hydraulic pressure	X NA NA	X NA NA	O NA NA
Air shutdown damper when used	X X X	X X X	X X O
Remote emergency stop	NA X NA	NA X NA	NA X NA

Indicator Function (at battery voltage)	NFPA 99 Level 1 CV S RA	NFPA 110 Level 1 CV S RA	NFPA 110 Level 2 CV S RA
Symbology: CV: Control panel-mounted visual. S: Shutdown of EPS indication. RA: Remote audible. Symbology: CV: Control panel-mounted visual. S: Shutdown of EPS indication. RA: Remote audible. X: Required. O: Optional. NA: Not applicable.			

2.20.5 Time-Delay on Alarms

For startup of the engine-generator set, install time-delay devices bypassing the low lubricating oil pressure alarm during cranking, and the coolant-fluid outlet temperature alarm. Submit the magnitude of monitored values which define alarm or action set points, and the tolerance (plus and/or minus) at which the devices activate the alarm or action for items contained within the alarm panels. The lube-oil time-delay device must return its alarm to normal status after the engine starts. The coolant time-delay device must return its alarm to normal status 5 minutes after the engine starts.

2.21 SYNCHRONIZING PANEL

Provide panel as specified in paragraph PANELS and provide controls, gauges, meters, and displays to include:

a. Frequency meters, dial type, with a range of 90 to 110 percent of rated frequency. Do not use vibrating-reed type meters . One must monitor generator output frequency ("Generator Frequency Meter") and the other must monitor the frequency of the parallel source ("Bus Frequency Meter").

b. Voltmeters, ac, dial type, 3-phase, with 4-position selector switch for the generator output ("Generator Volt Meter") and for the parallel power source ("Bus volt meter").

c. Automatic synchronizer.

d. Manual synchronizing controls.

e. Indicating lights for supplementary indication of synchronization.

f. Synchroscope.

g. Wattmeter, indicating.

2.22 PANELS

Each panel must be of the type and kind necessary to provide specified functions. Mount panels as shown. Mount instruments flush or semiflush. Provide convenient access to the back of panels to facilitate maintenance. Calibrate instruments using recognized industry calibration standards. Provide a panel identification plate identifying the panel function. Provide a plate identifying the device and its function for each instrument and device on the panel. Provide switch plates identifying the switch-position function.

2.22.1 Enclosures

Design enclosures for the application and environment, conforming to NEMA ICS 6. Locking mechanisms must be keyed alike.

Provide for each engine-generator set and fabricate from zinc coated or phosphatized and shop primed 16 gage minimum sheet steel in accordance with the manufacturer's standard design. Provide a complete, weatherproof enclosure for the engine, generator, and auxiliary systems and equipment. Support exhaust piping and silencer so that the turbocharger is not subjected to exhaust system weight or lateral forces generated in connecting piping that exceed the engine manufacturer's maximum allowed forces and moments. The housing must have sufficient louvered openings to allow entrance of outside air for engine and generator cooling at full load. Design louvered openings to exclude driving rain and snow. Provide properly arranged and sized, hinged panels in the enclosure to allow convenient access to the engine, generator, and control equipment for maintenance and operational procedures. Provide hinged panels with spring type latches which must hold the panels closed securely and will not allow them to vibrate. Brace the housing internally to prevent excessive vibration when the set is in operation

2.22.2 Analog

Provide analog electrical indicating instruments in accordance with UL 1437 with semi-flush mounting. Switchboard, switchgear, and control-room panel-mounted instruments must have 250 degree scales with an accuracy of not less than 99 percent. Unit-mounted instruments must be the manufacturer's standard with an accuracy of not less than 98 percent. The instrument's operating temperature range must be minus 4 to plus 158 degrees F. Distorted generator output voltage waveform of a crest factor less than 5 must not affect metering accuracy for phase voltages, hertz and amps.

2.22.3 Electronic

Electronic indicating instruments must be true RMS indicating instruments, 100 percent solid state, state-of-the-art, microprocessor controlled to provide specified functions. Provide control, logic, and function devices that are compatible as a system, sealed, dust and water tight, and that utilize modular components with metal housings and digital instrumentation. Provide an interface module to decode serial link data from the electronic panel and translate alarm, fault and status conditions to set of relay contacts. Instrument accuracy less than 98 percent for unit mounted devices and 99 percent for control room, panel mounted devices, throughout a temperature range of minus 4 to 158 degrees F is not acceptable. Provide LED or back lit LCD data display. Additionally, the display must provide indication of cycle programming and diagnostic codes

for troubleshooting. Numeral height must be 0.5 inch .

2.22.4 Parameter Display

Provide indication or readouts of the tachometer, lubricating-oil pressure, ac voltmeter, ac ammeter, frequency meter, and safety system parameters. Specify a momentary switch for other panels.

2.23 SURGE PROTECTION

Electrical and electronic components must be protected from, or designed to withstand the effects of surges from switching and lightning.

2.24 MANUAL ENGINE-GENERATOR-SET SYSTEM OPERATION

Provide complete facilities for manual starting and testing of each set without load, loading and unloading of each set, and synchronization of each set with an energized bus.

2.25 STATION BATTERY SYSTEM

Provide a station battery system including the battery, battery rack, spacers, automatic battery charger and distribution panelboard with overcurrent protection, metering and relaying. Size components to withstand the seismic acceleration forces specified. Provide batteries that have a rated life of 20 years and a manufacturer's 5-year, no cost replacement guarantee.

2.25.1 Battery Charger

Furnish a current-limiting, 120-volt battery charger to automatically recharge the batteries. Provide a charger that is capable of an equalize charging rate and a floating-charge rate for maintaining the batteries in a fully charged condition. Equip the charger with a low-voltage alarm relay, 0- to 24-hour equalizing timer, an ammeter to indicate charging rate, and necessary circuit breakers. The charger must conform to the requirements of UL 1236. A battery is considered to be fully depleted when the voltage falls to a level incapable of operating the equipment loads served by the battery.

2.26 BASE

Provide a steel base. Design the base to rigidly support the engine-generator set, ensure permanent alignment of rotating parts, be arranged to provide easy access to allow changing of lube-oil, and ensure that alignment is maintained during shipping and normal operation. The base must permit skidding in any direction during installation and must withstand and mitigate the affects of synchronous vibration of the engine and generator. Provide base with suitable holes for anchor bolts and jacking screws for leveling.

2.27 THERMAL INSULATION

Provide thermal insulation as specified in Section 23 07 00 THERMAL INSULATION FOR MECHANICAL SYSTEMS.

2.28 PAINTING AND FINISHING

Clean, prime and paint the engine-generator set in accordance with the

manufacturer's standard color and practice.

2.29 FACTORY INSPECTION AND TESTS

Submit six complete reproducible copies of the factory inspection result on the checklist format specified below. Perform the factory tests on each engine-generator set. The component manufacturer's production line test is acceptable as noted. Run each engine-generator set for at least 1 hour at rated output capacity prior to inspections. Complete inspections and make all necessary repairs prior to testing. Use engine generator controls and protective devices that are provided by the generator set manufacturer as part of the standard package for factory tests. When controls and switchgear are not provided as part of the generator set manufacturer's standard package, the actual controls and protective devices provided for the project are not required to be used during the factory test. The Contracting Officer may provide one or more representatives to witness inspections and tests.

2.29.1 Factory Inspection

Perform inspections prior to beginning and after completion of testing of the assembled engine-generator set. Look for leaks, looseness, defects in components, proper assembly, etc. and note any item found to be in need of correction as a necessary repair. Use the following checklist for the inspection:

INSPECTION ITEM	GOOD	BAD	NOTES
Drive belts			
Governor and adjustments			
Engine timing mark			
Starting motor			
Starting aids			
Coolant type and concentration			
Radiator drains			
Block coolant drains			
Coolant fill level			
All coolant line connections			
All coolant hoses			
Combustion air filter			
Combustion air silencer			

INSPECTION ITEM	GOOD	BAD	NOTES
Lube oil type			
Lube oil sump drain			
Lube-oil filter			
Lube-oil-level indicator			
Lube-oil-fill level			
All lube-oil line connections			
All lube-oil lines			
Fuel type and amount			
All fuel-line connections			
All fuel lines			
Fuel filter			
Coupling and shaft alignment			
Voltage regulators			
Battery-charger connections			
All wiring connections			
Instrumentation			
Hazards to personnel			
Base			
Nameplates			
Paint			
Exhaust-heat recovery unit			
Switchboard			
Switchgear			

2.29.2 Factory Tests

Submit a letter giving notice of the proposed dates of factory inspections and tests at least 14 days prior to beginning tests, including:

a. A detailed description of the manufacturer's procedures for factory tests at least 14 days prior to beginning tests.

b. Six copies of the Factory Test data described below in 8-1/2 by 11 inch binders having a minimum of 3 rings from which material may readily be removed and replaced, including a separate section for each test. Separate sections by heavy plastic dividers with tabs. Provide full size (8-1/2 by 11 inch minimum) data plots showing grid lines, with full resolution.

(1) A detailed description of the procedures for factory tests.

(2) A list of equipment used, with calibration certifications.

(3) A copy of measurements taken, with required plots and graphs.

(4) The date of testing.

(5) A list of the parameters verified.

(6) The condition specified for the parameter.

(7) The test results, signed and dated.

(8) A description of adjustments made.

On engine-generator set tests where the engine and generator are required to be connected and operated together, the load power factor must be the power factor specified in the engine generator set parameter schedule. For engine-generator set with dual-fuel operating capability, perform the following tests using the primary fuel type. Perform electrical measurements in accordance with IEEE 120. Temperature limits in the rating of electrical equipment and for the evaluation of electrical insulation must be in accordance with IEEE 1. In the following tests where measurements are to be recorded after stabilization of an engine-generator set parameter (voltage, frequency, current, temperature, etc.), stabilization is considered to have occurred when measurements are maintained within the specified bandwidths or tolerances, for a minimum of four consecutive readings. Tests specifically for the generator may be performed utilizing any prime mover.

a. Insulation Resistance for Stator and Exciter Test, IEEE 115 and IEEE 43, to the performance criteria in NEMA MG 1, Part 22. Generator manufacturer's production line test is acceptable.

b. High Potential Test, in accordance with IEEE 115 and NEMA MG 1, test voltage in accordance with NEMA MG 1. Generator manufacturer's production line test is acceptable.

c. Winding Resistance Test, Stator and Exciter, in accordance with IEEE 115. Generator manufacturer's production line test is acceptable.

d. Phase Balance Voltage Test, to the performance criteria specified in paragraph GENERATOR. This test can be performed with any prime mover. Generator manufacturer's production line test results are acceptable.

(1) Start and operate the generator at no load.

(2) Adjust a regulated phase voltage (line-to-neutral) to rated voltage.

(3) Read and record the generator frequency, line-to-neutral voltages, and the line-to-line voltages.

(4) Apply 75 percent rated load and record the generator frequency, line-to-neutral voltages, and the line-to-line voltages.

(5) Apply rated load and record the generator frequency, line-to-neutral voltages, and the line-to-line voltages.

(6) Calculate average line-neutral voltage and percent deviation of individual line-neutral voltages from average for each load condition.

e. Current Balance on Stator Winding Test, by measuring the current on each phase of the winding with the generator operating at 100 percent of Rated Output Capacity, with the load impedance equal for each of the three phases: to the performance criteria specified in paragraph GENERATOR.

f. Voltage Waveform Deviation and Distortion Test in accordance with IEEE 115 to the performance criteria specified in paragraph GENERATOR. Use high-speed recording instruments capable of recording voltage waveform deviation and all distortion, including harmonic distortion. Include appropriate scales to provide a means to measure and interpret results.

g. Voltage and Frequency Droop Test. Verify that the output voltage and frequency are within the specified parameters as follows:

(1) With the generator operating at no load, adjust voltage and frequency to rated voltage and frequency. Record the generator output frequency and line-line and line-neutral voltages.

(2) Increase load to Rated Output Capacity. Record the generator output frequency and line-line and line-neutral voltages.

(3) Calculate the percent droop for voltage and frequency with the following equations:

$$\text{Voltage droop percent} = \frac{\text{(No-Load Volts) - (Rated Capacity Volts)}}{\text{(Service-Load Volts)}} \times 100$$

$$\text{Frequency droop percent} = \frac{\text{(No-Load Hertz) - (Rated Capacity Hertz)}}{\text{(Service-Load Hertz)}} \times 100$$

(4) Repeat steps 1 through 3 two additional times without making any adjustments.

h. Frequency and Voltage Stability and Transient Response. Verify that the engine-generator set responds to addition and dropping of blocks of load in accordance with the transient response requirements. Document maximum voltage and frequency variation from bandwidth and verify that voltage and frequency return to and stabilize within the specified bandwidth, within the specified response time period. Document results in tabular form and with high resolution, high speed

strip chart recorders or comparable digital recorders, as approved by the Contracting Officer. Include the following tabular data:

(1) Ambient temperature (at 15 minute intervals).

(2) Generator output current (before and after load changes).

(3) Generator output voltage (before and after load changes).

(4) Frequency (before and after load changes).

(5) Generator output power (before and after load changes).

(6) Graphic representations must include the actual instrument trace of voltage and frequency showing: charts marked at start of test; observed steady-state band; mean of observed band; momentary overshoot and undershoot (generator terminal voltage and frequency) and recovery time for each load change together with the voltage and frequency maximum and minimum trace excursions for each steady state load condition prior to and immediately following each load change. Generator terminal voltage and frequency transient recovery time for each step load increase and decrease.

(a) Perform and record engine manufacturer's recommended pre-starting checks and inspections.

(b) Start the engine, make and record engine manufacturer's after-starting checks and inspections during a reasonable warm-up period and no load. Verify stabilization of voltage and frequency within specified bandwidths.

(c) With the unit at no load, apply the Maximum Step Load Increase.

(d) Apply load in steps equal to the Maximum Step Load Increase until the addition of one more step increase will exceed the Service Load.

(e) Decrease load to the unit such that addition of the Maximum Step Load Increase will load the unit to 100 percent of Service Load.

(f) Apply the Maximum Step Load Increase.

(g) Decrease load to zero percent in steps equal to the Maximum Step Load Decrease.

(h) Repeat steps (c) through (g).

j. Test Voltage Unbalance with Unbalanced Load (Line-to-Neutral) to the performance criteria specified in paragraph GENERATOR. Prototype test data is acceptable in lieu of the actual test. Submit manufacturer's standard certification that prototype tests were performed for the generator model proposed. This test may be performed using any prime mover.

(1) Start and operate the generator set at rate voltage, no load, rated frequency, and under control of the voltage regulator. Read

and record the generator frequency, line-to-neutral voltages, and the line-to-line voltages.

(2) Apply the specified load between terminals L_1-L_2, L_2-L_0, and L_3-L_0 in turn. Record all instrument readings at each line-neutral condition.

(3) Express the greatest difference between any two of the line-to-line voltages and any two of the line-to-neutral voltages as a percent of rated voltage.

(4) Compare the largest differences expressed in percent with the maximum allowable difference specified.

PART 3 EXECUTION

3.1 EXAMINATION

After becoming familiar with all details of the job, perform a Site Visit to verify the information shown on the drawings, before performing any work. Submit a letter stating the date the site was visited and listing discrepancies found. Notify the Contracting Officer in writing of any discrepancies.

3.2 GENERAL INSTALLATION

Provide clear space for operation and maintenance in accordance with NFPA 70 and IEEE C2. Submit a copy of the manufacturer's installation procedures and a detailed description of the manufacturer's recommended break-in procedure. Install pipe, duct, conduit, and ancillary equipment to facilitate easy removal and replacement of major components and parts of the engine-generator set.

3.3 PIPING INSTALLATION

Weld piping. Provide flanged valve connections. Provide flanged connections at equipment. Provide threaded connections to the engine if the manufacturers standard connection is threaded. Except where otherwise specified, use welded flanged fittings to allow for complete dismantling and removal of each piping system from the facility without disconnecting or removing any portion of any other system's equipment or piping. Make connections to equipment with vibration isolation-type flexible connectors. Support and align piping and tubing to prevent stressing of flexible hoses and connectors. Flash pipes extending through the roof. Install piping clear of windows, doors and openings, to permit thermal expansion and contraction without damage to joints or hangers, and install a 1/2 inch drain valve with cap at each low point.

The installation of gas engines must conform to the requirements of NFPA 37 and its references therein, including NFPA 54, NFPA 58, and ASME B31.3.

3.3.1 Support

Provide hangers, inserts, and supports to accommodate any insulation and conforming to MSS SP-58. Space supports no more than 7 feet on center for pipes 2 inches in diameter or less, no more than 12 feet on center for pipes larger than 2 inches but smaller than 4 inches in diameter, and not more than 17 feet on center for pipes larger than 4 inches in diameter. Provide supports at pipe bends or change of direction.

3.3.1.1 Ceiling and Roof

Support exhaust piping with appropriately sized Type 41 single pipe roll and threaded rods; support all other piping with appropriately sized Type 1 clevis and threaded rods.

3.3.1.2 Wall

Make wall supports for pipe by suspending the pipe from appropriately sized Type 33 brackets with the appropriate ceiling and roof pipe supports.

3.3.2 Flanged Joints

Provide flanges that are Class 125 type, drilled, and of the proper size and configuration to match the equipment and engine connections. Provide gasketed flanged joints that are square and tight.

3.3.3 Cleaning

After fabrication and before assembly, piping interiors must be manually wiped clean of debris.

3.3.4 Pipe Sleeves

Fit pipes passing through construction such as ceilings, floors, or walls with sleeves. Extend each sleeve through and fasten in its respective structure and cut flush with each surface. Build the structure tightly to the sleeve. The inside diameter of each sleeve must be minimum 1/2 inch, and where pipes pass through combustible materials 1 inch larger than the outside diameter of the passing pipe or pipe insulation/covering.

3.4 ELECTRICAL INSTALLATION

Perform electrical installation in compliance with NFPA 70, IEEE C2, and Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. For vibration isolation, provide flexible fittings for conduit, cable trays, and raceways attached to engine-generator sets; provide flexible stranded conductor for metallic conductor cables installed on the engine generator set and from the engine generator set to equipment not mounted on the engine generator set; and provide crimp-type terminals or lugs for terminations of conductors on the engine generator set.

3.5 FIELD PAINTING

Perform field painting as specified in Section 09 90 00 PAINTS AND COATINGS.

3.6 ONSITE INSPECTION AND TESTS

Perform and report on factory tests and inspections prior to shipment. Provide certified copies of manufacturer's test data and results. Test procedures must conform to ASME, IEEE, IEC, and ANSI standards, and to ISO requirements on testing, as appropriate and applicable. The manufacturer performing the tests must provide equipment, labor, and consumables necessary for tests and measuring and indicating devices must be certified to be within calibration. Tests must indicate satisfactory operation and attainment of specified performance. If satisfactory, equipment tested will be given a tentative approval. Equipment must not be shipped before

approval of the factory test reports for the following tests.

Submit a letter giving notice of the proposed dates of onsite inspections and tests at least 14 days prior to beginning tests.

a. Submit a detailed description of the Contractor's procedures for onsite tests including the test plan and a listing of equipment necessary to perform the tests at least 7 days prior to beginning tests.

b. Submit six copies of the onsite test data described below in 8-1/2 by 11 inch binders having a minimum of 3 rings from which material may readily be removed and replaced, including a separate section for each test. Separate sections by heavy plastic dividers with tabs. Provide full size (8-1/2 by 11 inch minimum) data plots showing grid lines, with full resolution.

(1) A detailed description of the procedures for onsite tests.

(2) A list of equipment used, with calibration certifications.

(3) A copy of measurements taken, with required plots and graphs.

(4) The date of testing.

(5) A list of the parameters verified.

(6) The condition specified for the parameter.

(7) The test results, signed and dated.

(8) A description of adjustments made.

3.6.1 Test Conditions

3.6.1.1 Data

Make and record measurements of all parameters necessary to verify that each set meets specified parameters. If the results of any test step are not satisfactory, make adjustments, replacements, or repairs and repeat the step until satisfactory results are obtained. Unless otherwise indicated, record data in 15 minute intervals during engine-generator set operation and include: readings of all engine-generator set meters and gauges for electrical and power parameters; oil pressure; ambient temperature; and engine temperatures available from meters and gauges supplied as permanent equipment on the engine-generator set. Perform electrical measurements in accordance with IEEE 120. Definitions of terms are in accordance with IEEE 100. Provide temperature limits in the rating of electrical equipment and for the evaluation of electrical insulations in accordance with IEEE 1.

3.6.1.2 Power Factor

Submit the generator capability curve showing generator kVA output capability (kW vs. kvar) for both leading and lagging power factors ranging from 0 to 1.0. For all engine-generator set operating tests the load power factor must be the power factor specified in the engine-generator set parameter schedule.

3.6.1.3 Contractor Supplied Items

Provide equipment and supplies required for inspections and tests including fuel, test instruments, and loadbanks at the specified power factors.

3.6.1.4 Instruments

Verify readings of panel gauges, meters, displays, and instruments provided as permanent equipment during test runs, using test instruments of greater precision and accuracy. Test instrument accuracy must be within the following: current plus or minus 1.5 percent, voltage plus or minus 1.5 percent, real power plus or minus 1.5 percent, reactive power plus or minus 1.5 percent, power factor plus or minus 3 percent, frequency plus or minus 0.5 percent. Calibrate test instruments by a recognized standards laboratory within 30 days prior to testing.

3.6.1.5 Sequence

Provide the sequence of testing as specified in the approved testing plan unless variance is authorized by the Contracting Officer. Perform field testing in the presence of the Contracting Officer. Schedule and sequence tests in order to optimize run-time periods; however, follow the general order of testing: Construction Tests; Inspections; Pre-operational Tests; Safety Run Tests; Performance Tests; and Final Inspection.

3.6.2 Construction Tests

Perform individual component and equipment functional tests for fuel piping, coolant piping, and lubricating-oil piping, electrical circuit continuity, insulation resistance, circuit protective devices, and equipment not provided by the engine-generator set manufacturer prior to connection to the engine-generator set.

3.6.2.1 Piping Test

a. Flush lube-oil and fuel-oil piping with the same type of fluid intended to flow through the piping, until the outflowing fluid has no obvious sediment or emulsion.

b. Test fuel piping which is external to the engine-generator set in accordance with NFPA 30. Pressure all remaining piping which is external to the engine-generator set with air pressure at 150 percent of the maximum anticipated working pressure, but not less than 150 psi, for a period of 2 hours to prove the piping has no leaks. If piping is to be insulated, perform the test before the insulation is applied.

3.6.2.2 Electrical Equipment Tests

a. Perform low-voltage cable insulation integrity tests for cables connecting the generator breaker to the automatic transfer switch. Test low-voltage cable, complete with splices, for insulation resistance after the cables are installed, in their final configuration, ready for connection to the equipment, and prior to energization. Apply a test voltage of 500 volts dc for one minute between each conductor and ground and between all possible combinations conductors in the same trench, duct, or cable, with all other conductors in the same trench, duct, or conduit. Provide the minimum value of insulation as follows:

(1) R in meg-ohms = (rated voltage in kV plus 1) x 304.8/(length of cable in meters)

(2) R in meg-ohms = (rated voltage in kV plus 1) x 1000/(length of cable in feet)

(3) Each cable failing this test must be repaired or replaced. The repair cable must be retested until failures have been eliminated.

c. Ground-Resistance Tests. Measure the resistance of each grounding electrode system using the fall-of-potential method defined in IEEE 81. On systems consisting of interconnected ground rods, perform tests after interconnections are complete. Take measurements in normally dry weather, not less than 48 hours after rainfall. Provide site diagram indicating location of test probes with associated distances, and provide a plot of resistance vs. distance. The combined resistance of separate systems may be used to meet the requirements resistance, but the specified number of electrodes must still be provided as follows:

d. Examine and test circuit breakers and switchgear in accordance with the manufacturer's published instructions for functional testing.

3.6.3 Inspections

Perform the following inspections jointly by the Contracting Officer and the Contractor, after complete installation of each engine-generator set and its associated equipment, and prior to startup of the engine-generator set. Submit a letter certifying that all facilities are complete and functional; that each system is fully functional; and that each item of equipment is complete, free from damage, adjusted, and ready for beneficial use. Perform checks applicable to the installation. Document and submit the results of those which are physical inspections (I) in accordance with paragraph SUBMITTALS. Present manufacturer's data for the inspections designated (D) at the time of inspection. Verify that equipment type, features, accessibility, installation and condition are in accordance with the contract specification. Provide manufacturer's statements to certify provision of features which cannot be verified visually.

Drive belts	I
Governor type and features	I
Engine timing mark	I
Starting motor	I
Starting aids	I
Coolant type and concentration	D
Radiator drains	I

Block coolant drains	I
Coolant fill level	I
Coolant line connections	I
Coolant hoses	I
Combustion air filter	I
Intake air silencer	I
Lube oil type	D
Lube oil sump drain	I
Lube-oil filter	I
Lube-oil level indicator	I
Lube-oil fill level	I
Lube-oil line connections	I
Lube-oil lines	I
Fuel type	D
Fuel level	I
Fuel-line connections	I
Fuel lines	I
Fuel filter	I
Access for maintenance	I
Voltage regulator	I
Battery-charger connections	I
Wiring and terminations	I
Instrumentation	I
Hazards to personnel	I
Base	I
Nameplates	I
Paint	I

Exhaust-heat system	I
Exhaust muffler	I
Switchboard	I
Switchgear	I
Access provided to controls	I
Enclosure is weather resistant	I
Engine and generator mounting bolts (application)	I

3.6.4 Engine Tests

Perform customary commercial factory tests in accordance with ISO 3046 on each engine and associated engine protective device, including, but not limited to the following:

a. Perform dynamometer test at rated power. Record horsepower at rated speed and nominal characteristics such as lubricating oil pressure, jacket water temperature, and ambient temperature.

b. Test and record the values that the low oil pressure alarm and protective shutdown devices actuate prior to assembly on the engine.

c. Test and record values that the high jacket water temperature alarm and protective shutdown devices actuate prior to assembly on the engine.

3.6.5 Generator Tests

Tests must be performed on the complete factory assembled generator prior to shipment. Conduct tests in accordance with IEEE 115, and NEMA MG 1.

3.6.5.1 Routine Tests

Perform the following routine tests on the generators and their exciters:

a. Resistance of armature and field windings.

b. Mechanical balance.

c. Phases sequence.

d. Open circuit saturation curve and phase (voltage) balance test.

e. Insulation resistance of armature and field windings.

f. High potential tes.t

3.6.5.2 Design Tests

Submit the following design tests made on prototype machines that are

physically and electrically identical to the generators specified.

a. Temperature rise test

b. Short circuit saturation curve and current balance test

3.6.6 Assembled Engine-Generator Set Tests

Perform the following tests on the assembled engine-generator set.

3.6.6.1 Initial Stabilization Readings

Operate the engine-generator set and allow the set to stabilize at rated kW at rated power factor, rated voltage, and rated frequency. During this period record instrument readings for output power (kW), terminal voltage, line current, power factor, frequency (rpm) generator (exciter) field voltage and current, lubricating oil pressure, jacket water temperature, and ambient temperature at minimum intervals of 15 minutes. Adjust the load, voltage, and frequency to maintain rated load at rated voltage and frequency. Adjustments to load, voltage, or frequency controls must be recorded on the data sheet at the time of adjustment. Stabilization must be considered to have occurred when four consecutive voltage and current recorded readings of the generator (or exciter) field either remain unchanged or have only minor variations about an equilibrium condition with no evident continued increase or decrease in value after the last adjustment to the load, voltage, or frequency has been made.

3.6.6.2 Regulator Range Test

Remove load and record instrument readings (after transients have subsided). Adjust voltage to the maximum attainable value or to a value just prior to actuation of the overvoltage protection device. Apply rated load and adjust voltage to the minimum attainable value or a value just prior to activation of the under-voltage protection device. The data sheets must indicate the voltage regulation as a percent of rated voltage and the maximum and minimum voltages attainable. Voltage regulation must be defined as follows:

$$\text{Percent Regulation} = \frac{((\text{No-Load Voltage}) - (\text{Rated-Load Voltage})) \times 100}{(\text{Rated-Load Voltage})}$$

3.6.6.3 Frequency Range Test

Adjust the engine-generator set frequency for the maximum attainable frequency at rated load. Record instrument readings. Adjust the engine-generator set frequency for the specified minimum attainable frequency at rated load. Record instrument readings. Reduce the load to zero and adjust the engine-generator set frequency for the maximum attainable frequency. Record instrument readings. Adjust the engine-generator set frequency for the minimum attainable frequency. Record instrument readings. The data sheet must show the maximum and minimum frequencies attained at rated load, and at no load.

3.6.6.4 Transient Response Test

Drop the load to no load and re-apply rated load three times to ensure that the no load and rated load voltage and frequency values are repeatable and that the frequency and voltage regulation is within the

limits specified. Record generator terminal voltage and frequency using a high speed strip chart recorder. The data sheet must show the following results:

a. Frequency

(1) Stability bandwidth or deviation in percent of rated frequency.

(2) Recovery time.

(3) Overshoot and undershoot.

b. Voltage

(1) Stability bandwidth or deviation in percent of rated voltage.

(2) Recovery time.

(3) Overshoot and undershoot.

3.6.7 Pre-operational Tests

3.6.7.1 Protective Relays

Visually and mechanically inspect, adjust, test, and calibrate protective relays in accordance with the manufacturer's published instructions. Include pick-up, timing, contact action, restraint, and other aspects necessary to ensure proper calibration and operation. Implement relay settings in accordance with the installation coordination study. Manually or electrically operate relay contacts to verify that the proper breakers and alarms initiate. Field test relaying current transformers in accordance with IEEE C57.13.1.

3.6.7.2 Insulation Test

Test generator and exciter circuits insulation resistance in accordance with IEEE 43. Take stator readings including generator leads to switchboard at the circuit breaker. Record results of insulation resistance tests. Readings must be within limits specified by the manufacturer. Verify mechanical operation, insulation resistance, protective relay calibration and operation, and wiring continuity of switchboard assembly. Do not damage generator components during test.

3.6.7.3 Engine-Generator Connection Coupling Test

When the generator provided is a two-bearing machine, inspect and check the engine-generator connection coupling by dial indicator to prove that no misalignment has occurred. Use the dial indicator to measure variation in radial positioning and axial clearance between the coupling halves. Take readings at four points, spaced 90 degrees apart. Align solid couplings and pin-type flexible couplings within a total indicator reading of 0.0005 to 0.001 inch for both parallel and angular misalignment. For gear-type or grid-type couplings, 0.002 inch will be acceptable.

3.6.8 Safety Run Test

For the following tests, repeat the associated safety tests if any parts are changed, or adjustments made to the generator set, its controls, or auxiliaries.

a. Perform and record engine manufacturer's recommended prestarting checks and inspections.

b. Start the engine, record the starting time, make and record engine manufacturer's after-starting checks and inspections during a reasonable warm-up period.

c. Activate the manual emergency stop switch and verify that the engine stops.

d. Remove the high and pre-high lubricating oil temperature sensing elements from the engine and temporarily install a temperature gauge in their normal locations on the engine (required for safety, not for recorded data). Where necessary provide temporary wiring harness to connect the sensing elements to their permanent electrical leads.

e. Start the engine, record the starting time, make and record engine manufacturer's after-starting checks and inspections during a reasonable warm-up period. Operate the engine-generator set at no load until the output voltage and frequency stabilize. Monitor the temporarily installed temperature gauges. If either temperature reading exceeds the value required for an alarm condition, activate the manual emergency stop switch.

f. Immerse the elements in a vessel containing controlled-temperature hot oil and record the temperature at which the pre-high alarm activates and the temperature at which the engine shuts down. Remove the temporary temperature gauges and reinstall the temperature sensors on the engine.

g. Remove the high and pre-high coolant temperature sensing elements from the engine and temporarily install a temperature gauge in their normal locations on the engine (required for safety, not for recorded data). Where necessary provide temporary wiring harness to connect the sensing elements to their permanent electrical leads.

h. Start the engine, record the starting time, make and record engine manufacturer's after-starting checks and inspections during a reasonable warm-up period. Operate the engine generator-set at no load until the output voltage and frequency stabilize.

i. Immerse the elements in a vessel containing controlled-temperature hot oil and record the temperature at which the pre-high alarm activates and the temperature at which the engine shuts down. Remove the temporary temperature gauges and reinstall the temperature sensors on the engine.

j. Start the engine, record the starting time, make and record engine manufacturer's after-starting checks and inspections during a reasonable warm-up period.

k. Operate the engine generator-set for at least 2 hours at 75 percent of Service Load.

l. Verify proper operation and set-points of gauges and instruments.

m. Verify proper operation of ancillary equipment.

n. Manually adjust the governor to increase engine speed past the over-speed limit. Record the RPM at which the engine shuts down.

o. Start the engine, record the starting time, make and record engine manufacturer's after-starting checks and inspections and operate the engine generator-set for at least 15 minutes at 75 percent of Service Load.

p. Manually adjust the governor to increase engine speed to within 2 percent of the over-speed trip speed previously determined and operate at that point for 5 minutes. Manually adjust the governor to the rated frequency.

q. Manually fill the day tank to a level above the overfill limit. Record the level at which the overfill alarm sounds. Verify shutdown of the fuel transfer pump. Drain the day tank down below the overfill limit.

r. Shut down the engine. Remove the time-delay low lube oil pressure alarm bypass and try to start the engine.

s. Attach a manifold to the engine oil system (at the oil pressure sensor port) that contains a shutoff valve in series with a connection for the engine's oil pressure sensor followed by an oil pressure gauge ending with a bleed valve. Move the engine's oil pressure sensor from the engine to the manifold. Open the manifold shutoff valve and close the bleed valve.

t. Start the engine, record the starting time, make and record engine manufacturer's after-starting checks and inspections and operate the engine generator-set for at least 15 minutes at 75 percent of Service Load.

u. Close the manifold shutoff valve. Slowly allow the pressure in the manifold to bleed off through the bleed valve while watching the pressure gauge. Record the pressure at which the engine shuts down. Catch oil spillage from the bleed valve in a container. Add the oil from the container back to the engine, remove the manifold, and reinstall the engine's oil pressure sensor on the engine.

v. Start the engine, record the starting time, make and record engine manufacturer's after-starting checks and inspections and operate the engine generator-set for at least 15 minutes at 100 percent of Service Load. Record the maximum sound level in each frequency band at a distance of 75 feet from the end of the exhaust and air intake piping directly along the path of intake and discharge for horizontal piping; or at a radius of 75 feet from the engine at 45 degrees apart in all directions for vertical piping. If a sound limiting enclosure is provided, modify or replace the enclosure, the muffler, and intake silencer must be modified or replaced as required to meet the sound requirements contained within this specification

w. Manually drain off fuel slowly from the day tank to empty it to below the low fuel level limit and record the level at which the audible alarm sounds. Add fuel back to the day tank to fill it above low level alarm limits.

3.6.9 Performance Tests

In the following tests, where measurements are to be recorded after

stabilization of an engine-generator set parameter (voltage, frequency, current, temperature, etc.), stabilization is considered to have occurred when measurements are maintained within the specified bandwidths or tolerances, for a minimum of four consecutive readings. For the following tests, repeat the associated tests if any parts are changed, or adjustments made to the generator set, its controls, or auxiliaries.

3.6.9.1 Continuous Engine Load Run Test

Test the engine-generator set and ancillary systems at service load to demonstrate durability; verify that heat of extended operation does not adversely affect or cause failure in any part of the system; and check all parts of the system. If the engine load run test is interrupted for any reason, repeat the entire test. Accomplish the engine load run test during daylight hours. After each change in load in the following test, measure the vibration at the end bearings (front and back of engine, outboard end of generator) in the horizontal, vertical, and axial directions. Verify that the vibration is within the allowable range. Take data taken at 15 minute intervals and include the following:

Electrical: Output amperes, voltage, real and reactive power, power factor, frequency.

Pressure: Lube-oil.

Temperature: Coolant, Lube-oil, Exhaust, Ambient.

a. Perform and record engine manufacturer's recommended prestarting checks and inspections. Include as a minimum checking of coolant fluid, fuel, and lube-oil levels.

b. Start the engine, make and record engine manufacturer's after-starting checks and inspections during a reasonable warmup period.

c. Operate the engine generator-set for 2 hours at 75 percent of Service Load.

d. Increase load to 100 percent of Service Load and operate the engine generator-set for 4 hours.

e. For prime rated units, increase load to 110 percent of Service Load and operate the engine generator-set for 2 hours.

f. Decrease load to 100 percent of Service Load and operate the engine generator-set for 2 hours or until all temperatures have stabilized.

g. Remove load from the engine-generator set.

3.6.9.2 Voltage and Frequency Droop Test

For the following steps, verify that the output voltage and frequency return to and stabilize within the specified bandwidth values following each load change. Record the generator output frequency and line-line and line-neutral voltages following each load change.

a. With the generator operating at no load, adjust voltage and frequency to rated voltage and frequency.

b. Increase load to 100 percent of Rated Output Capacity. Record the

generator output frequency and line-line and line-neutral voltages.

c. Calculate the percent droop for voltage and frequency with the following equations.

$$\text{Voltage droop percent} = \frac{\text{No-load volts - rated output capacity volts}}{\text{Rated output capacity volts}} \times 100$$

$$\text{Frequency droop percent} = \frac{\text{No load hertz - rated output capacity hertz}}{\text{Rated output capacity volts}} \times 100$$

d. Repeat steps a. through c. two additional times without making any adjustments.

3.6.9.3 Voltage Regulator Range Test

a. While operating at no load, verify that the voltage regulator adjusts from 90 to 110 percent of rated voltage.

b. Increase load to 100 percent of Rated Output Capacity. Verify that the voltage regulator adjusts from 90 to 110 percent of rated voltage.

3.6.9.4 Governor Adjustment Range Test

a. While operating at no load, verify that the governor adjusts from 90 to 110 percent of rated frequency.

b. Increase load to 100 percent of Rated Output Capacity. Verify that the governor adjusts from 90 to 110 percent of rated frequency.

3.6.9.5 Frequency and Voltage Stability and Transient Response

Verify that the engine-generator set responds to addition and dropping of blocks of load in accordance with the transient response requirements. Document maximum voltage and frequency variation from bandwidth and verify that voltage and frequency return to and stabilize within the specified bandwidth, within the specified response time period. Document results in tabular form and with high resolution, high speed strip chart recorders or comparable digital recorders, as approved by the Contracting Officer. Include the following tabular data:

(1) Ambient temperature (at 15 minute intervals).

(2) Generator output current (before and after load changes).

(3) Generator output voltage (before and after load changes).

(4) Frequency (before and after load changes).

(5) Generator output power (before and after load changes.

(6) Include the actual instrument trace of voltage and frequency in graphic representations showing:

Charts marked at start of test; observed steady-state band; mean of observed band; momentary overshoot and undershoot (generator terminal

voltage and frequency) and recovery time for each load change together with the voltage and frequency maximum and minimum trace excursions for each steady state load condition prior to and immediately following each load change. Generator terminal voltage and frequency transient recovery time for each step load increase and decrease.

a. Perform and record engine manufacturer's recommended prestarting checks and inspections.

b. Start the engine, make and record engine manufacturer's after-starting checks and inspections during a reasonable warm-up period and no load. Verify stabilization of voltage and frequency within specified bandwidths.

c. With the unit at no load, apply the Maximum Step Load Increase.

d. Apply load in steps equal to the Maximum Step Load Increase until the addition of one more step increase will exceed the Service Load.

e. Decrease load to the unit such that addition of the Maximum Step Load Increase will load the unit to 100 percent of Service Load.

f. Apply the Maximum Step Load Increase.

g. Decrease load to zero percent in steps equal to the Maximum Step Load Decrease.

h. Repeat steps c. through g.

3.6.10 Parallel Operation Test

Test the capability of each engine-generator set to parallel and share load with other generator sets, individually and in all combinations. This test must be performed with the voltage regulator and governor adjustment settings used for the Frequency and Voltage Stability and Transient Response test. If settings are changed during the performance of this test, a voltage and frequency stability and transient response test must be performed for each engine generator set using the setting utilized in this test. During operations record load-sharing characteristics of each set in parallel operation. Include the following data:

(1) Ambient temperature (at 15 minute intervals).

(2) Generator output current (before and after load changes).

(3) Generator output voltage (before and after load changes).

(4) Power division and exchange between generator sets.

(5) Real power (watts) and reactive power (vars) on each set.

3.6.10.1 Combinations

Connect each set, while operating at no load, parallel with one other set in the system, operating at service load, until all possible combinations have been achieved. Verify stabilization of voltage and frequency within specified bandwidths and proportional sharing of real and reactive loads. Document stabilization of voltage and frequency within specified

bandwidth, the active power division, active power exchange, reactive power division, and voltage and frequency stability and transient response in the following steps for each combination.

a. Divide the load proportionally between the sets and operate in parallel for 15 minutes.

b. Increase the load, in steps equal to the Maximum Step Increase, until each set is loaded to its service load.

c. Decrease the load, in steps equal to the Maximum Step Decrease, until each set is loaded to approximately 25 percent of its service load.

d. Increase the load, in steps equal to the Maximum Step Increase, until each set is loaded to approximately 50 percent of its service load Verify stabilization of voltage and frequency within specified bandwidths and proportional sharing of real and reactive load.

e. Reduce the sum of the loads on both sets to the output rating of the smaller set.

f. Transfer a load equal to the output rating of the smaller of the 2 sets to and from each set. Verify stabilization of voltage and frequency within specified bandwidths and proportional sharing of real and reactive load.

g. Document the active power division, active power exchange, reactive power division, and voltage and frequency stability and transient response.

3.6.10.2 Multiple Combinations

Connect each set, while operating at no load, parallel with all multiple combinations of all other set in the system, while operating at service load, until all multiple combinations of parallel operations have been achieved.

3.6.11 Parallel Operation Test (Commercial Source)

Connect each set parallel with the commercial power source. Operate in parallel for 15 minutes. Verify stabilization of voltage and frequency within specified bandwidths. Record the output voltage, frequency, and loading to demonstrate ability to synchronize with the commercial power source.

3.6.12 Automatic Operation Tests

Test the automatic operating system to demonstrate automatic starting, loading and unloading, the response to loss of operating engine-generator sets, and paralleling of each engine-generator set. Utilize load banks at the indicated power factor and actual loads to be served for this test, and the loading sequence is the indicated sequence. Record load-sharing characteristics during all operations. Perform this test for a minimum of two successive, successful tests. Include the following data:

(1) Ambient temperature (at 15 minute intervals).

(2) Generator output current (before and after load changes).

(3) Generator output voltage (before and after load changes).

(4) Generator output frequency (before and after load changes).

(5) Power division and exchange between generator sets.

(6) Real and reactive power on each set.

a. Initiate loss of the preferred power source and verify the specified sequence of operation.

b. Verify resetting of automatic starting and transfer logic.

3.6.13 Automatic Operation Tests for Stand-Alone Operation

Test the automatic loading system to demonstrate automatic starting, and loading and unloading of each engine-generator set. Utilize the actual loads to be served for this test, and the loading sequence is the indicated sequence. Perform this test for a minimum of two successive, successful tests. Include the following data:

(1) Ambient temperature (at 15 minute intervals).

(2) Generator output current (before and after load changes).

(3) Generator output voltage (before and after load changes).

(4) Generator output frequency (before and after load changes).

a. Initiate loss of the primary power source and verify automatic sequence of operation.

b. Restore the primary power source and verify sequence of operation.

c. Verify resetting of controls to normal.

3.7 GROUNDING

NFPA 70 and IEEE C2, except that grounding systems must have a resistance to solid earth ground not exceeding 5 ohms.

3.7.1 Grounding Electrodes

. Connect ground conductors to the upper end of ground rods by exothermic weld or compression connector. Provide compression connectors at equipment end of ground conductors.

3.7.2 Engine-Generator Set Grounding

Provide separate copper grounding conductors and connect them to the ground system as indicated. When work in addition to that indicated or specified is required to obtain the specified ground resistance, the provision of the contract covering "Changes" must apply.

3.7.3 Connections

Make joints in grounding conductors by exothermic weld or compression connector.

3.7.4 Grounding and Bonding Equipment

UL 467, except as indicated or specified otherwise.

3.8 START-UP ENGINEER

Provide the services of a qualified factory trained start-up engineer, regularly employed by the engine-generator set manufacturer. The start-up services must include conducting preliminary operations and functional acceptance tests. The start-up engineer must be present at the engine generator set installation-site, full-time, while preliminary operations and functional acceptance tests are being conducted.

3.9 PREREQUISITES FOR FUNCTIONAL ACCEPTANCE TESTING

Completion of the following requirements is mandatory prior to scheduling functional acceptance tests for the engine-generator set and auxiliary equipment.

3.9.1 Generator Sets

Complete as specified in the paragraph ACCEPTANCE CHECKS AND TESTS.

3.9.2 Preliminary Operations

The start-up engineer must conduct manufacturer recommended start-up procedures and tests to verify that the engine-generator set and auxiliary equipment are ready for functional acceptance tests. Give the Contracting Officer 15 days' advance notice that preliminary operations will be conducted. After preliminary operation has been successfully conducted, the start-up engineer will notify the Contracting Officer in writing stating the engine-generator set and auxiliary equipment are ready for functional acceptance tests.

3.9.3 Preliminary Assembled Operation and Maintenance Manuals

Preliminary assembled operation and maintenance manuals must have been submitted to and approved by the Contracting Officer. Manuals must be prepared as specified in the paragraph ASSEMBLED OPERATION AND MAINTENANCE MANUALS.

3.9.4 Functional Acceptance Test Procedure

Test procedure must be prepared by the start-up engineer specifically for the engine-generator set and auxiliary equipment. The test agenda must cover the requirements specified in the paragraph FUNCTIONAL ACCEPTANCE TESTS. The test procedure must indicate in detail how tests are to be conducted. A statement of the tests that are to be performed without indicating how the tests are to be performed is not acceptable. Indicate what work is planned on each workday and identify the calendar dates of the planned workdays. Specify what additional technical support personnel is needed such as factory representatives for major equipment. Specify on which testing workday each technical support personnel is needed. Data recording forms to be used to document test results are to be submitted with the proposed test procedure. A list of test equipment and instruments must also be included in the test procedure.

3.9.5 Test Equipment

Test equipment and instruments must be on hand prior to scheduling field tests or, subject to Contracting Officer approval, evidence must be provided to show that arrangements have been made to have the necessary equipment and instruments on-site prior to field testing.

3.10 FIELD QUALITY CONTROL

Give Contracting Officer 30 days' notice of dates and times scheduled for tests which require the presence of the Contracting Officer. The Contracting Officer will coordinate with the using activity and schedule a time that will eliminate or minimize interruptions and interference with the activity operations. The Contractor must be responsible for costs associated with conducting tests outside of normal working hours and with incorporating special arrangements and procedures, including temporary power conditions. The Contractor must provide labor, equipment, fuel, test load, and consumables required for the specified tests. The test load must be a cataloged product. Calibration of measuring devices and indicating devices must be certified. Refer to Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM, for requirements for a cataloged product. Perform the following field tests.

3.10.1 Acceptance Checks and Tests

Perform in accordance with the manufacturer's recommendations, and include the following visual and mechanical inspections and electrical tests, performed in accordance with NETA ATS.

3.10.1.1 Circuit Breakers - Low Voltage Insulated Case/Molded Case

a. Visual and Mechanical Inspection

(1) Compare nameplate data with specifications and approved shop drawings.

(2) Inspect circuit breaker for correct mounting.

(3) Operate circuit breaker to ensure smooth operation.

(4) Inspect case for cracks or other defects.

(5) Verify tightness of accessible bolted connections and cable connections by calibrated torque-wrench method. Thermo-graphic survey is not required.

(6) Inspect mechanism contacts and arc chutes in unsealed units.

b. Electrical Tests

(1) Perform contact-resistance tests.

(2) Perform insulation-resistance tests.

(3) Adjust breaker(s) for final settings in accordance with engine-generator set manufacturer's requirements.

3.10.1.2 Current Transformers

a. Visual and Mechanical Inspection

(1) Compare equipment nameplate data with specifications and approved shop drawings.

(2) Inspect physical and mechanical condition.

(3) Verify correct connection.

(4) Verify that adequate clearances exist between primary and secondary circuit.

(5) Verify tightness of accessible bolted electrical connections by calibrated torque-wrench method. Thermo-graphic survey is not required.

(6) Verify that all required grounding and shorting connections provide good contact.

b. Electrical Tests

(1) Perform insulation-resistance tests.

(2) Perform polarity tests.

(3) Perform ratio-verification tests.

3.10.1.3 Metering and Instrumentation

a. Visual and Mechanical Inspection

(1) Compare equipment nameplate data with specifications and approved shop drawings.

(2) Inspect physical and mechanical condition.

(3) Verify tightness of electrical connections.

b. Electrical Tests

(1) Determine accuracy of meters at 25, 50, 75, and 100 percent of full scale.

(2) Calibrate watt-hour meters according to manufacturer's published data.

(3) Verify all instrument multipliers.

(4) Electrically confirm that current transformer secondary circuits are intact.

3.10.1.4 Battery Systems

a. Visual and Mechanical Inspection

(1) Compare equipment nameplate data with specifications and approved shop drawings.

(2) Inspect physical and mechanical condition.

(3) Verify tightness of accessible bolted electrical connections by calibrated torque-wrench method. Thermo-graphic survey is not required.

(4) Measure electrolyte specific gravity and temperature and visually check fill level.

(5) Verify adequacy of battery support racks, mounting, anchorage, and clearances.

b. Electrical Tests

(1) Set charger float and equalizing voltage levels.

(2) Verify all charger functions and alarms.

(3) Measure each cell voltage and total battery voltage with charger energized and in float mode of operation.

(4) Perform a capacity load test.

3.10.1.5 Engine-Generator Set

a. Visual and Mechanical Inspection

(1) Compare equipment nameplate data with specifications and approved shop drawings.

(2) Inspect physical and mechanical condition.

(3) Inspect for correct anchorage and grounding.

b. Electrical and Mechanical Tests

(1) Perform an insulation-resistance test on generator winding with respect to ground. Calculate polarization index.

(2) Perform phase rotation test to determine compatibility with load requirements.

3.10.1.6 Grounding System

a. Visual and Mechanical Inspection

(1) Inspect ground system for compliance with contract plans and specifications.

b. Electrical Tests

(1) Perform ground-impedance measurements utilizing the fall-of-potential method defined in IEEE 81. On systems consisting of interconnected ground rods, perform tests after interconnections are complete. Take measurements in normally dry weather, not less than 48 hours after rainfall. Provide site diagram indicating location of test probes with associated distances, and provide a plot of resistance vs. distance.

3.10.2 Functional Acceptance Tests

The tests must be performed by the start-up engineer. Upon successful test completion, the start-up engineer must provide the Contracting Officer with a written test report within 15 calendar days showing the tests performed and the results of each test. The report must include the completed approved test data forms and certification from the start-up engineer that the test results fall within the manufacturer's recommended limits and meet the specified requirements performance. The report must be dated and signed by the start-up engineer, and submitted for approval by the Contracting Officer. The Contracting Officer will witness final acceptance tests. Testing must include, but not be limited to, the following:

a. Verify proper functioning of each engine protective shutdown device and pre-shutdown alarm device. Testing of the devices must be accomplished by simulating device actuation and observing proper alarm and engine shutdown operation.

b. Verify proper functioning of the engine over-speed trip device. Testing of the over-speed trip device must be accomplished by raising the speed of the engine-generator set until an over-speed trip is experienced.

c. Verify proper functioning of the crank cycle/terminate relay. Testing of the relay must be accomplished by engaging the starter motor with the engine being prevented from running. Observe the complete crank/rest cycle as described in the paragraph STARTING SYSTEM.

d. Verify proper functioning of the following automatic and manual operations. Testing must include, but not be limited to, the following:

   (1) Loss of Utility: Initiate a normal power failure with connected test load of rated kW at 1.0 power factor. Record time delay on start, cranking time until engine starts and runs, time to come up to operating speed, voltage and frequency overshoot, and time to achieve steady state conditions with all switches transferred to emergency position.

   (2) Return of Utility: Return normal power and record time delay on retransfer for each automatic transfer switch, and time delay on engine cool-down and shutdown.

   (3) Manual starting.

   (4) Emergency stop.

e. Operate the engine-generator set at rated current (amperes) until the jacket water temperature stabilizes. Stabilization will be considered to have occurred when three consecutive temperature readings remain unchanged. Continue to operate the generator set for an additional 2 hours. Record instrument readings for terminal voltage, line current, frequency (Hz), engine speed rpm, lubricating oil pressure, jacket water temperature, and ambient temperature at 5 minute intervals for first 15 minutes and at 15 minute intervals thereafter.

3.11 DEMONSTRATION

Upon completion of the work and at a time approved by the Contracting Officer, the Contractor must provide instructions by a qualified instructor to the Government personnel in the proper operation and maintenance of the equipment. Government personnel must receive training comparable to the equipment manufacturer's factory training. The duration of instruction must be for not less than one 8 hour working day for instruction of operating personnel and not less than one 8 hour working day for instruction of maintenance personnel.

3.11.1 Instructor's Qualification Resume

Instructors must be regular employees of the engine-generator set manufacturer. The instruction personnel provided to satisfy the requirements above must be factory certified by the related equipment manufacturer to provide instruction services. Submit the name and qualification resume of instructor to the Contracting Officer for approval.

3.11.2 Training Plan

Submit training plan 30 calendar days prior to training sessions. Training plan must include scheduling, content, outline, and training material (handouts). Content must include, but not be limited to, the following:

3.11.2.1 Operating Personnel Training

This instruction includes operating the engine-generator set, auxiliary equipment including automatic transfer switches in all modes, and the use of all functions and features specified.

3.11.2.2 Maintenance Personnel Training

Training must include mechanical, hydraulic, electrical, and electronic instructions for the engine-generator set and auxiliary equipment including automatic transfer switches.

a. Mechanical Training: Must include at least the following:

(1) A review of mechanical diagrams and drawings.

(2) Component location and functions.

(3) Troubleshooting procedures and techniques.

(4) Repair procedures.

(5) Assembly/disassembly procedures.

(6) Adjustments (how, when, and where).

(7) Preventive maintenance procedures.

(8) Review of flow diagram.

(9) Valve locations and function.

(10) Valve and hydraulic equipment adjustment and maintenance

procedures.

(11) Hydraulic system maintenance and servicing.

(12) Lubrication points, type, and recommended procedures and frequency.

b. Electrical and Electronic Maintenance Training: Must include at least the following:

(1) A review of electrical and electronic systems including wiring diagrams and drawings.

(2) Troubleshooting procedures for the machine and control systems.

(3) Electrical and electronic equipment servicing and care.

(4) Use of diagnostics to locate the causes of malfunction.

(5) Procedures for adjustments (locating components, adjustments to be made, values to be measured, and equipment required for making adjustments).

(6) Maintenance and troubleshooting procedures for microprocessor or minicomputer where applicable.

(7) Circuit board repair procedures where applicable (with schematics provided).

(8) Use of diagnostic tapes.

(9) Recommended maintenance servicing and repair for motors, switches, relays, solenoids, and other auxiliary equipment and devices.

3.12 ONSITE TRAINING

Conduct a training course for the operating staff as designated by the Contracting Officer. The training period must start after the system is functionally completed but prior to final acceptance.

a. Submit a letter giving the date proposed for conducting the onsite training course, the agenda of instruction, a description of the digital video recording to be provided. The course instructions must cover pertinent points involved in operating, starting, stopping, servicing the equipment, as well as major elements of the operation and maintenance manuals. Additionally, the course instructions must demonstrate routine maintenance procedures as described in the operation and maintenance manuals.

b. Submit a digital video recording of the manufacturers operating and maintenance training course.

c. One full size reproducible Mylar ach drawing must accompany the booklets. Mylars must be rolled and placed in a heavy cardboard tube with threaded caps on each end. The manual must include step-by-step procedures for system startup, operation, and shutdown; drawings, diagrams, and single-line schematics to illustrate and define the electrical, mechanical, and hydraulic systems together with their controls, alarms, and safety systems; the manufacturer's name, model

number, and a description of equipment in the system. The instructions must include procedures for interface and interaction with related systems to include automatic transfer switches and fire alarm/suppression systems. Each booklet must include a CD containing an ASCII file of the procedures.

d. Provide approved operation and maintenance manuals for the training course. Post approved instructions prior to the beginning date of the training course. Coordinate the training course schedule with the using service's work schedule, and submit for approval 14 days prior to beginning date of proposed beginning date of training.

3.13 INSTALLATION

Installation must conform to the applicable requirements of IEEE C2, NFPA 30, NFPA 37, and NFPA 70.

3.14 FINAL TESTING AND INSPECTION

a. Start the engine, record the starting time, make and record all engine manufacturer's after-starting checks and inspections during a reasonable warm-up period.

b. Increase the load in steps no greater than the Maximum Step Load Increase to 100 percent of Service Load, and operate the engine-generator set for at least 30 minutes. Measure the vibration at the end bearings (front and back of engine, outboard end of generator) in the horizontal, vertical, and axial directions. Verify that the vibration is within the same range as previous measurements and is within the required range.

c. Remove load and shut down the engine-generator set after the recommended cool down period.

d. Remove the lube oil filter and have the oil and filter examined by the engine manufacturer for excessive metal, abrasive foreign particles, etc. Verify any corrective action for effectiveness by running the engine for 8 hours at Service Load, then re-examine the oil and filter.

e. Remove the fuel filter and examine the filter for trash, abrasive foreign particles, etc.

f. Visually inspect and check engine and generator mounting bolts for tightness and visible damage.

g. Replace air, oil, and fuel filters with new filters.

3.15 MANUFACTURER'S FIELD SERVICE

The engine generator-set manufacturer must furnish a qualified representative to supervise the installation of the engine generator-set, assist in the performance of the onsite tests, and instruct personnel as to the operational and maintenance features of the equipment.

3.16 POSTED DATA AND INSTRUCTIONS

Post Data and Instructions prior to field acceptance testing of the engine generator set. Provide two sets of instructions/data, typed and framed under weatherproof laminated plastic, and post side-by-side where

directed. Include a one-line diagram, wiring and control diagrams and a complete layout of the system in the first set. Include the condensed operating instructions describing manufacturer's pre-start checklist and precautions; startup procedures for test-mode, manual-start mode, and automatic-start mode (as applicable); running checks, procedures, and precautions; and shutdown procedures, checks, and precautions in the second set. Submit posted data including wiring and control diagrams showing the key mechanical and electrical control elements, and a complete layout of the entire system.

a. Include procedures for interrelated equipment (such as heat recovery systems, co-generation, load-shedding, and automatic transfer switches). Provide two sets of typed instructions/data in 8-1/2 x 11 inch format, laminated in weatherproof plastic, and placed in three-ring vinyl binders. Place the binders as directed by the Contracting Officer. Provide the instructions prior to acceptance of the engine generator set installation.

b. Include a one-line diagram, wiring and control diagrams and a complete layout of the system in the first set. Include the condensed operating instructions describing manufacturer's pre-start checklist and precautions; startup procedures for test-mode, manual-start mode, and automatic-start mode (as applicable); running checks, procedures, and precautions; and shutdown procedures, checks, and precautions in the second set. Include procedures for interrelated equipment (such as heat recovery systems, co-generation, load-shedding, and automatic transfer switches).

c. Submit instructions including: the manufacturers pre-start checklist and precautions; startup procedures for test-mode, manual-start mode, and automatic-start mode (as applicable); running checks, procedures, and precautions; and shutdown procedures, checks, and precautions. Include procedures for interrelated equipment (such as heat recovery systems, co-generation, load-shedding, and automatic transfer switches). Provide weatherproof instructions, laminated in plastic, and post where directed.

3.17 ACCEPTANCE

Submit drawings which accurately depict the as-built configuration of the installation, upon acceptance of the engine-generator set installation. Revise layout drawings to reflect the as-built conditions and submit them with the as-built drawings. Final acceptance of the engine-generator set will not be given until the Contractor has successfully completed all tests and all defects in installation material or operation have been corrected.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 26 - ELECTRICAL

SECTION 26 41 00

LIGHTNING PROTECTION SYSTEM

PART 1 GENERAL

1.1 REFERENCES
1.2 RELATED REQUIREMENTS
1.2.1 Verification of Dimensions
1.2.2 System Requirements
1.2.3 Lightning Protection System Installers Documentation
1.3 SUBMITTALS
1.4 QUALITY ASSURANCE
1.4.1 Installation Drawings
1.4.1.1 Overall System Drawing
1.4.1.2 Major Components
1.4.2 Component UL Listed and Labeled
1.4.3 Lightning Protection and Grounding System Test Plan
1.4.4 Lightning Protection System Inspection Certificate
1.5 SITE CONDITIONS

PART 2 PRODUCTS

2.1 MATERIALS
2.1.1 Main and Bonding Conductors
2.1.2 Copper Only
2.2 COMPONENTS
2.2.1 Air Terminals
2.2.2 Ground Rods
2.2.3 Grounding Plates
2.2.4 Connections and Terminations
2.2.5 Connector Fittings

PART 3 EXECUTION

3.1 INTEGRAL SYSTEM
3.1.1 Roof-Mounted Components
3.1.1.1 Air Terminals
3.1.1.2 Roof Conductors
3.1.2 Down Conductors
3.1.3 Ground Connections
3.1.4 Grounding Electrodes
3.1.5 Grounding Plates
3.2 APPLICATIONS
3.2.1 Nonmetallic Exterior Walls with Metallic Roof
3.2.2 Personnel Ramps and Covered Passageways
3.3 INTERFACE WITH OTHER STRUCTURES
3.3.1 Fences
3.4 RESTORATION
3.5 FIELD QUALITY CONTROL

3.5.1 Lightning Protection and Grounding System Test

-- End of Section Table of Contents --

SECTION 26 41 00

LIGHTNING PROTECTION SYSTEM

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 81	(2012) Guide for Measuring Earth Resistivity, Ground Impedance, and Earth Surface Potentials of a Ground System

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National Electrical Code
NFPA 780	(2023) Standard for the Installation of Lightning Protection Systems

U.S. AIR FORCE (USAF)

AFI 32-1065	(2017) Grounding Systems

UNDERWRITERS LABORATORIES (UL)

UL 96	(2016) UL Standard for Safety Lightning Protection Components
UL 467	(2022) UL Standard for Safety Grounding and Bonding Equipment
UL Electrical Construction	(2012) Electrical Construction Equipment Directory

1.2 RELATED REQUIREMENTS

1.2.1 Verification of Dimensions

Confirm all details of work, verify all dimensions in field, and advise Contracting Officer of any discrepancy before performing work. Obtain prior approval of Contracting Officer before making any departures from the design.

1.2.2 System Requirements

Provide a system furnished under this specification consisting of the latest UL Listed products of a manufacturer regularly engaged in production of lightning protection system components. Comply with NFPA 70, NFPA 780, and UL 96.

1.2.3 Lightning Protection System Installers Documentation

Provide documentation showing that the installer is certified with a commercial third-party inspection company whose sole work is lightning protection, or is a UL Listed Lightning Protection Installer. In either case, the documentation must show that they have completed and passed the requirements for certification or listing, and have a minimum of 2 years documented experience installing lightning protection systems for DoD projects of similar scope and complexity.

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Overall lightning protection system; G

Each major component; G

SD-06 Test Reports

Lightning Protection and Grounding System Test Plan; G

Lightning Protection and Grounding System Test; G

SD-07 Certificates

Lightning Protection System Installers Documentation; G

Component UL Listed and Labeled; G

Lightning protection system inspection certificate; G

Roof manufacturer's warranty; G

1.4 QUALITY ASSURANCE

In each standard referred to herein, consider the advisory provisions to be mandatory, as though the word "shall" or "must" has been substituted for "should" wherever it appears. Interpret references in these standards to "authority having jurisdiction," or words of similar meaning, to mean Contracting Officer.

1.4.1 Installation Drawings

1.4.1.1 Overall System Drawing

Submit installation shop drawing for the overall lightning protection system. Include on the drawings the physical layout of the equipment (plan view and elevations), mounting details, relationship to other parts of the work, and wiring diagrams.

1.4.1.2 Major Components

Submit detail drawings for each major component including manufacturer's descriptive and technical literature, catalog cuts, and installation instructions.

1.4.2 Component UL Listed and Labeled

Submit proof of compliance that components are UL Listed and Labeled. Listing alone in UL Electrical Construction, which is the UL Electrical Construction Directory, is not acceptable evidence. In lieu of Listed and Labeled, submit written certificate from an approved, nationally recognized testing organization equipped to perform such services, stating that items have been tested and conform to requirements and testing methods of Underwriters Laboratories.

1.4.3 Lightning Protection and Grounding System Test Plan

Provide a lightning protection and grounding system test plan. Detail both the visual inspection and electrical testing of the system and components in the test plan. Identify (number) the system test points/locations along with a listing or description of the item to be tested and the type of test to be conducted. As a minimum, include a sketch of the facility and surrounding lightning protection system as part of the specific test plan for each structure. Include the requirements specified in paragraph, "Testing of Integral Lightning Protection System" in the test plan.

1.4.4 Lightning Protection System Inspection Certificate

Provide certification from a commercial third-party inspection company whose sole work is lightning protection, stating that the lightning protection system complies with NFPA 780 and AFI 32-1065. Third party inspection company cannot be the system installer or the system designer. Alternatively, provide a UL Lightning Protection Inspection Master Label Certificate for each facility indicating compliance to NFPA 780 and AFI 32-1065. In either case, AFI 32-1065 takes precedence over NFPA 780, whether or not it is more stringent.

Inspection must cover every connection, air terminal, conductor, fastener, accessible grounding point and other components of the lightning protection system to ensure 100% system compliance. This includes witnessing the tests for the resistance measurements for ground rods with test wells, and for continuity measurements for bonds. It also includes verification of proper surge protective devices for power, data and telecommunication systems. Random sampling or partial inspection of a facility is not acceptable.

1.5 SITE CONDITIONS

Confirm all details of work, verify all dimensions in field, and advise Contracting Officer of any discrepancy before performing work. Obtain prior approval of Contracting Officer before changing the design.

PART 2 PRODUCTS

2.1 MATERIALS

Do not use a combination of materials that forms an electrolytic couple of

such nature that corrosion is accelerated in the presence of moisture unless moisture is permanently excluded from the junction of such metals. Where unusual conditions exist which would cause corrosion of conductors, provide conductors with protective coatings, such as tin or lead, or oversize conductors. Where a mechanical hazard is involved, increase conductor size to compensate for the hazard or protect conductors. When metallic conduit or tubing is provided, electrically bond conductor to conduit or tubing at the upper and lower ends by clamp type connectors or welds (including exothermic). All lightning protection components, such as bonding plates, air terminals, air terminal supports and braces, chimney bands, clips, connector fittings, and fasteners are to comply with the requirements of UL 96 classes as applicable.

2.1.1 Main and Bonding Conductors

NFPA 780 and UL 96 Class I, Class II, or Class II modified materials as applicable.

2.1.2 Copper Only

Provide copper conductors, except where aluminum conductors are required for connection to aluminum equipment.

2.2 COMPONENTS

2.2.1 Air Terminals

Provide solid air terminals with a blunt tip. Tubular air terminals are not permitted. Support air terminals more than 24 inches in length by suitable brace, supported at not less than one-half the height of the terminal.

2.2.2 Ground Rods

Provide ground rods made of solid copper conforming to conform to UL 467. Provide ground rods that are not less than 3/4 inch in diameter and 10 feet in length. Do not mix ground rods of copper-clad steel or solid copper on the job.

2.2.3 Grounding Plates

Provide grounding plates made of solid copper conforming to UL 96.

2.2.4 Connections and Terminations

Provide connectors for splicing conductors that conform to UL 96, class as applicable. Conductor connections can be made by clamps or welds (including exothermic). Provide style and size connectors required for the installation.

2.2.5 Connector Fittings

Provide connector fittings for "end-to-end", "Tee", or "Y" splices that conform to NFPA 780 and UL 96.

PART 3 EXECUTION

3.1 INTEGRAL SYSTEM

Provide a lightning protection system that meets the requirements of NFPA 780. Lightning protection system consists of air terminals, roof conductors, down conductors, ground connections, grounding electrodes and ground ring electrode conductor. Expose conductors on the structures except where conductors are required to be in protective sleeves. Bond secondary conductors with grounded metallic parts within the building. Make interconnections within side-flash distances at or below the level of the grounded metallic parts.

3.1.1 Roof-Mounted Components

Coordinate with the roofing manufacturer and provide certification that the roof manufacturer's warranty is not violated by the installation methods for air terminals and roof conductors.

3.1.1.1 Air Terminals

In areas of snow or constant wind, ensure that a section of roofing material (minimum dimensional area of 1 square foot) is first glued to the roof and then the air terminal is glued to it unless the roof manufacturer recommends another solution. Use a standing seam base for installation of air terminals on a standing seam metal roof that does not produce any roof penetrations.

3.1.1.2 Roof Conductors

Use a standing seam base for installation of roof conductors on a standing seam metal roof that does not produce any roof penetrations.

3.1.2 Down Conductors

Protect exposed down conductors from physical damage as required by NFPA 780. Use Schedule 80 PVC to protect down conductors. Paint the Schedule 80 PVC to match the surrounding surface with paint that is approved for use on PVC. Down conductors are to be concealed within the wall cavities.

3.1.3 Ground Connections

Attach each down conductor and ground ring electrode to ground rods by welding (including exothermic), brazing, or compression. All connections to ground rods below ground level must be by exothermic weld connection or with a high compression connection using a hydraulic or electric compression tool to provide the correct circumferential pressure. Accessible connections above ground level and in test wells can be accomplished by mechanical clamping.

3.1.4 Grounding Electrodes

Extend driven ground rods vertically into the existing undisturbed earth for a distance of not less 10 feet. Set ground rods not less than 3 feet nor more than 8 feet, from the structure foundation, and at least beyond the drip line for the facility. After the completed installation, measure the total resistance to ground using the fall-of-potential method described in IEEE 81. Maximum allowed resistance of a driven ground rod

is 25 ohms, under normally dry conditions . Contact the Contracting Officer for direction on how to proceed when two of any three ground rods, driven not less than 10 feet into the ground, a minimum of 10 feet apart, and equally spaced around the perimeter, give a combined value exceeding 50 ohms immediately after having driven. For ground ring electrode, provide continuous No. 1/0 bare stranded copper cable. Lay ground ring electrode around the perimeter of the structure in a trench not less than 3 feet nor more than 8 feet from the nearest point of the structure foundation, and at least beyond the drip line for the facility. Install ground ring electrode to a minimum depth of 30 inches. Install a ground ring electrode in earth undisturbed by excavation, not earth fill, and do not locate beneath roof overhang, or wholly under paved areas or roadways where rainfall cannot penetrate to keep soil moist in the vicinity of the cable.

3.1.5 Grounding Plates

Provide a grounding plate for each down conductor. Set grounding plates not less than 3 feet nor more than 8 feet, from the structure foundation, and at least beyond the drip line for the facility. Grounding plate is to be buried as deeply in the existing dirt as local conditions allow, without exceeding 10 feet in depth.

3.2 APPLICATIONS

3.2.1 Nonmetallic Exterior Walls with Metallic Roof

Bond metal roof sections together which are insulated from each other so that they are electrically continuous, having a surface contact of at least 3 square inches.

3.2.2 Personnel Ramps and Covered Passageways

Place a down conductor and a driven ground at one of the corners where the ramp connects to each building or structure. Connect down conductor and driven ground to the ground ring electrode or nearest ground connection of the building or structure. Where buildings or structures and connecting ramps are clad with metal, separately bond the metal of the buildings and ramps to a down conductor as close to grade as possible.

3.3 INTERFACE WITH OTHER STRUCTURES

3.3.1 Fences

Bond metal fence and gate systems to the lightning protection system whenever the fence or gate is within 6 feet of any part of the lightning protection system in accordance with ANSI C2.

3.4 RESTORATION

Where sod has been removed, place sod as soon as possible after completing the backfilling. Restore, to original condition, the areas disturbed by trenching, storing of dirt, cable laying, and other work. Overfill to accommodate for settling. Include necessary topsoil, fertilizing, liming, seeding, sodding, sprigging or mulching in any restoration. Maintain disturbed surfaces and replacements until final acceptance.

3.5 FIELD QUALITY CONTROL

3.5.1 Lightning Protection and Grounding System Test

Test the lightning protection and grounding system to ensure continuity is not in excess of 1 ohm and that resistance to ground is not in excess of 25 ohms. Provide documentation for the measured values at each test point. Test the ground rod for resistance to ground before making connections to the rod. Tie the grounding system together and test for resistance to ground. Make resistance measurements in dry weather, not earlier than 48 hours after rainfall. Include in the written report: locations of test points, measured values for continuity and ground resistances, and soil conditions at the time that measurements were made. Submit results of each test to the Contracting Officer.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 26 - ELECTRICAL

SECTION 26 51 00

INTERIOR LIGHTING

PART 1 GENERAL

1.1 REFERENCES
1.2 RELATED REQUIREMENTS
1.3 DEFINITIONS
1.4 SUBMITTALS
1.5 QUALITY ASSURANCE
1.5.1 Luminaire Drawings
1.5.2 Luminaire Design Data
1.5.3 ANSI/IES LM-79 Test Report
1.5.4 ANSI/IES LM-80 Test Report
1.5.5 ANSI/IES TM-21 Test Report
1.5.6 ANSI/IES TM-30 Test Report
1.5.7 LED Driver and Dimming Switch Compatibility Certificate
1.5.8 Photometric Plan
1.5.8.1 Computer-generated Photometric Plans
1.5.8.2 Schematic Photometric Plan Calculations
1.5.8.3 Final Photometric Plan Calculations
1.5.9 Occupancy/Vacancy Sensor Coverage Layout
1.5.10 Test Laboratories
1.5.11 Regulatory Requirements
1.5.12 Standard Products
1.5.12.1 Alternative Qualifications
1.5.12.2 Material and Equipment Manufacturing Date
1.6 WARRANTY
1.6.1 Luminaire Warranty
1.6.2 Lighting Controls Warranty
1.7 OPERATION AND MAINTENANCE MANUALS
1.7.1 Lighting System
1.7.2 Lighting Control System

PART 2 PRODUCTS

2.1 PRODUCT COORDINATION
2.2 LUMINAIRES
2.2.1 Luminaires
2.2.2 Luminaires for Hazardous Locations
2.3 LIGHT SOURCES
2.3.1 LED Light Sources
2.3.1.1 Linear LED Lamps
2.4 LED DRIVERS
2.4.1 Remote LED Drivers
2.5 LIGHTING CONTROLS
2.5.1 System
2.5.1.1 Localized Control Systems
2.5.1.1.1 Local Area Controller

2.5.1.2 Centralized Control Systems
2.5.1.2.1 Gateway
2.5.2 Devices
2.5.2.1 Switches
2.5.2.2 Digital Switch Timers
2.5.2.3 Wall Box Dimmers
2.5.2.4 Scene Wallstations
2.5.2.5 Occupancy/Vacancy Sensors
2.5.2.5.1 Integrated Sensors
2.5.2.5.2 Power Packs
2.6 EXIT AND EMERGENCY LIGHTING EQUIPMENT
2.6.1 Exit Signs
2.6.1.1 Exit Signs with Battery Backup
2.6.2 LED Emergency Drivers
2.6.3 Self-Diagnostic Circuitry for LED Drivers
2.7 LUMINAIRE MOUNTING ACCESSORIES
2.7.1 Suspended Luminaires
2.7.2 Recess and Surface Mounted Luminaires
2.7.3 Luminaire Support Hardware
2.7.3.1 Wire
2.7.3.2 Wire for Humid Spaces
2.7.3.3 Threaded Rods
2.7.3.4 Straps
2.7.4 Power Hook Luminaire Hangers
2.8 EQUIPMENT IDENTIFICATION
2.8.1 Manufacturer's Nameplate
2.8.2 Labels
2.9 FACTORY APPLIED FINISH

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Light Sources
3.1.2 Luminaires
3.1.2.1 Suspended Luminaires
3.1.2.2 Recessed and Semi-Recessed Luminaires
3.1.3 LED Drivers
3.1.4 Exit Signs
3.1.5 Lighting Controls
3.1.5.1 Scene Wallstations
3.1.5.2 Occupancy/Vacancy Sensors
3.1.5.3 Photosensors
3.2 FIELD QUALITY CONTROL
3.2.1 Tests
3.2.1.1 Lighting Control Verification Tests
3.2.1.2 Emergency Lighting Test
3.3 CLOSEOUT ACTIVITIES
3.3.1 Commissioning
3.3.2 Training
3.3.2.1 Maintenance Staff Training
3.3.2.2 End-User Training

-- End of Section Table of Contents --

SECTION 26 51 00

INTERIOR LIGHTING

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ASTM INTERNATIONAL (ASTM)

ASTM A580/A580M	(2018) Standard Specification for Stainless Steel Wire
ASTM A641/A641M	(2019) Standard Specification for Zinc-Coated (Galvanized) Carbon Steel Wire
ASTM A653/A653M	(2020) Standard Specification for Steel Sheet, Zinc-Coated (Galvanized) or Zinc-Iron Alloy-Coated (Galvannealed) by the Hot-Dip Process
ASTM A1008/A1008M	(2021a) Standard Specification for Steel, Sheet, Cold-Rolled, Carbon, Structural, High-Strength Low-Alloy, High-Strength Low-Alloy with Improved Formability, Solution Hardened, and Bake Hardenable
ASTM B164	(2003; R 2014) Standard Specification for Nickel-Copper Alloy Rod, Bar, and Wire
ASTM B633	(2019) Standard Specification for Electrodeposited Coatings of Zinc on Iron and Steel
ASTM D4674 REV A	(2002; R 2010) Standard Practice for Accelerated Testing for Color Stability of Plastics Exposed to Indoor Office Environments

EUROPEAN UNION (EU)

Directive 2011/65/EU	(2011) Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment

ILLUMINATING ENGINEERING SOCIETY (IES)

ANSI/IES LM-79	(2019) Approved Method: Electrical and Photometric Measurements of Solid State Lighting Products
ANSI/IES LM-80	(2020) Approved Method: Measuring Luminous

	Flux and Color Maintenance of LED Packages, Arrays and Modules
ANSI/IES LS-1	(2020) Lighting Science: Nomenclature and Definitions for Illuminating Engineering
ANSI/IES TM-15	(2020) Technical Memorandum: Luminaire Classification System for Outdoor Luminaires
ANSI/IES TM-21	(2021) Technical Memorandum: Projecting Long-TermLuminous, Photon, and Radiant Flux Maintenance of LED Light Sources
ANSI/IES TM-30	(2020) Technical Memorandum: IES Method for Evaluating Light Source Color Rendition
IES Lighting Library	IES Lighting Library

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 100	(2000; Archived) The Authoritative Dictionary of IEEE Standards Terms
IEEE C2	(2023) National Electrical Safety Code
IEEE C62.41	(1991; R 1995) Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

ANSI C78.54	(2019) Specification Sheet for Tubular Fluorescent Replacement and Retrofit LED Lamps
NEMA 77	(2017) Temporal Light Artifacts: Test Methods and Guidance for Acceptance Criteria
NEMA 250	(2020) Enclosures for Electrical Equipment (1000 Volts Maximum)
NEMA ANSLG C78.377	(2017) Electric Lamps— Specifications for the Chromaticity of Solid State Lighting Products
NEMA C82.77-10	(2020) Harmonic Emission Limits - Related Power Quality Requirements
NEMA SSL 1	(2016) Electronic Drivers for LED Devices, Arrays, or Systems
NEMA SSL 3	(2011) High-Power White LED Binning for General Illumination
NEMA SSL 7A	(2015) Phase-Cut Dimming for Solid State Lighting: Basic Compatibility

NEMA WD 1	(1999; R 2020) Standard for General Color Requirements for Wiring Devices
NEMA WD 7	(2011; R 2016; R 2021) Occupancy Motion Sensors Standard

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National Electrical Code
NFPA 101	(2021; TIA 21-1) Life Safety Code

U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)

47 CFR 15	Radio Frequency Devices

UNDERWRITERS LABORATORIES (UL)

UL 20	(2018; Reprint Jan 2021) UL Standard for Safety General-Use Snap Switches
UL 94	(2013; Reprint Apr 2022) UL Standard for Safety Tests for Flammability of Plastic Materials for Parts in Devices and Appliances
UL 508	(2018; Reprint Jul 2021) UL Standard for Safety Industrial Control Equipment
UL 844	(2012; Reprint Oct 2021) UL Standard for Safety Luminaires for Use in Hazardous (Classified) Locations
UL 916	(2015; Reprint Oct 2021) UL Standard for Safety Energy Management Equipment
UL 924	(2016; Reprint May 2020) UL Standard for Safety Emergency Lighting and Power Equipment
UL 1472	(2015) UL Standard for Safety Solid-State Dimming Controls
UL 1598	(2021; Reprint Jun 2021) Luminaires
UL 1993	(2017) Self-Ballasted Lamps and Lamp Adapters
UL 2043	(2013) Fire Test for Heat and Visible Smoke Release for Discrete Products and Their Accessories Installed in Air-Handling Spaces
UL 8750	(2015; Reprint Sep 2021) UL Standard for Safety Light Emitting Diode (LED) Equipment for Use in Lighting Products

1.2 RELATED REQUIREMENTS

Materials not considered to be luminaires, luminaire accessories, or lighting equipment are specified in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Commissioning requirements for Army and Air Force projects are specified in Section 01 91 00.15 10 TOTAL BUILDING COMMISSIONING. Emergency lighting requirements are specified in Section 26 52 00.00 40 EMERGENCY LIGHTING.

1.3 DEFINITIONS

a. Unless otherwise specified or indicated, electrical and electronics terms used in these specifications and on the drawings, must be as defined in IEEE 100 and ANSI/IES LS-1.

b. For LED luminaire light sources, "Useful Life" is the operating hours before reaching 70 percent of the initial rated lumen output (L70) with no catastrophic failures under normal operating conditions. This is also known as 70 percent "Rated Lumen Maintenance Life" as defined in ANSI/IES LM-80.

c. For LED luminaires, "Luminaire Efficacy" (LE) is the appropriate measure of energy efficiency, measured in lumens/watt. This is gathered from LM-79 data for the luminaire, in which absolute photometry is used to measure the lumen output of the luminaire as one entity, not the source separately and then the source and housing together.

d. Total harmonic distortion (THD) is the root mean square (RMS) of all the harmonic components divided by the total fundamental current.

1.4 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Luminaire Drawings; G

Occupancy/Vacancy Sensor Coverage Layout; G; S

Lighting Control System One-Line Diagram; G

Sequence of Operation for Lighting Control System; G

SD-03 Product Data

Luminaires; G

Light Sources; G

LED Drivers; G

Luminaire Warranty; G

Lighting Controls Warranty; G

Local Area Controller; G

Gateway; G

Switches; G

Digital Switch Timers; G

Wall Box Dimmers; G

Scene Wallstations; G

Occupancy/Vacancy Sensors; G

Power Packs; G

Power Hook Luminaire Hangers; G

Exit Signs; G

Emergency Drivers; G

Linear LED Lamps; G

SD-05 Design Data

Luminaire Design Data; G

Photometric Plan; G

SD-06 Test Reports

ANSI/IES LM-79 Test Report; G

ANSI/IES LM-80 Test Report; G

ANSI/IES TM-21 Test Report; G

ANSI/IES TM-30 Test Report; G

Occupancy/Vacancy Sensor Verification Test; G

Photosensor Verification Test; G

SD-07 Certificates

LED Driver and Dimming Switch Compatibility Certificate; G

SD-10 Operation and Maintenance Data

Lighting System, Data Package 5; G

Lighting Control System, Data Package 5; G

Maintenance Staff Training Plan; G

End-User Training Plan; G

1.5 QUALITY ASSURANCE

Data, drawings, and reports must employ the terminology, classifications and methods prescribed by the IES Lighting Library as applicable, for the lighting system specified.

1.5.1 Luminaire Drawings

Include dimensions, accessories installation details, and construction details. Photometric data, including CRI, CCT, LED driver type, zonal lumen data, and candlepower distribution data must accompany shop drawings.

1.5.2 Luminaire Design Data

a. Provide safety certification and file number for the luminaire family that must be listed, labeled, or identified in accordance with the NFPA 70. Applicable testing bodies are determined by the US Occupational Safety Health Administration (OSHA) as Nationally Recognized Testing Laboratories (NRTL) and include: CSA (Canadian Standards Association), ETL (Edison Testing Laboratory), and UL (Underwriters Laboratories).

b. Provide long term lumen maintenance projections for each LED luminaire in accordance with ANSI/IES TM-21. Data used for projections must be obtained from testing in accordance with ANSI/IES LM-80.

1.5.3 ANSI/IES LM-79 Test Report

Submit test report on manufacturer's standard production model of specified luminaire. Testing must be performed at the same operating drive current as specified luminaire. Include all applicable and required data in IES format as outlined under "14.0 Test Report" in ANSI/IES LM-79.

1.5.4 ANSI/IES LM-80 Test Report

Submit report on manufacturer's standard production LED light source (package, array, or module) of specified luminaire. Testing must be performed at the same operating drive current as specified luminaire. Include all applicable and required data as outlined under "8.0 Test Report" in ANSI/IES LM-80.

1.5.5 ANSI/IES TM-21 Test Report

Submit test report on manufacturer's standard production LED light source (package, array, or module) of specified luminaire. Testing must be performed at the same operating drive current as specified luminaire. Include all applicable and required data, as well as required interpolation information as outlined under "7.0 Report" in ANSI/IES TM-21.

1.5.6 ANSI/IES TM-30 Test Report

Submit color vector graphic in accordance with ANSI/IES TM-30 on manufacturer's standard production LED light source (package, array, or module) of specified luminaire. Include spectral distribution of test LED light source.

1.5.7 LED Driver and Dimming Switch Compatibility Certificate

Submit certification from the luminaire, driver, or dimmer switch manufacturer that ensures compatibility and operability between devices without flickering and to specified dimming levels.

1.5.8 Photometric Plan

1.5.8.1 Computer-generated Photometric Plans

Computer-generated photometric plans for each space are required to verify proposed luminaires and locations meet the required performance criteria of the design using the applicable light loss factor (LLF).

Target illumination levels are provided for each Interior Application. Depending on the application and the recommendations provided by the IES, values are given as one of the following:

a. Minimum: No values anywhere on the calculation grid may be less than this value, within a 10 percent margin of error.

b. Minimum Average: An average, taken over the entire task area for the application, may not be less than this value, within a 10 percent margin of error.

c. Maximum: No values anywhere on the calculation grid may be greater than this value, within a 10 percent margin of error.

d. Maximum Average: An average, taken over the entire task area for the application, may not be greater than this value, within a 10 percent margin of error.

e. Uniformity: Unless otherwise noted, uniformity is calculated as a ratio of the average calculated illuminance over the minimum calculated illuminance of the calculation grid.

1.5.8.2 Schematic Photometric Plan Calculations

Schematic photometric plan calculations must include:

a. Horizontal illuminance measurements at workplane or other designated height above finished floor, taken at a maximum of every one foot across the task area.

b. Average maintained illuminance level.

c. Minimum and maximum maintained illuminance levels.

d. Lighting power density (Watts per square foot).

e. LLF. Recommended LLF is 0.81 for LED luminaires but LLF varies based on environment and application.

1.5.8.3 Final Photometric Plan Calculations

Final photometric plan calculations must include:

a. Horizontal illuminance measurements at workplane or other designated height above finished floor, taken at a maximum of every one foot across the task area.

b. Where applicable, vertical illuminance measurements at designated surface, taken at a maximum of every one foot across task area.

c. Minimum and maximum maintained illuminance levels.

d. Average maintained illuminance level.

e. Average to minimum and maximum to minimum ratios for horizontal illuminance.

f. Lighting power density (Watts per square foot).

g. LLF. Recommended LLF is 0.81 for LED luminaires but LLF varies based on environment and application.

1.5.9 Occupancy/Vacancy Sensor Coverage Layout

Provide floor plans showing coverage layouts of all devices using manufacturer's product information.

1.5.10 Test Laboratories

Test laboratories for the ANSI/IES LM-79 and ANSI/IES LM-80 test reports must be one of the following:

a. National Voluntary Laboratory Accreditation Program (NVLAP) accredited for solid-state lighting testing as part of the Energy-Efficient Lighting Products laboratory accreditation program for both LM-79 and LM-80 testing.

b. One of the qualified labs listed on the Department of Energy - LED Lighting Facts Approved Testing Laboratories List for LM-79 testing.

c. One of the EPA-Recognized Laboratories listed for LM-80 testing.

1.5.11 Regulatory Requirements

Equipment, materials, installation, and workmanship must be in accordance with the mandatory and advisory provisions of NFPA 70, unless more stringent requirements are specified or indicated. Provide luminaires and assembled components that are approved by and bear the label of UL for the applicable location and conditions unless otherwise specified.

1.5.12 Standard Products

Provide materials and equipment that are products of manufacturers regularly engaged in the production of such products which are of equal material, design, and workmanship. Products must have been in satisfactory commercial or industrial use for six months prior to bid opening. The six-month period must include applications of equipment and materials

under similar circumstances and of similar size. The product must have been on sale on the commercial market through advertisements, manufacturers' catalogs, or brochures during the six-month period. Where two or more items of the same class of equipment are required, these items must be products of a single manufacturer; however, the component parts of the item need not be the products of the same manufacturer unless stated in this section.

1.5.12.1 Alternative Qualifications

Products having less than a six-month field service record will be acceptable if a certified record of satisfactory field operation for not less than 6000 hours, exclusive of the manufacturers' factory or laboratory tests, is furnished.

1.5.12.2 Material and Equipment Manufacturing Date

Do not use products manufactured more than six months prior to date of delivery to site, unless specified otherwise.

1.6 WARRANTY

Support all equipment items by service organizations which are reasonably convenient to the equipment installation in order to render satisfactory service to the equipment on a regular and emergency basis during the warranty period of the contract.

1.6.1 Luminaire Warranty

Provide and transfer to the government the original LED luminaire manufacturers standard commercial warranty for each different luminaire manufacturer used in the project.

a. Provide a written five year minimum replacement warranty for material, luminaire finish, and workmanship. Provide written warranty document that contains all warranty processing information needed, including customer service point of contact, whether or not a return authorization number is required, return shipping information, and closest return location to the luminaire location.

   (1) Finish warranty must include failure and substantial deterioration such as blistering, cracking, peeling, chalking, or fading.

   (2) Material warranty must include:

      (a) All LED drivers and integral control equipment.

      (b) Replacement when more than 15 percent of LED sources in any lightbar or subassembly(s) are defective, non-starting, or operating below 70 percent of specified lumen output.

b. Warranty period must begin in accordance with the manufacturer's standard warranty starting date.

c. Provide replacements that are promptly shipped, without charge, to the using Government facility point of contact and that are identical to or an improvement upon the original equipment. All replacements must include testing of new components and assembly.

1.6.2 Lighting Controls Warranty

Provide and transfer to the government the original lighting controls manufacturers standard commercial warranty for each different lighting controls manufacturer used in the project. Warranty coverage must begin from date of final system commissioning or three months from date of delivery, whichever is the earliest. Warranty service must be performed by a factory-trained engineer or technician.

a. Unless otherwise noted, provide a written five year minimum warranty on the complete system for all systems with factory commissioning. Provide warranty that covers 100 percent of the cost of any replacement parts and services required over the five years which are directly attributable to the product failure. Failures include, but are not limited to, the following:

   (1) Software: Failure of input/output to execute switching or dimming commands.

   (2) Damage of electronic components due to transient voltage surges.

   (3) Failure of control devices, including but not limited to occupancy sensors, photosensors, and manual wall station control devices.

b. Provide a written five year minimum warranty on all input devices against defect in workmanship or materials provided by device manufacturer.

c. Provide a written five year minimum warranty on all control components attached to luminaires against defect in workmanship or materials.

1.7 OPERATION AND MAINTENANCE MANUALS

1.7.1 Lighting System

Provide operation and maintenance manuals for the lighting system in accordance with Section 01 78 23 OPERATION AND MAINTENANCE DATA that provide basic data relating to the design, operation, and maintenance of the lighting system for the building. Include the following:

a. Manufacturers' operating and maintenance manuals.

b. Luminaire shop drawings for modified and custom luminaires.

c. Luminaire Manufacturers' standard commercial warranty information as specified in paragraph LUMINAIRE WARRANTY.

1.7.2 Lighting Control System

Provide operation and maintenance manuals for the lighting control system in accordance with Section 01 78 23 OPERATION AND MAINTENANCE DATA that provide basic data relating to the design, operation, and maintenance of the lighting control system for the building. Include the following:

a. Lighting control system layout and wiring plan.

b. Lighting control system one-line diagram.

c. Product data for all devices, including installation and programming

instructions.

d. Occupancy/vacancy sensor coverage layout.

e. Training materials, such as videos or in-depth manuals, that cover basic operation of the lighting control system and instructions on modifying the lighting control system. Training materials must include calibration, adjustment, troubleshooting, maintenance, repair, and replacement.

f. Sequence of operation descriptions for each typical room type, including final programming, schedules, and calibration settings.

PART 2 PRODUCTS

2.1 PRODUCT COORDINATION

2.2 LUMINAIRES

UL 1598, NEMA C82.77-10. Provide luminaires as indicated in the luminaire schedule and NL plates or details on project plans, complete with light source, wattage, and lumen output indicated. All luminaires of the same type must be provided by the same manufacturer. Luminaires must be specifically designed for use with the driver and light source provided.

2.2.1 Luminaires

UL 8750, ANSI/IES LM-79, ANSI/IES LM-80. For all luminaires, provide:

a. Complete system with LED drivers and light sources.

b. Housings constructed of non-corrosive materials. All new aluminum housings must be anodized or powder-coated. All new steel housings must be treated to be corrosion resistant.

c. ANSI/IES TM-21, ANSI/IES LM-80. Minimum L70 lumen maintenance value of 50,000 hours unless otherwise indicated in the luminaire schedule. Luminaire drive current value must be identical to that provided by test data for luminaire in question.

d. Minimum efficacy as specified in the luminaire schedule. Theoretical models of initial lamp lumens per watt are not acceptable. If efficacy values are not listed in the luminaire schedule, provide luminaires that meet the following minimum values:

Luminaire Style	Minimum Luminaire Efficacy
Recessed 1 by 4, 2 by 4, and 2 by 2	100 LPW
Recessed Downlight (fixed, adjustable, wallwash)	80 LPW
Linear, Accent (undercabinet, cove)	45 LPW
Linear, Ambient (indirect wall mount, linear pendent)	100 LPW

Luminaire Style	Minimum Luminaire Efficacy
High Bay, Low Bay, and Industrial Locations	100 LPW
Food Service and Hazardous Locations	60 LPW
Other (track, residential diffusers)	50 LPW
Exterior Wall Sconce	50 LPW
Steplight	30 LPW
Parking Garage Luminaire	100 LPW

e. UL listed for dry or damp location typical of interior installations. Any luminaire mounted on the exterior of the building must be UL listed for wet location typical of exterior installations.

f. LED driver and light source package, array, or module are accessible for service or replacement without removal or destruction of luminaire.

g. Lenses constructed of heat tempered borosilicate glass, UV-resistant acrylic, or silicone. Provide polycarbonate vandal-resistant lenses as indicated. Sandblasting, etching and polishing must be performed as indicated in the luminaire description.

h. ANSI/IES TM-15. Provide exterior building-mounted luminaires that do not exceed the BUG ratings as listed in the luminaire schedule. If BUG ratings are not listed in the luminaire schedule, provide luminaires that meet the following minimum values for each application and mounting conditions:

Lighting Application	Mounting Conditions	BUG Rating
Exterior Wall Sconce	Above 4 feet AFF	B1-U0-G2
Exterior Wall Sconce	Below or at 4 feet AFF	B4-U0-G4
Steplight	Above 4 feet AFF	B1-U1-G2
Steplight	Below or at 4 feet AFF	B4-U1-G4
Parking Garage Luminaire	Ceiling mounted	B4-U4-G3

i. For all recessed luminaires that are identified to be in contact with insulation, provide luminaires that are IC-rated.

j. For all recessed luminaires that are to be installed in air plenums, require housings that are Chicago Plenum rated.

2.2.2 Luminaires for Hazardous Locations

In addition to requirements stated herein, provide LED luminaires for hazardous locations which conform to UL 844 or which have Factory Mutual

certification for the class and division indicated.

2.3 LIGHT SOURCES

NEMA ANSLG C78.377, NEMA SSL 3. Provide type, delivered lumen output, and wattage as indicated in the luminaire schedule on project plans.

2.3.1 LED Light Sources

Provide LED light sources that meet the following requirements:

a. NEMA ANSLG C78.377. Emit white light and have a nominal CCT of 3500 Kelvin.

b. Minimum Color Rendering Index (CRI) of 80.

c. Directive 2011/65/EU. Restriction of Hazardous Substances (RoHS) compliant.

d. Light source color consistency by utilizing a binning tolerance within a 3-step McAdam ellipse.

e. Color maintenance value of no greater than 0.003 (delta u'v') at 6000 hours as listed in ANSI/IES LM-79 Test Report.

2.3.1.1 Linear LED Lamps

Provide linear LED Lamps that are compatible with existing instant-start or programmed-start ballasts, and meet the following additional requirements:

a. UL 1993 UL Type A linear LED lamp.

b. Power Factor greater than or equal to 0.90 at full input power and across specified dimming range.

c. Maximum Total Harmonic Distortion (THD) less than or equal to 20 percent at full input power and across specified dimming range.

d. Lumen per watt efficacy no less than 120.

e. Minimum beam angle of 180 degrees.

f. Lamp datasheet complies with ANSI C78.54. Manufacturer must provide list of all ballasts that are compatible for use with lamp.

2.4 LED DRIVERS

NEMA SSL 1, UL 8750. Provide LED drivers that are electronic, UL Class 1 or Class 2, constant-current type and that comply with the following requirements:

a. The combined driver and LED light source system does not exceed the minimum luminaire efficacy values as listed in the luminaire schedule provided.

b. Operates at a voltage of 120-277 volts at 50/60 hertz, with input voltage fluctuations of plus/minus 10 percent.

c. Power Factor (PF) greater than or equal to 0.90 at full input power and across specified dimming range.

d. Maximum Total Harmonic Distortion (THD) less than 20 percent at full input power and across specified dimming range.

e. Operates for at least 50,000 hours at maximum case temperature and 90 percent non-condensing relative humidity.

f. Withstands Category A surges of 2 kV without impairment of performance. Provide surge protection that is integral to the driver.

g. Integral thermal protection that reduces the output power to protect the driver and light source from damage if the case temperature approaches or exceeds the driver's maximum operating temperature.

h. 47 CFR 15. Complies with the requirements of the Federal Communications Commission (FCC) rules and regulations, Non-Consumer (Class A) for EMI/RFI (conducted and radiated).

i. Class A sound rating.

j. Directive 2011/65/EU. Restriction of Hazardous Substances (RoHS) compliant.

k. Provide dimming capability as indicated in the luminaire schedule on project plans. Dimmable drivers must dim down to 10 percent. Dimmable drivers must be controlled by a Class 2 low voltage 0-10VDC controller dimming signal protocol unless otherwise specified. LED drivers of the same family/series must track evenly across multiple luminaires at all light levels.

2.4.1 Remote LED Drivers

Provide remote LED Drivers that are UL listed for dry locations typical of interior installations. Provide LED driver in junction box or housing with mounting plate. Housing must allow for field connections to occur inside the housing or must contain mechanical connections.

2.5 LIGHTING CONTROLS

Provide lighting control systems that do not switch off battery-operated or emergency backup luminaires or exit signs in path of egress. Provide system with override of lighting control devices controlling luminaires in path of egress with activation of fire alarm system.

2.5.1 System

Provide lighting control system that operates the lighting system as described in the lighting control strategies in the project plans. Submit Sequence of Operation for Lighting Control System describing the operation of the proposed lighting control system and devices. Sequence of Operation must provide the strategies identified in the lighting control strategies.

2.5.1.1 Localized Control Systems

Provide room or area-wide lighting control system capable of manual control, time-based control, and receiving input from photosensors and

occupancy/vacancy sensors.

2.5.1.1.1 Local Area Controller

Provide controller designed for single area or room with the following requirements:

a. Operates at a voltage of 120 volts at 50/60 hertz.

b. 2 zone, with 1 relay rated 20 amps with one manual dimmer per zone.

c. Provide inputs for occupancy/vacancy sensors, photosensors, and low-voltage wall switches.

d. Provide daylight harvesting capability with full-range dimming control with input from photosensor.

e. Provide capability for receptacle load control from occupancy sensors.

f. Provide full 'OFF' function with input from external time clock input.

g. Capable of 0-10V dimming.

i. Provide override 'ON' function with input from Fire Alarm Control Panel for all emergency lighting. Controller must not turn off power to emergency batteries or exit signs.

2.5.1.2 Centralized Control Systems

Provide a centralized lighting control system capable of manual control, time-based control, receiving input from photosensors and occupancy/vacancy sensors, with the capabilities of controlling, monitoring, and programming changes from one centralized on-site location, and integration with other building systems.

2.5.1.2.1 Gateway

Provide hardware and software to enable the BAS to monitor, control, display, and record data for use in processing reports. Provide BACnet communication interface that enables remote control and monitoring of lighting from a workstation according to read access points and write access points listed in this section. Control features and monitoring points displayed locally at lighting panel must be available through the Gateway. Provide Gateway that meets the following requirements:

a. Microprocessor-based communications device that perform bi-directional protocol translation.

b. Support full bi-directional communication and translation.

c. Contain its own microprocessor, RAM, battery, communication ports, and power supply.

d. Support an additional 5 percent points for future expansion.

2.5.2 Devices

2.5.2.1 Switches

When used for non-digital loads, devices must be rated at 20 Amps inductive load, and be compatible with the lighting control systems.

2.5.2.2 Digital Switch Timers

Provide line-voltage toggle switches that allow manual control to ON and automatically switches lighting load to OFF. Device operates with the use of paddle, button, or toggle, and operates at 120-277 volts. Device allows for programming of auto off timer from 2 minutes to 12 hours.

2.5.2.3 Wall Box Dimmers

UL 1472, UL 20, IEEE C62.41, NEMA 77, NEMA SSL 7A. Dimmers must provide flicker-free, continuously variable light output throughout the dimming range of 10 percent to 100 percent. Devices must be capable of operating at their full rated capacity regardless of being single or ganged-mounted, and be compatible with three-way and four-way switching scenarios.

Provide wall-box dimmers that meet the following requirements:

a. Device operates as an independent control device.

b. Device operates with the use of a vertical slider, paddle, rotary, button, or toggle with adjacent vertical slider.

c. Finish of device matches switches and outlets in the same area.

d. Back box in wall has sufficient depth to accommodate body of switch and wiring.

e. Dimmer is capable of controlling 0-10 volt LED drivers. Dimmers and the drivers they control must be provided from the same manufacturer or tested and certified as compatible for use together.

f. Radio frequency interference suppression is integral to device.

2.5.2.4 Scene Wallstations

Provide scene wallstations that are compatible with the other components of the lighting control system and capable of Class 1 or 2 wiring methods in accordance with the NEC and local codes. Provide devices that contain on/off group, preset scene functions, or dim up/dim down interface through front panel. Programming of new scenes or zone assignments must be accomplished by authorized personnel from the space being controlled. Provide labeling for each button, including laminated sheet with scene descriptions to be posted near each scene controller.

2.5.2.5 Occupancy/Vacancy Sensors

IEEE C62.41, NEMA WD 1, UL 94, UL 916, UL 508, ASTM D4674 REV A, NEMA WD 7. Provide occupancy/vacancy sensors with coverage patterns as indicated on manufacturer shop drawings. Provide no less quantity of sensors as shown on plans, but add additional sensors when required to fulfill coverage requirement for the specific model of sensor provided. Provide sensor types as described in the sequence of operations. Sensor locations and

quantities are shown in shop drawings provided by the lighting control system manufacturer. Provide occupancy sensor operation that requires movement to activate luminaires controlled and turns luminaires off after a set time of inactivity. Provide vacancy sensor operation that requires manual control to activate luminaires and turns luminaires off after a set time of inactivity. Provide ceiling or wall-mounted occupancy/vacancy sensors that meet the following requirements:

a. Operating voltage of 120-277 volts.

b. Time delay of 30 seconds to 30 minutes with at least four intermediate time delay settings.

c. Sensors are mounted as shown on plans.

d. Does not exceed a maximum load requirement of 20mA at 24VDC.

e. Shielded or controlled by internal logic to adjust sensitivity to avoid false triggering due to ambient temperature, air temperature variations or HVAC air movement.

f. Sensor is equipped to automatically energize the connected load upon loss of normal power when located in a means of egress.

g. Occupancy and vacancy operation is field-adjustable and programmable with push-button or dip switch on the sensor device.

h. No leakage current to load when in the off mode.

i. Utilize zero-crossing circuitry to prevent damage from high inrush current and to promote long life operation.

2.5.2.5.1 Integrated Sensors

Provide integrated occupancy/vacancy sensors that mount directly to the luminaires as indicated in project plans. Sensor mounts to standard junction box or directly to luminaire using a straight nipple mount.

2.5.2.5.2 Power Packs

UL 2043. Provide power packs to provide power to lighting control sensors as required in accordance with the manufacturer's specifications. Provide power packs that meet the following requirements:

a. Operate at an input voltage of 120-277 VAC, with an output voltage 12-24 VDC at 225 mA.

b. Constructed of plenum-rated, high-impact thermoplastic enclosure.

c. Utilizes zero-crossing circuitry to prevent damage from inrush current.

e. Directive 2011/65/EU. Restriction of Hazardous Substances (RoHS) compliant.

2.6 EXIT AND EMERGENCY LIGHTING EQUIPMENT

2.6.1 Exit Signs

UL 924, NFPA 101. Provide wattage as indicated in the luminaire schedule

on project plans. Provide LED Exit Signs that meet the following criteria:

a. Housing constructed of UV-stable, thermo-plastic.

b. UL listed for damp location.

d. 6 inch high, 3/4 inch stroke red lettering on face of sign with chevrons on either side of lettering to indicate direction.

e. Single or double face as indicated in project plans and luminaire schedule.

2.6.1.1 Exit Signs with Battery Backup

Equip with automatic power failure device, test switch, and pilot light, and fully automatic high/low trickle charger in a self-contained power pack. Battery must be sealed, maintenance free nickel-cadmium type, and must operate unattended for a period of not less than five years. Emergency run time must be a minimum of 1-1/2 hours. LEDs must have a minimum rated life of 10 years. In lieu of battery, can use a nonradioactive photoluminescent plate.

2.6.2 LED Emergency Drivers

UL 924, NFPA 101. Provide LED emergency driver with automatic power failure detection, test switch and LED indicator (or combination switch/indicator) located on luminaire exterior, and fully-automatic solid-state charger, battery and inverter integral to a self-contained housing. Provide self-diagnostic function integral to emergency driver. Integral nickel-cadmium battery is required to supply a minimum of 90 minutes of emergency power at 10 watts, 10-50 VDCcompatible with LED forward voltage requirements, constant output. Driver must be RoHS compliant, rated for installation in plenum-rated spaces and damp locations, and be warranted for a minimum of five years.

2.6.3 Self-Diagnostic Circuitry for LED Drivers

UL 924, NFPA 101. Provide emergency lighting unit with fully-automatic, integral self-testing/diagnostic electronic circuitry. Circuitry must provide for a one minute diagnostic test every 28 days, and a 30 minute diagnostic test every six months, minimum. Any malfunction of the unit must be indicated by LED(s) visible from the exterior of the luminaire. A manual test switch must also be provided to perform a diagnostic test at any given time.

2.7 LUMINAIRE MOUNTING ACCESSORIES

2.7.1 Suspended Luminaires

a. Provide hangers capable of supporting twice the combined weight of luminaires supported by hangers.

b. Hangers must allow luminaires to swing within an angle of 45 degrees. Brace pendents 4 feet or longer to limit swinging.

c. Single-unit suspended luminaires must have cable hangers. Multiple-unit or continuous row luminaires with a separate power supply cord must have a tubing or stem for wiring at one point and a tubing or rod suspension provided for each unit length of chassis,

including one at each end.

d. Provide all linear pendent and surface mounted luminaires with two supports per four-foot section or three per eight-foot section unless otherwise recommended by manufacturer.

2.7.2 Recess and Surface Mounted Luminaires

Provide access to light source and LED driver from bottom of luminaire. Provide trim and lenses for the exposed surface of flush-mounted luminaires as indicated on project drawings and specifications. Luminaires recessed in ceilings which have a fire resistive rating of one hour or more must be enclosed in a box which has a fire resistive rating equal to that of the ceiling. For surface mounted luminaires with brackets, provide flanged metal stem attached to outlet box, with threaded end suitable for supporting the luminaire rigidly in design position. Flanged part of luminaire stud must be of broad base type, secured to outlet box at not fewer than three points.

2.7.3 Luminaire Support Hardware

2.7.3.1 Wire

ASTM A641/A641M. Galvanized, soft tempered steel, minimum 0.11 inches in diameter, or galvanized, braided steel, minimum 0.08 inches in diameter.

2.7.3.2 Wire for Humid Spaces

ASTM A580/A580M. Composition 302 or 304, annealed stainless steel, minimum 0.11 inches in diameter.

ASTM B164. UNS NO4400, annealed nickel-copper alloy, minimum 0.11 inches in diameter.

2.7.3.3 Threaded Rods

Threaded steel rods, 3/16 inch diameter, zinc or cadmium coated.

2.7.3.4 Straps

Galvanized steel, one by 3/16 inch, conforming to ASTM A653/A653M, with a light commercial zinc coating or ASTM A1008/A1008M with an electrodeposited zinc coating conforming to ASTM B633, Type RS.

2.7.4 Power Hook Luminaire Hangers

UL 1598. Provide an assembly consisting of through-wired power hook housing, interlocking plug and receptacle, power cord, and luminaire support loop. Power hook housing must be cast aluminum having two 3/4 inch threaded hubs. Support hook must have safety screw. Luminaire support loop must be cast aluminum with provisions for accepting 3/4 inch threaded stems. Power cord must include 16 inches of 3 conductor No. 16 Type SO cord. Assembly must be rated 120 volts or 277 volts, 15 amperes.

2.8 EQUIPMENT IDENTIFICATION

2.8.1 Manufacturer's Nameplate

Each item of equipment must have a nameplate bearing the manufacturer's

name, address, model number, and serial number securely affixed in a conspicuous place; the nameplate of the distributing agent will not be acceptable.

2.8.2 Labels

UL 1598. All luminaires must be clearly marked for operation of specific light sources and LED drivers. The labels must be easy to read when standing next to the equipment, and durable to match the life of the equipment to which they are attached. Note the following light source characteristics in the format "Use Only _____":

a. Correlated Color Temperature (CCT) and Color Rendering Index (CRI) for all luminaires.

b. Driver and dimming protocol.

All markings related to light source type must be clear and located to be readily visible to service personnel, but unseen from normal viewing angles when light sources are in place. LED drivers must have clear markings indicating dimming type and indicate proper terminals for the various outputs.

2.9 FACTORY APPLIED FINISH

NEMA 250. Provide all luminaires and lighting equipment with factory-applied painting system that as a minimum, meets requirements of corrosion-resistance testing.

PART 3 EXECUTION

3.1 INSTALLATION

IEEE C2, NFPA 70.

3.1.1 Light Sources

When light sources are not provided as an integral part of the luminaire, deliver light sources of the type, wattage, lumen output, color temperature (CCT), color rendering index (CRI), and voltage rating indicated to the project site and install just prior to project completion, if not already installed in the luminaires from the factory.

3.1.2 Luminaires

Set luminaires plumb, square, and level with ceiling and walls, in alignment with adjacent luminaires and secure in accordance with manufacturers' directions and approved drawings. Provide accessories as required for ceiling construction type indicated on Finish Schedule. Luminaire catalog numbers do not necessarily denote specific mounting accessories for type of ceiling in which a luminaire may be installed. Provide wires, straps, or rods for luminaire support in this section. Install luminaires with vent holes free of air blocking obstacles.

3.1.2.1 Suspended Luminaires

Measure mounting heights from the bottom of the luminaire for ceiling-mounted luminaires and to center of luminaire for wall-mounted luminaires. Obtain architect approval of the exact mounting height on the

job before commencing installation and, where applicable, after coordinating with the type, style, and pattern of the ceiling being installed. Support suspended luminaires from structural framework of ceiling or from inserts cast into slab.

a. Provide suspended luminaires with 45 degree swivel hangers so that they hang plumb and level.

b. Locate so that there are no obstructions within the 45 degree range in all directions.

c. The stem, canopy and luminaire must be capable of 45 degree swing.

d. Rigid pendent stem, aircraft cable, rods, or chains 4 feet or longer excluding luminaire must be braced to prevent swaying using three cables at 120 degree separation.

e. Suspended luminaires in continuous rows must have internal wireway systems for end to end wiring and must be properly aligned to provide a straight and continuous row without bends, gaps, light leaks or filler pieces.

f. Utilize aligning splines on extruded aluminum luminaires to assure minimal hairline joints.

g. Support steel luminaires to prevent "oil-canning" effects.

h. Match supporting pendents with supported luminaire. Aircraft cable must be stainless steel.

i. Match finish of canopies to match the ceiling, and provide low profile canopies unless otherwise shown.

j. Maximum distance between suspension points must be 10 feet or as recommended by the manufacturer, whichever is less.

3.1.2.2 Recessed and Semi-Recessed Luminaires

a. Support recessed and semi-recessed luminaires independently from the building structure by a minimum of two wires, straps or rods per luminaire and located near opposite corners of the luminaire. Secure horizontal movement with clips provided by manufacturer. Ceiling grid clips are not allowed as an alternative to independently supported luminaires.

b. Support round luminaires or luminaires smaller in size than the ceiling grid independently from the building structure by a minimum of four wires, straps or rods per luminaire, spaced approximately equidistant around.

c. Do not support luminaires by acoustical tile ceiling panels.

d. Where luminaires of sizes less than the ceiling grid are indicated to be centered in the acoustical panel, support each independently and provide at least two 3/4 inch metal channels spanning, and secured to, the ceiling tees for centering and aligning the luminaire.

e. Luminaires installed in suspended ceilings must also comply with the requirements of Section 09 51 00 ACOUSTICAL CEILINGS.

f. Adjust aperture rings on all applicable ceiling recessed luminaires to accommodate various ceiling material thickness. Coordinate cut-out size in ceiling to ensure aperture covers cut-out entirely. Install aperture rings such that the bottom of the ring is flush with finished ceiling or not more than 1/16 inch above. Do not install luminaires such that the aperture ring extends below the finished ceiling surface.

g. For luminaire recessed in plaster ceilings, provide plaster frames for setting. Install setting such that the bottom of the frame is flush with finished ceiling. Support luminaires with plaster frames utilizing yokes or leveling lugs. Do not mount luminaires or support elements to ducts or pipes. Yokes must support a luminaire by no fewer than two bolts each.

3.1.3 LED Drivers

Provide LED drivers integral to luminaire as constructed by the manufacturer.

3.1.4 Exit Signs

NFPA 101. Wire exit signs and emergency lighting units ahead of the local switch, to the normal lighting circuit located in the same room or area.

Serve from an emergency panel. Provide only one source of control, which would be the circuit breaker in the emergency panel. Paint source of control red and provide lockout capability.

3.1.5 Lighting Controls

3.1.5.1 Scene Wallstations

Submit labeling templates for all scene wallstations, ganged faceplates and other manual control cover plates. Label each scene control button with approved scene description.

3.1.5.2 Occupancy/Vacancy Sensors

a. Provide quantity of sensor units indicated as a minimum. Provide additional units to give full coverage over controlled area. Full coverage must provide hand and arm motion detection for office and administration type areas and walking motion for industrial areas, warehouses, storage rooms and hallways.

b. Locate ceiling-mounted sensors no closer than 6 feet from the nearest HVAC supply or return diffuser.

c. Locate the sensor(s) as indicated and in accordance with the manufacturer's recommendations.

3.1.5.3 Photosensors

Locate and aim sensor as indicated and in accordance with the manufacturer's recommendations. Adjust sensor set-point in accordance with the manufacturer's recommendations and for the indicated light level of the area of coverage, measured at the work plane.

3.2 FIELD QUALITY CONTROL

3.2.1 Tests

3.2.1.1 Lighting Control Verification Tests

Verify lighting control system and devices operate according to approved sequence of operations. Verification tests are to be completed after commissioning.

a. Verify occupancy/vacancy sensors operate as described in sequence of operations. Provide testing of sensor coverage, sensitivity, and time-out settings in all spaces where sensors are placed. This is to be completed only after all furnishings have been installed. Submit occupancy/vacancy sensor verification test.

b. Verify photosensors operate as described in sequence of operations. Provide testing of sensor coverage, aiming, and calibration in all spaces where sensors are placed. This is to be completed only after all furnishings have been installed. Submit photosensor verification test.

c. Verify wall box dimmers and scene wallstations operate as described in sequence of operations.

3.2.1.2 Emergency Lighting Test

Interrupt power supply to demonstrate proper operation of emergency lighting. If adjustments are made to the lighting system, re-test system to show compliance with standards.

3.3 CLOSEOUT ACTIVITIES

3.3.1 Commissioning

NFPA 101. Commission all components of the lighting system and lighting control system in accordance with Section 01 91 00.15 10 TOTAL BUILDING COMMISSIONING. Factory Trained Field Service Technician is responsible for calibration and programming sequences for input devices and systems in accordance with the requirements described in the sequence of operation.

3.3.2 Training

3.3.2.1 Maintenance Staff Training

Submit a Maintenance Staff Training Plan at least 30 calendar days prior to training session that describes training procedures for Owner's personnel in the operation and maintenance of lighting and lighting control system. Provide on-site training which demonstrates full system functionality, assigning schedules, calibration adjustments for light levels and sensor sensitivity, integration procedures for connecting to third-party devices, and manual override including information on appropriate use. Provide protocols for troubleshooting, maintenance, repair, and replacement, and literature on available system updates and process for implementing updates.

3.3.2.2 End-User Training

Submit an End-User Training Plan at least 30 calendar days prior to

training session that describes training procedures for end-users on the lighting control system. Provide users with a list of control devices located within user-occupied spaces, such as photosensors and occupancy and vacancy sensors, including information on the proper operation and schedule for each device. Provide demonstration for each type of interface. Provide users with the building schedule as currently commissioned, including conditional programming based on astronomic time clock functionality. Provide users with the correct contact information for maintenance personnel who will be available to address any lighting control issues.

Provide laminated instructions to the user at each scene wallstation. Provide only instructions relevant to the functionality of the specific scene wallstation. Provide a description of each labeled scene control button. If the room utilizes occupancy/vacancy sensors or photosensors, include a description of this functionality on the instruction sheet.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 26 - ELECTRICAL

SECTION 26 52 00.00 40

EMERGENCY LIGHTING

PART 1 GENERAL

1.1 REFERENCES
1.2 ADMINISTRATIVE REQUIREMENTS
1.2.1 Preinstallation Meetings
1.3 SUBMITTALS

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION
2.1.1 Performance Requirements
2.2 MANUFACTURED UNITS
2.2.1 Central Emergency Lighting Systems
2.2.2 Self-Testing Module

PART 3 EXECUTION

3.1 INSTALLATION
3.2 FIELD QUALITY CONTROL
3.3 WARRANTY

-- End of Section Table of Contents --

SECTION 26 52 00.00 40

EMERGENCY LIGHTING

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National Electrical Code
NFPA 101	(2021; TIA 21-1) Life Safety Code

UNDERWRITERS LABORATORIES (UL)

UL 924	(2016; Reprint May 2020) UL Standard for Safety Emergency Lighting and Power Equipment

1.2 ADMINISTRATIVE REQUIREMENTS

1.2.1 Preinstallation Meetings

No later than 30 days after contract award, submit installation drawings for the Central Emergency Lighting Systems, indicating the location of installed fixtures.

Submit material, equipment, and fixture lists showing the manufacturer's style or catalog numbers, specification and drawing reference numbers, and a sample warranty. Also submit the manufacturer's catalog data and certificates of conformance for the following items:

a. Emergency Lighting Egress Units

b. Emergency Fluorescent Lighting

c. Central Emergency Lighting Systems

d. Accessories

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Central Emergency Lighting Systems; G

SD-03 Product Data

Material, Equipment, and Fixture Lists; G

Sample Warranty; G

Central Emergency Lighting Systems; G

SD-06 Test Reports

System Operational Tests; G

SD-07 Certificates

Certificates of Conformance

SD-11 Closeout Submittals

Warranty

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION

Furnish emergency lighting units completely assembled with wiring and mounting devices, ready for installation at the locations indicated. Equip fixtures with lamps. Ensure that emergency lighting units are suitable for operation on the ac supply circuit to which they are to be electrically connected.

2.1.1 Performance Requirements

Provide emergency lighting units conforming to UL 924 and NFPA 101.

2.2 MANUFACTURED UNITS

2.2.1 Central Emergency Lighting Systems

Provide a central power system providing emergency power at 277 volts, 60 hertz, for a minimum period of 90 minutes. Design the system to handle surges during loss and recovery of the voltage, and to deliver its full rated output to the designated lamp load. Provide backup ac source for power.

2.2.2 Self-Testing Module

Provide a self-testing module for the emergency lighting equipment that performs the following functions:

a. Continuous monitoring of charger operation and battery voltage with visual indication of normal operation and of malfunction.

b. Monthly discharge cycling of battery with monitoring of transfer circuit function, battery capacity, and emergency lamp operation with visual indication of malfunction. Conduct the battery capacity test using a synthetic load.

c. Manual test switch to simulate a discharge test cycle.

d. Low-voltage battery disconnect (LVD) and brown-out protection circuit.

PART 3 EXECUTION

3.1 INSTALLATION

Permanently fix in place the emergency lighting unit and install wiring for each unit in accordance with NFPA 70. Use the same panel bus or branch circuit as that serving the normal lighting in the area for the branch circuit feeding the unit equipment, and connect ahead of the area switches. Keep remotely connected emergency lighting circuit wiring independent of all other wiring and equipment, and do not enter the same conduit, cable, box, or cabinet with other wiring unless the fixture is supplied from two sources.

3.2 FIELD QUALITY CONTROL

Demonstrate emergency lighting units to operate satisfactorily in the presence of the Contracting Officer.

Perform and submit System Operational Tests in accordance with referenced standards in this section.

3.3 WARRANTY

Submit 2 copies of warranty, signed by an authorized representative, designating the Government as warrantee, to the Contracting Officer, 5 days before project closeout.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 26 - ELECTRICAL

SECTION 26 53 00.00 40

EXIT SIGNS

PART 1 GENERAL

1.1 REFERENCES
1.2 ADMINISTRATIVE REQUIREMENTS
1.2.1 Pre-Installation Meetings
1.3 SUBMITTALS
1.4 WARRANTY

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION
2.2 COMPONENTS
2.2.1 Contemporary Fixtures
2.2.2 Light Emitting Diodes (LEDs) Exit Lighting Fixtures

PART 3 EXECUTION

3.1 INSTALLATION
3.2 FIELD QUALITY CONTROL
3.2.1 Tests

-- End of Section Table of Contents --

SECTION 26 53 00.00 40

EXIT SIGNS

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 101	(2021; TIA 21-1) Life Safety Code

U.S. DEPARTMENT OF ENERGY (DOE)

DOE LT-4	(2005) How to Buy Energy-Efficient Exit Signs

UNDERWRITERS LABORATORIES (UL)

UL 924	(2016; Reprint May 2020) UL Standard for Safety Emergency Lighting and Power Equipment

1.2 ADMINISTRATIVE REQUIREMENTS

1.2.1 Pre-Installation Meetings

No more than 30 days after Contract Award, the Contracting Officer will schedule a Pre-Installation Meeting. Submit material, equipment, and fixture lists for the following showing manufacturer's product data, including style or catalog numbers, specification and drawing reference numbers, warranty information, and fabrication site:

a. Exit Lighting Units

b. Contemporary Fixtures

c. Accessories

Submit exit lighting units outline drawings indicating overall physical features, dimensions, ratings, service requirements, and weights of equipment.

Submit certificates clearly indicating the energy efficiencies of each fixture type, and conformance with 42 U.S.C. 8253(f) "Use of Energy and Water Efficiency in Federal Buildings, September 2012", and DOE’s Facility Energy Management Guidelines and Criteria for Energy and Water Evaluations in Covered Facilities, http://www1.eere.energy.gov/femp/technologies/procuring_eeproducts.html

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Material, Equipment, and Fixture Lists; G

SD-02 Shop Drawings

Exit Lighting Units; G

Exit Lighting Units Outline Drawings; G

SD-03 Product Data

Exit Lighting Units; G

Contemporary Fixtures; G

Accessories; G

SD-06 Test Reports

Operational Tests; G

SD-07 Certificates

Energy Efficiencies; G

1.4 WARRANTY

Provide a five year warranty for all components.

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION

Provide emergency exit lighting fixtures conforming to UL 924, NFPA 101, and as specified.

Provide exit lighting fixtures completely assembled with wiring and mounting devices, ready for installation at the locations indicated. Ensure ceiling-mounted fixtures are designed to be supported independent of the ceiling and equipped with lamps.

Provide exit lighting fixtures having efficiencies in accordance with the recommended levels specified in DOE LT-4.

2.2 COMPONENTS

2.2.1 Contemporary Fixtures

Provide contemporary exit lighting fixtures having a fixture body with edge-lighted plastic exit-sign panels, face trims, lamps, lampholders, and mounting brackets for top, back, and end mounting to walls and ceilings in

accordance with NFPA 101, as indicated.

2.2.2 Light Emitting Diodes (LEDs) Exit Lighting Fixtures

Provide exit lighting fixtures with sheet metal enclosures, including frames, battery charger, batteries, red light emitting diodes (LEDs), and mounting brackets with mounting plates suitable for securing the fixture to a 4-inch outlet box. Ensure fixture features include:

a. Continuous charging

b. Automatic switching to standby batteries upon loss of power

c. Overload protection

d. Short circuit protection

e. Test switch

f. Low voltage disconnect

g. Switch controlled left and right LED directional arrows

h. Field connectable to operate from 277 volts

i. Brightness not less than ten (10) candlepower

Provide unit battery system with minimum operating time of three (3) hours for double faced fixtures and seven (7) hours for single faced fixtures.

PART 3 EXECUTION

3.1 INSTALLATION

Connect fixtures to the main panel bus through overcurrent protection. Use emergency lighting panel where available.

3.2 FIELD QUALITY CONTROL

3.2.1 Tests

Field test exit lighting to demonstrate satisfactory operation in the presence of the Contracting Officer.

Perform and submit operational tests in accordance with referenced standards in this section.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 26 - ELECTRICAL

SECTION 26 55 53.00 40

SECURITY LIGHTING

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 QUALITY CONTROL
1.3.1 Standard Products
1.4 PROJECT/SITE CONDITIONS

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION
2.1.1 Lighting System
2.1.1.1 Electrical Requirements
2.1.2 System Design
2.2 EQUIPMENT
2.2.1 Interface Lighting System and Power Distribution
2.2.2 Aerial Cable Hardware
2.2.3 Cable Splices and Connectors
2.2.4 Cable Boxes
2.2.5 Manholes, Handholes, and Pullboxes
2.2.6 Conduit, Ducts and Fittings
2.2.6.1 Conduit, Rigid Steel
2.2.6.2 Conduit Coatings
2.2.6.3 Conduit Fittings and Outlets
2.2.6.4 Non-Metallic Duct
2.2.7 Transformers
2.2.8 Wireway, Raintight, Support
2.2.9 Nameplates
2.2.10 Spare Parts
2.3 COMPONENTS
2.3.1 Protection of Security Lighting System Components
2.3.1.1 Components and Conductors
2.3.1.2 Tamper Provisions
2.3.2 Cable
2.3.2.1 Insulated Cable
2.3.2.2 Messenger Cable
2.3.2.3 Bare Copper Conductors
2.3.3 Electrical Enclosures
2.3.3.1 Interior Enclosures
2.3.3.2 Exposed-to-Weather Enclosures
2.3.4 Illumination
2.3.5 Luminaire Components
2.3.6 Photometric Distribution Classification
2.3.7 Luminaires, Floodlighting
2.3.7.1 HID and Incandescent
2.4 MATERIALS

2.4.1 Corrosion Protection
2.4.1.1 Aluminum Materials
2.4.1.2 Ferrous Metal Materials
2.4.1.3 Finishing

PART 3 EXECUTION

3.1 PREPARATION
3.1.1 Current Site Conditions
3.1.2 Existing Equipment
3.2 INSTALLATION
3.2.1 Enclosure Penetrations
3.2.2 Prevention of Corrosion
3.2.2.1 Aluminum
3.2.2.2 Steel Conduits
3.2.2.3 Cold Galvanizing
3.2.3 Cable Installation
3.2.3.1 Splices
3.2.3.2 Installation in Duct Lines
3.2.4 Direct Burial
3.2.4.1 Trenching
3.2.4.2 Requirements for Installation in Duct
3.2.4.3 Location of Cable Splices
3.2.4.4 Markers
3.2.4.5 Warning Tape
3.2.5 Messenger Cable
3.2.5.1 Installation
3.2.5.2 Grounding and Bonding Connections
3.2.5.3 Grounding Conductors and Electrodes
3.2.5.4 Ground Resistance Testing
3.2.6 Aerial Cable Splices
3.2.7 Lashing Wire
3.2.8 Stress Loops
3.2.9 Connections to Buildings
3.2.10 Duct Lines
3.2.10.1 Requirements
3.2.10.2 Treatment
3.2.10.3 Concrete Encasement
3.2.10.4 Installation of Couplings
3.2.10.5 Concrete
3.2.10.6 Duct Line Markers
3.2.11 Handholes
3.2.11.1 Construction
3.2.11.2 Appurtenances
3.2.11.3 Cable Pulling-in Irons
3.2.11.4 Ground Rods
3.2.12 Lighting
3.2.12.1 Lamps
3.2.12.2 Fixture Installation
3.2.13 Transformer Installation
3.2.14 CCTV Alarm Interface
3.3 FIELD QUALITY CONTROL
3.3.1 Operating Test
3.3.2 Ground Resistance Measurements
3.4 CLOSEOUT ACTIVITIES
3.4.1 Operations and Maintenance Manuals
3.4.2 Record Drawings

-- End of Section Table of Contents --

SECTION 26 55 53.00 40

SECURITY LIGHTING

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ASTM INTERNATIONAL (ASTM)

ASTM A48/A48M	(2003; R 2021) Standard Specification for Gray Iron Castings
ASTM A123/A123M	(2017) Standard Specification for Zinc (Hot-Dip Galvanized) Coatings on Iron and Steel Products
ASTM A153/A153M	(2016a) Standard Specification for Zinc Coating (Hot-Dip) on Iron and Steel Hardware
ASTM A575	(2020) Standard Specification for Steel Bars, Carbon, Merchant Quality, M-Grades
ASTM A576	(2017) Standard Specification for Steel Bars, Carbon, Hot-Wrought, Special Quality
ASTM B2	(2013) Standard Specification for Medium-Hard-Drawn Copper Wire
ASTM B8	(2011; R 2017) Standard Specification for Concentric-Lay-Stranded Copper Conductors, Hard, Medium-Hard, or Soft
ASTM B117	(2019) Standard Practice for Operating Salt Spray (Fog) Apparatus
ASTM C478	(2018) Standard Specification for Circular Precast Reinforced Concrete Manhole Sections
ASTM D1654	(2008; R 2016; E 2017) Standard Test Method for Evaluation of Painted or Coated Specimens Subjected to Corrosive Environments

ILLUMINATING ENGINEERING SOCIETY (IES)

ANSI/IES RP-8	(2018; Addenda 1 2020; Errata 1-2 2021) Recommended Practice for Design and Maintenance of Roadway and Parking Facility Lighting

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 81	(2012) Guide for Measuring Earth Resistivity, Ground Impedance, and Earth Surface Potentials of a Ground System
IEEE C2	(2023) National Electrical Safety Code
IEEE C62.41.1	(2002; R 2008) Guide on the Surges Environment in Low-Voltage (1000 V and Less) AC Power Circuits
IEEE C62.41.2	(2002) Recommended Practice on Characterization of Surges in Low-Voltage (1000 V and Less) AC Power Circuits
IEEE C135.1	(1999) Standard for Zinc-Coated Steel Bolts and Nuts for Overhead Line Construction

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

ANSI C80.1	(2020) American National Standard for Electrical Rigid Steel Conduit (ERSC)
ANSI C119.1	(2016) Electric Connectors - Sealed Insulated Underground Connector Systems Rated 600 Volts
ANSI C136.2	(2015) American National Standard for Roadway and Area Lighting Equipment: Luminaires Voltage Classification
ANSI C136.3	(2020) Roadway and Area Lighting Equipment - Luminaire Attachments
ANSI C136.6	(2004) American National Standard for Roadway Lighting Equipment - Metal Heads and Reflector Assemblies - Mechanical and Optical Interchangeability
ANSI C136.9	(2003) American National Standard for Roadway and Area Lighting Equipment - Socket Support Assemblies for Metal Heads - Mechanical Interchangeability
ANSI C136.11	(2011; R 2016; STBL 2021) Roadway Lighting Equipment - Multiple Parallel Wired Sockets
ANSI C136.15	(2020) American National Standard for Roadway and Area Lighting Equipment - Luminaire Field Identification
ANSI/NEMA OS 1	(2013; R 2020) Sheet-Steel Outlet Boxes, Device Boxes, Covers, and Box Supports
NEMA 250	(2020) Enclosures for Electrical Equipment (1000 Volts Maximum)

NEMA ICS 6	(1993; R 2016) Industrial Control and Systems: Enclosures
NEMA RN 1	(2005; R 2013) Polyvinyl-Chloride (PVC) Externally Coated Galvanized Rigid Steel Conduit and Intermediate Metal Conduit
NEMA TC 6 & 8	(2020) Standard for Polyvinyl Chloride (PVC) Plastic Utilities Duct for Underground Installations
NEMA TC 9	(2020) Standard for Fittings for Polyvinyl Chloride (PVC) Plastic Utilities Duct for Underground Installation

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2020; TIA 22-1; ERTA 1 2022) National Electrical Code

TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)

TIA-232	(1997f; R 2012) Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange

UNDERWRITERS LABORATORIES (UL)

UL 6	(2007; Reprint Sep 2019) UL Standard for Safety Electrical Rigid Metal Conduit-Steel
UL 44	(2018; Reprint May 2021) UL Standard for Safety Thermoset-Insulated Wires and Cables
UL 98	(2016) UL Standard for Safety Enclosed and Dead-Front Switches
UL 467	(2022) UL Standard for Safety Grounding and Bonding Equipment
UL 486A-486B	(2018; Reprint May 2021) UL Standard for Safety Wire Connectors
UL 506	(2017; Reprint Jan 2022) UL Standard for Safety Specialty Transformers
UL 514A	(2013; Reprint Jun 2022) UL Standard for Safety Metallic Outlet Boxes
UL 514B	(2012; Reprint May 2020) Conduit, Tubing and Cable Fittings
UL 514C	(2014; Reprint Feb 2020) UL Standard for Safety Nonmetallic Outlet Boxes, Flush-Device Boxes, and Covers
UL 651	(2011; Reprint May 2022) UL Standard for

	Safety Schedule 40, 80, Type EB and A Rigid PVC Conduit and Fittings
UL 651A	(2011; Reprint Mar 2017) UL Standard for Safety Schedule 40 and 80 High Density Polyethylene (HDPE) Conduit
UL 854	(2020) Standard for Service-Entrance Cables
UL 870	(2016; Reprint Mar 2019) UL Standard for Safety Wireways, Auxiliary Gutters, and Associated Fittings
UL 1203	(2013; Reprint Apr 2022) UL Standard for Safety Explosion-Proof and Dust-Ignition-Proof Electrical Equipment for Use in Hazardous (Classified) Locations
UL 1449	(2021) UL Standard for Safety Surge Protective Devices
UL 1598	(2021; Reprint Jun 2021) Luminaires

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Lighting System; G

Detail Drawings; G

SD-03 Product Data

Spare Parts; G

Equipment

SD-06 Test Reports

Operating Test; G

Ground Resistance Measurements; G

SD-07 Certificates

Operating Test Procedures; G

SD-10 Operation and Maintenance Data

Operations and Maintenance Manuals; G

SD-11 Closeout Submittals

Record Drawings; G

1.3 QUALITY CONTROL

1.3.1 Standard Products

Provide materials and equipment which are the standard products of manufacturer regularly engaged in the manufacture of such products, and which essentially duplicate equipment that has been in satisfactory use at least two years prior to bid opening.

1.4 PROJECT/SITE CONDITIONS

Lighting equipment that is usable in their original configuration without modification may be reused with Government approval. Perform a field survey, including testing and inspection of existing lighting equipment and control lines intended to be incorporated into the lighting system, and furnish a report to the Government. For those items considered nonfunctioning, provide specification sheets, or written functional requirements to support the findings and the estimated cost to correct the deficiency with the report. As part of the report, include the scheduled need date for connection to all existing equipment.

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION

2.1.1 Lighting System

Configure the lighting system as specified and shown. Include all fixtures, hardware, poles, cables, connectors, adapters and appurtenances needed to provide a fully functional lighting system.

a Design Requirements for CCTV Assessment Lighting

Configure the CCTV Assessment Lighting system as specified and shown. Ensure equipment conforms to NFPA 70 and IEEE C2. Provide sufficient light for optimum CCTV assessment of each zone in the configuration. Include all fixtures, hardware, poles, cables, connectors, adapters, and appurtenances needed to provide a fully functional lighting system.

2.1.1.1 Electrical Requirements

Provide equipment which operates from a voltage source as shown; plus or minus 10 percent, and at 60 Hz, plus or minus 2 percent.

a. Power Line Surge Protection

Provide transient voltage surge suppressors for all electronic equipment, meeting the requirements of IEEE C62.41.1 and IEEE C62.41.2, and UL listed as tested in accordance with UL 1449. Do not use fuses as surge suppression.

b. Interface CCTV Lighting and CCTV System

Interface infrared lights to the CCTV system and provide automatic, alarm actuated call-up of the light associated with the alarm zone.

2.1.2 System Design

Submit detail drawings for the complete system and for lighting fixtures, cable boxes, handholes, transformers, and controllers. For CCTV lighting, include in date:

a. Infrared light call-up response time.

b. Lamp strike and restrike times.

c. System startup and shutdown operations.

d. Manuals for CCTV Assessment Lighting equipment.

e. A typical zone layout showing light locations, isolux patterns, and lighting ratios.

Submit data published by the manufacturer of each item on the list of equipment and material, to permit verification that the item proposed is of the correct size, properly rated or applied, or is otherwise suitable for the application and fully conforms to the requirements specified.

2.2 EQUIPMENT

2.2.1 Interface Lighting System and Power Distribution

Provide conductors as indicated.

2.2.2 Aerial Cable Hardware

Provide zinc coated aerial cable hardware conforming to IEEE C135.1, with steel hardware material conforming to ASTM A575 and ASTM A576, hot-dip galvanized in accordance with ASTM A153/A153M.

2.2.3 Cable Splices and Connectors

Provide cable splices and connectors conforming to UL 486A-486B. Provide underground splices and connectors conforming to the requirements of ANSI C119.1.

2.2.4 Cable Boxes

Provide cable boxes and covers made of cast iron with zinc coated or aluminized finish, of the sizes indicated on drawings. Provide minimum inside dimensions of not less than 12 inches square by 6 inches deep and not less than required to house the cable splice. Install a suitable gasket between the box and cover for a watertight seal. Install a sufficient number of screws to hold the cover in place along the entire surface of contact. Provide grounding lugs.

2.2.5 Manholes, Handholes, and Pullboxes

Provide manholes, handholes, pullboxes,and related frames and covers as indicated, with strengths conforming to the requirements of IEEE C2. Provide precast concrete manholes with the required strength established by ASTM C478. Provide frames and covers for manholes made of gray cast iron. Provide a machine-finished seat to ensure a matching joint between frame and cover. Cast iron is to comply with ASTM A48/A48M, Class 30B, minimum. Provide handholes for low voltage cables installed in parking

lots, sidewalks, and turf areas made from an aggregate consisting of sand and with continuous woven glass strands having an overall compressive strength of at least 10,000 psi and a flexural strength of at least 5,000 psi. Provide pullbox and handhole covers in parking lots, sidewalks, and turf areas of the same material as the box. Provide concrete pullboxes consisting of precast reinforced concrete boxes, extensions, bases, and covers. Install a sufficient number of tamperproof bolts to hold the cover firmly in place along the entire surface of contact; and include a tool for the tamperproof bolts.

2.2.6 Conduit, Ducts and Fittings

2.2.6.1 Conduit, Rigid Steel

Provide rigid steel conduit conforming to ANSI C80.1 and UL 6.

2.2.6.2 Conduit Coatings

Coat underground metallic conduit and fittings with a plastic resin system conforming to NEMA RN 1, Type 40. Epoxy systems may also be used.

2.2.6.3 Conduit Fittings and Outlets

a. Boxes, Metallic Outlets

ANSI/NEMA OS 1 and UL 514A.

b. Boxes, Nonmetallic, Outlet and Flush-Device Boxes and Covers

ANSI/NEMA OS 1 and UL 514C.

c. Boxes, Outlet for Use in Hazardous (Classified) Locations

UL 1203.

d. Boxes, Switch (Enclosed), Surface Mounted

UL 98.

e. Fittings for Conduit and Outlet Boxes

UL 514B.

f. Fittings for Use in Hazardous (Classified) Locations

UL 1203.

g. Fittings, PVC, for Use with Rigid PVC Conduit and Tubing

UL 514B.

2.2.6.4 Non-Metallic Duct

Provide non-metallic duct lines and fittings utilized for underground installation suitable for the application, consisting of thick-wall, single, round-bore type, using material of one type. Provide acrylonitrile-butadiene-styrene (ABS) duct conforming to NEMA TC 6 & 8 and NEMA TC 9, with high-density conduit conforming to UL 651A. Provide Schedule 40 polyvinyl chloride (PVC) conforming to UL 651. Provide

schedule 40 polyvinyl chloride (PVC) conforming to UL 651.

Provide all plastic utility duct and fittings manufactured without a UL label or listing with a certification as follows: "The materials are suitable for use with 167 degree F wiring. No reduction of properties in excess of that specified for materials with a UL label or listing will be experienced if samples of the finished product are operated continuously under the normal conditions that produce the highest temperature in the duct."

2.2.7 Transformers

Provide transformers conforming to UL 506. Provide rust-inhibiting treatment and standard finish by the manufacturer on all exterior transformer cases.

2.2.8 Wireway, Raintight, Support

Provide raintight wireway conforming to UL 870. When used for supporting floodlights on wood poles, provide wireway as indicated.

2.2.9 Nameplates

Provide each major component of equipment with a nonferrous metal or engraved plastic nameplate which shows, as a minimum, the manufacturer's name and address, the catalog or style number, the electrical rating in volts, and the capacity in amperes or watts.

2.2.10 Spare Parts

Submit spare parts data for each different item of material and equipment specified, after approval of detail drawings for materials and equipment, and not later than 4 months before the date of beneficial occupancy. Include in data a complete list of parts, special tools, and supplies, with current unit prices and sources of supply.

2.3 COMPONENTS

2.3.1 Protection of Security Lighting System Components

2.3.1.1 Components and Conductors

Protect Security lighting system conductors from damage. Install lighting system conductors in raceways or by means of direct burial, as shown. Where the conductors leave the underground systems, encase the conductors in rigid steel conduit of the indicated size. Provide wire guards to protect security lighting luminaries mounted below 20 feet. House exterior group-located electrical equipment such as time switches, safety switches, and magnetic contactors in a NEMA ICS 6, Type 4 enclosure. Provide an individual enclosure where only one piece of equipment is provided at a location.

2.3.1.2 Tamper Provisions

Provide enclosures, cabinets, housings (other than luminaire housings), boxes, raceways, conduits, and fittings having hinged doors or removable covers, and which contain any part of the security lighting system (including power sources), with corrosion-resistant tamper switches, connected to an Intrusion Detection System (IDS), that initiates an alarm

signal when the door or cover is opened or moved. Make tamper switches inaccessible until the switch is activated. Conceal switch leads and mounting hardware from the exterior of the enclosure. For pull or junction boxes which contain no splices or connections the covers may be protected by 1/4 inch tack welds on four sides of each cover rather than by tamper switches. Affix labels to indicate they contain no connections. Do not indicate on labels that the box is part of the security system.

2.3.2 Cable

Provide all wire and cable not indicated as government furnished equipment, capable of withstanding the jobsite environment for a minimum of 20 years.

2.3.2.1 Insulated Cable

Provide USE type cable conforming to UL 854, with copper conductors and type RHW or XHHW insulation conforming to UL 44, including green ground conductor. Provide cable with insulation of a thickness not less than that given in TABLE 15.1 of UL 854, rated 600 volts. Provide parts of the cable system, such as splices and terminations, rated not less than 600 volts. The size and number of conductors and the number of cables are as indicated. Strand conductors larger than No. 8 AWG.

2.3.2.2 Messenger Cable

Provide a messenger cable system to support aerial cable, including guys, hardware and appurtenances needed to install the messenger cable, and capable of supporting the weight of the lighting system cable with the required messenger cable tensioning without exceeding 30 percent of its breaking strength under 60 degrees F conditions of no ice and no wind. Size the messenger so that ice and wind loading normally encountered at the site does not cause the messenger to exceed 50 percent of its breaking strength. Size appurtenances, guys, and hardware to exceed the rated breaking strength of the messenger cable. Provide galvanized zinc coated steel or aluminum clad steel messenger cables.

2.3.2.3 Bare Copper Conductors

Provide medium-hard-drawn copper conductors conforming to ASTM B2 and ASTM B8.

2.3.3 Electrical Enclosures

Provide metallic enclosures as needed to house the security and CCTV lighting equipment conforming to NEMA ICS 6 and NEMA 250. Provide enclosures with lockable or padlock handles. Deliver keys for lockable enclosures to the Contracting Officer. Provide enclosures as specified or as shown on the drawings.

2.3.3.1 Interior Enclosures

Provide enclosures to house lighting equipment in an interior environment meeting the requirements of a NEMA 12 enclosure as defined in NEMA 250.

2.3.3.2 Exposed-to-Weather Enclosures

Provide enclosures to house lighting equipment in an outdoor environment

meeting the requirements of a NEMA 4 enclosure as defined in NEMA 250.

2.3.4 Illumination

2.3.5 Luminaire Components

Provide luminaire components conforming to the following:

a. Attachments, ANSI C136.3;

b. Voltage classification, ANSI C136.2;

c. Field identification marking, ANSI C136.15;

d. Interchangeability, ANSI C136.6 and ANSI C136.9; and

e. Sockets, ANSI C136.11.

2.3.6 Photometric Distribution Classification

Provide photometrics conforming to ANSI/IES RP-8.

2.3.7 Luminaires, Floodlighting

2.3.7.1 HID and Incandescent

Provide HID lighting fixtures conforming to UL 1598. Provide incandescent lighting fixtures conforming to UL 1598.

2.4 MATERIALS

2.4.1 Corrosion Protection

2.4.1.1 Aluminum Materials

Do not use aluminum.

2.4.1.2 Ferrous Metal Materials

a. Hardware

Provide hot-dip galvanized ferrous metal hardware in accordance with ASTM A153/A153M and ASTM A123/A123M.

b. Equipment

Provide equipment and component items, including but not limited to metal poles and ferrous metal luminaires not hot-dip galvanized or porcelain enamel finished, with corrosion-resistant finishes which withstand 120 hours of exposure to the salt spray test specified in ASTM B117 without loss of paint or release of adhesion of the paint primer coat to the metal surface in excess of 1/16-inch from the test mark, with a scribed test mark and test evaluation rated not less than 7 in accordance with TABLE 1, (procedure A) of ASTM D1654.

Coat cut edges or otherwise damaged surfaces of hot-dip galvanized sheet steel or mill galvanized sheet steel with a zinc rich paint conforming to the manufacturer's standard.

2.4.1.3 Finishing

Painting required for surfaces not otherwise specified and finish painting of items only primed at the factory, are as specified in Section 09 90 00 PAINTS AND COATINGS.

PART 3 EXECUTION

3.1 PREPARATION

3.1.1 Current Site Conditions

Verify that site conditions are in agreement with the design package. Report all changes to the site or conditions that will affect performance of the system to the Government. Do not take any corrective action without written permission from the Government.

3.1.2 Existing Equipment

Connect to and utilize existing lighting equipment and devices as shown. Make written requests and obtain approval prior to disconnecting any control lines and equipment, and creating equipment downtime. Proceed with such work only after receiving Government approval of these requests. If any device fails after work has commenced on that device, diagnose the failure and perform any necessary corrections to the equipment. The Government is responsible for maintenance and repair of Government equipment.

3.2 INSTALLATION

Install all system components, including government furnished equipment, and appurtenances in accordance with the manufacturer's instructions, IEEE C2, and contract documents. Furnish necessary hardware, fixtures, cables, wire, connectors, interconnections, services, and adjustments required for a complete and operable system.

3.2.1 Enclosure Penetrations

Make enclosure penetrations from the bottom unless the system design requires penetrations from other directions. Seal all penetrations of interior enclosures involving transitions of conduit from interior to exterior, and penetrations on exterior enclosures with rubber silicone sealant to preclude the entry of water. Terminate the conduit riser in a hot-dipped galvanized metal cable terminator. Fill the terminator with an approved sealant as recommended by the cable manufacturer, and in such a manner that the cable is not damaged.

3.2.2 Prevention of Corrosion

3.2.2.1 Aluminum

Do not use aluminum in contact with earth or concrete, and where connected to dissimilar metal, protect with approved fittings and treatment.

3.2.2.2 Steel Conduits

Do not install steel conduits within concrete slabs-on-grade. Field wrap steel conduits installed underground or under slabs-on-grade, or penetrating slabs-on-grade, with 0.010 inch thick pipe-wrapping plastic

tape applied with a 50 percent overlap, or provide with a factory-applied plastic resin, epoxy coating. Zinc coating may be omitted from steel conduit which has a factory-applied epoxy coating.

3.2.2.3 Cold Galvanizing

Coat field welds and/or brazing on factory galvanized boxes, enclosures, conduits, etc. with a cold galvanized paint containing at least 95 percent zinc by weight.

3.2.3 Cable Installation

Provide cable and all parts of the cable system, such as splices and terminations, rated not less than 600 volts, with the size and number of conductors and the number of cables as indicated. Provide stranded conductors if larger than No. 8 AWG. Identify each circuit by means of fiber or nonferrous metal tags, or approved equal, in each handhole and junction box, and at each terminal.

3.2.3.1 Splices

Make splices below grade with nonpressure-filled resin systems using transparent, interlocking, self-venting, longitudinally split plastic molds. Make splices above grade with sealed insulated pressure connectors and provide insulation and jacket equal to that of the cable. In order to prevent moisture from entering the splice, cut back jackets to expose the required length of insulation between the jacket and the tapered end of the insulation.

3.2.3.2 Installation in Duct Lines

Install ground and neutral conductors in duct with the associated phase conductors. Make cable splices in handholes only.

3.2.4 Direct Burial

Provide minimum cover depth from top of cable to finished grade 30-inches for direct buried cable, but not less than the depth of the frost line.

3.2.4.1 Trenching

Excavate trenches to the depths required to provide the minimum cable cover, with the bottom of the trench smooth and free of stones and sharp objects. Where the bottom of the trench consists of material other than sand or earth, remove an additional 3-inch layer and replace with a 3-inch layer of sand or stone-free earth compacted to the approximate density of the surrounding firm soil. Unreel the cables unreeled in place along the side of or in the trench and carefully placed on the sand or earth bottom. Pulling cables into a direct-burial trench from a fixed reel position is not permitted. Where cables cross, provide a separation of at least 3-inches, unless the cables are protected by nonmetallic conduit sleeves at the crossing. Make the radius of bends in cables not less than 12 times the diameter of the cable. Do not leave the cables under longitudinal tension. Install the first layer of backfill, 6-inches thick, consisting of sand or stone-free earth. Place one-inch untreated planks, not less than 8-inches in width, or approved equal protection, end to end along the cable run, approximately 3 inches above the cable. Place a 5-mil, brightly colored plastic tape not less than 3-inchesin width and suitably inscribed at not more than 10-feet on centers, or other

approved dig-in warning indication, approximately 12-inches below finished grade levels of trenches. Provide selected backfill of sand or stone-free earth to a minimum depth of 3-inches above cables.

3.2.4.2 Requirements for Installation in Duct

Where indicated on drawing, install cable in duct lines. Install ground and neutral conductors in duct with the associated phase conductors. Install segments of direct-burial cable that cross under new railroad tracks, roads, or paving exceeding 5 feet in width, in plastic, or rubber duct encased in concrete in accordance with paragraph DUCT LINES. Pulling of cable into conduit from a fixed reel position is not permitted. At interfaces with direct-burial cable, center the direct-burial cable in the entrance to the duct, using an approved waterproof, nonhardening mastic compound to facilitate the centering. Where crossing existing railroad tracks, install coated rigid steel conduit under the tracks, in lieu of concrete-encased duct, in accordance with paragraph DUCT LINES in accordance with NFPA 70 and the regulations of the railroad.

3.2.4.3 Location of Cable Splices

Splices in direct-burial cable are not permitted in runs of 500 feet or less or at intervals of less than 500 feet in longer runs except as required for taps. Where cable splices in shorter intervals are required to avoid obstructions or damage to the cable, the location is as approved. Install cable splices in cable boxes or concrete handholes.

3.2.4.4 Markers

Locate cable and cable splice markers near the ends of cables, at each cable splice, approximately every 400 feet along the cable run, and at changes in direction of the cable run. Markers need not be placed along cables laid in relatively straight lines between lighting poles that are spaced less than 400 feet apart. Place markers approximately 2 feet to the right of the cable or cable splice when facing the longitudinal axis of the cable in the direction of the electrical load. Provide concrete markers with a 28 day compressive strength of 2500 psi in accordance with Section 03 30 00 CAST-IN-PLACE CONCRETE. Impress the letter "C" in the top of each marker.

3.2.4.5 Warning Tape

Place direct burial cable below a plastic warning tape buried in the same trench or slot. Place a 5 mil brightly colored plastic tape, not less than 3 inches in width and suitably inscribed at not more than 10 feet on centers with a continuous metallic backing and a corrosion-resistant 1 mil metallic foil core to permit easy location of the buried cable, approximately 12 inches below finished grade.

3.2.5 Messenger Cable

3.2.5.1 Installation

Attach messenger to poles with approved clamps,with not less than 5/8 inch through bolts. Do not exceed 30 percent of messenger cable rated tensioning rated breaking strength under 60 degrees F conditions of no ice and no wind. Stress messengers to a tension higher than the final tension in order to prestretch the cable, so that when the messenger is dead-ended under its final tension and sag, there is minimum variation from the

calculated values.

3.2.5.2 Grounding and Bonding Connections

Ground messengers and guy at corners, dead-ends, and entrances to each facility. Ground at intervals not exceeding 1000 feet. Provide new grounding conductors and electrodes at each ground connection. Fusion weld connections below grade. Fusion weld connections above grade or use UL 467 approved connectors.

3.2.5.3 Grounding Conductors and Electrodes

Provide soft drawn copper ground conductors, having a current capacity of at least 20 percent of that of the messenger to which it is connected, no smaller than No. 6 AWG. Connect the ground conductor to a ground rod of copper clad steel conforming to UL 467 not less than 3/4 inch in diameter by 10 feet in length. After installation is completed, ensure that the top of the ground is approximately 1 foot below finished grade. Protect the ground conductor by half-round wood, plastic, or fiber molding from the ground to a point at least 8 feet above the ground.

3.2.5.4 Ground Resistance Testing

Measure the resistance to ground using the fall-of-potential method described in IEEE 81. Do not exceed 25 ohms maximum resistance under normally dry conditions. Whenever the required ground resistance is not met, provide additional electrodes, as indicated, to achieve the specified ground resistance. Provide additional electrodes 10 feet long spaced a minimum of 10 feet apart, as a single extension type rod, 3/4 inch in diameter, up to 30 feet long driven perpendicular to grade. In high ground resistance, UL listed chemically charged ground rods may be used. If the resultant resistance exceeds 25 ohms measured not less than 48 hours after rainfall, notify the Contracting Officer immediately.

3.2.6 Aerial Cable Splices

Make splices in aerial cable within 3 feet of a pole and place inside a watertight enclosure. Form drip loops at the cable entrance to the enclosure. Place lashing clamps within 12 inches of the enclosure.

3.2.7 Lashing Wire

Wind lashing wire tightly around both the communication cable and the messenger cable by machine methods, with a minimum of one turn per 14 linear inches and not less than the number of turns per linear foot that is recommended by the cable manufacturer for the distance between cable support points and the combined ice and wind loading and extreme wind loading shown or normally encountered for the installed location. Place lashing clamps at all poles and splices.

3.2.8 Stress Loops

Form loops in the aerial cable at all points of connection and at all poles to prevent damage from thermal stress and wind loading. Protect aerial cable from chafing and physical damage with the use of spiral cut tubing and PVC tape, or plastic sleeves.

3.2.9 Connections to Buildings

Extend cables into the various buildings as indicated and properly connect to the indicated equipment. Provide empty conduits to the indicated equipment from a point 5 feet outside the building wall and 2 feet below finished grade . After installation of cables, seal conduits to prevent moisture or gases from entering the building.

3.2.10 Duct Lines

3.2.10.1 Requirements

Provide the numbers and size of ducts as indicated, laying duct lines with a minimum slope of 4 inches/100 feet. Depending on the contour of the finished grade, the high point may be at a terminal, a manhole, a handhole, or between manholes or handholes. Short radius manufactured 90 degree duct bends may be used only for pole or equipment risers, unless specifically indicated as acceptable. The minimum manufactured bend radius is 18 inches for ducts of less than 3 inches in diameter, and 36 inches for duct 3 inches or greater in diameter; for long sweep bends use a minimum radius of 25 feet for a change of direction of more than 5 degrees, either horizontally or vertically. Both curved and straight sections may be used to form long sweep bends,with a maximum curve of 30 degrees using manufactured bends. Provide ducts with end bells when duct lines terminate in manholes or handholes.

3.2.10.2 Treatment

Keep ducts clean of concrete, dirt, or foreign substances during construction. Make field cuts requiring tapers with proper tools and match factory tapers. Use a coupling recommended by the duct manufacturer when an existing duct is connected to a duct of different material or shape. Store ducts to avoid warping and deterioration with ends sufficiently plugged to prevent entry of any water or solid substances. Thoroughly clean ducts before installation. Store plastic ducts on a flat surface and protected from the direct rays of the sun.

3.2.10.3 Concrete Encasement

Provide ducts requiring concrete encasements in compliance with NFPA 70, except for electrical duct bank configurations for ducts 6 inches in diameter, which are determined by calculation and as shown on the drawings. Provide monolithic construction of duct line encasements. Where a connection is made to a previously poured encasement, bond or dowel the new encasement to the existing encasement. At any point, except railroad and airfield crossings, make tops of concrete encasements not less than the cover requirements listed in NFPA 70. At railroad and airfield crossings, encase duct lines with concrete and reinforce as indicated to withstand specified surface landings. Make tops of concrete encasement not less than 5 feet below tops of rails or airfield paving unless otherwise indicated. Where ducts are jacked under existing pavement, install rigid steel conduit. To protect the corrosion-resistant conduit coating, pre-drilling or installing conduit inside a larger iron pipe sleeve (jack-and-sleeve) is required. For crossings of existing railroads and airfield pavements greater than 50 feet in length, use the pre-drilling method or the jack-and-sleeve method. Use separators or spacing blocks of steel, concrete, plastic, or a combination of these materials placed not more than 4 foot on centers. Securely anchor ducts to prevent movement during the placement of concrete, and stagger joints

at least 6 inches vertically.

3.2.10.4 Installation of Couplings

Make joints in each type of duct in accordance with the manufacturer's recommendation for the particular type of duct and coupling selected and as approved. Make duct joints by brushing a plastic solvent on insides of plastic coupling fittings and on outsides of duct ends, then slip each duct and fitting together with a quick 1/4 turn to set the joint tightly.

3.2.10.5 Concrete

Provide concrete work as specified in Section 03 30 00 CAST-IN-PLACE CONCRETE, with plain concrete strength of, 2500 psi at 28 days, and reinforced concrete strength of 3000 psi at 28 days. Provide monolithic duct line encasement construction. Where a connection is made to an existing duct line, bond the concrete encasement or dowel to the existing encasement.

3.2.10.6 Duct Line Markers

Provide duct line markers at the ends of long duct line stubouts or for other duct locations that are indeterminate because of duct curvature or terminations at completely below-grade structures. In addition to markers, place a 5 mil brightly colored plastic tape, not less than 3 inches in width and suitably inscribed at not more than 10 feet on centers with a continuous metallic backing and a corrosion-resistant 1 mil metallic foil core to permit easy location of the duct line, approximately 12 inches below finished grade levels of such lines.

3.2.11 Handholes

Determine the exact locations after carefully considering the locations of other utilities, grading, and paving. Secure approval of exact before construction is started.

3.2.11.1 Construction

Construct handholes as indicated on drawings, including appurtenances, with top, walls, and bottom consisting of reinforced concrete. Provide monolithic walls and bottom. Provide 3000 psi concrete at 28 days. Precast concrete handholes having the same strength and inside dimensions as cast-in-place concrete handholes may be used. In paved areas, make the top of entrance covers flush with the finished surface of the paving. In unpaved areas, set the top of entrance covers approximately 1/2 inch above the finished grade. Where finished grades are in cut areas, install unmortared brick between the top of handhole and entrance frame to temporarily elevate the entrance cover to existing grade level. Where duct lines enter walls, the sections of duct may be cast in the concrete or may enter the wall through a suitable opening. Caulk the openings around entering duct lines tight with lead wool or other approved material.

3.2.11.2 Appurtenances

Provide the following appurtenances for each handhole.

3.2.11.3 Cable Pulling-in Irons

Install a cable pulling-in iron in the wall opposite each duct line

entrance.

3.2.11.4 Ground Rods

In each handhole, at a convenient point close to the wall, drive a ground rod conforming to paragraph GROUNDING CONDUCTORS AND ELECTRODES, into the earth before the floor is poured; with approximately 4 inches of the ground rod extending above the floor after pouring. When precast concrete units are used, the top of the ground rod may be below the floor; bring a No. 1/0 AWG copper ground conductor inside through a watertight sleeve in the wall.

3.2.12 Lighting

3.2.12.1 Lamps

Deliver lamps of the proper type, wattage, and voltage rating to the project in the original containers and install in the fixtures just before completion of the project.

3.2.12.2 Fixture Installation

Provide special fixtures as indicated on drawings. Illustrations shown on the drawings are indicative of the general type desired and are not intended to restrict selection of fixtures to any particular manufacturer. Fixtures of similar design, equivalent light-distribution and brightness characteristics, and equal finish and quality are acceptable as approved.

a. Accessories

Install accessories such as straps, mounting plates, nipples, or brackets as required for proper installation.

b. In-Line Fuses

Provide an in-line fuse for each fixture.

c. Special Fixtures

The types of special fixtures are designated by letters and numbers. For example, SP-1 denotes special type 1.

3.2.13 Transformer Installation

Install transformers for lighting fixtures on steel poles in the transformer base. Provide a transformer base for poles that require transformers. Securely mount transformers to steel supporting plates and bolt to wood poles.

3.2.14 CCTV Alarm Interface

Furnish and install an alarm interface with the lighting control system, compatible with the CCTV alarm annunciation system. Monitor alarm closures for processing by the system CPU with the alarm. Provide alarm inputs to the alarm interface by relay contact or through an TIA-232 interface, modular and allowing for system expansion. Configure the alarm interface to be installed at the site to handle all illustrated alarm points, with an expansion capability of not less than 10 percent. Provide

an output to actuate a video recorder.

3.3 FIELD QUALITY CONTROL

3.3.1 Operating Test

Submit operating test procedures and reports for the operating test to the Contracting Officer for approval. After receipt of written approval of the test procedures, schedule the tests. Deliver the final Operating Test procedures report after completion of the tests.

After the installation is completed and at such time as the Contracting Officer may direct, conduct an operating test for approval, in the presence of the Contracting Officer. Demonstrate that the equipment operates in accordance with the requirements specified. Furnish instruments and personnel required for the test The Government will furnish the necessary electric power.

3.3.2 Ground Resistance Measurements

Submit the measured resistance to ground of each separate grounding installation,in writing, indicating the location of the rods, the resistance of the soil in ohms per millimeter and the soil conditions at the time the measurements were made.

Measure the resistance to ground by the fall-of-potential method described in IEEE 81.

3.4 CLOSEOUT ACTIVITIES

3.4.1 Operations and Maintenance Manuals

Submit a draft copy of the operation and maintenance manuals, prior to beginning the tests for use during site testing. Submit final copies of the manuals as specified bound in hardback, loose-leaf binders, within 30 days after completing the field test. Update the draft copy used during site testing with any changes required, prior to final delivery of the manuals. Identify each manual's contents on the cover. Include names, addresses, and telephone numbers of each subcontractor installing equipment and systems, and nearest service representatives for each item of equipment for each system. Provide the manuals with a table of contents and tab sheets. Place tab sheets at the beginning of each chapter or section and at the beginning of each appendix. Include, upon delivery of the final copies, modifications made during installation checkout and acceptance.

3.4.2 Record Drawings

Maintain and keep up to date, a separate set of drawings, elementary diagrams and wiring diagrams of the lighting to be used for "record" drawings, showing all changes and additions to the lighting system. In addition to being complete and accurate, keep this set of drawings separate and do not use for installation purposes. Upon completion of the record drawings, a representative of the Government will review the as-built work with the Contractor. If the as-built work is not complete, the Contractor will be so advised and complete the work as required.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 27 - COMMUNICATIONS

SECTION 27 05 13.43

TELEVISION DISTRIBUTION SYSTEM

PART 1 GENERAL

1.1 REFERENCES
1.2 DEFINITIONS
1.2.1 Television Distribution System
1.2.2 Headend
1.2.3 Distribution System
1.2.4 Cable
1.3 SYSTEM DESCRIPTION
1.3.1 Headend
1.3.2 Distribution System
1.3.3 Cable
1.3.4 System Components
1.3.4.1 System Bandwidth
1.3.5 System Performance
1.3.5.1 Receiver Termination Signal Level
1.3.5.2 Distribution System
1.3.5.3 System Tolerance
1.4 SUBMITTALS
1.5 QUALITY ASSURANCE
1.5.1 Wiring Diagrams and Installation Details
1.5.2 Television Distribution System Loss Calculations
1.5.3 Operational Test Plan
1.5.4 Operational Test Procedures
1.5.5 Connector Installation

PART 2 PRODUCTS

2.1 ELECTRONIC EQUIPMENT
2.2 HEADEND EQUIPMENT
2.2.1 Headend Amplifiers
2.2.2 Attenuators
2.2.3 Power Supplies
2.3 DISTRIBUTION EQUIPMENT
2.3.1 Cables and Associated Hardware
2.3.1.1 Trunk Cable
2.3.1.2 Drop Cable
2.3.1.3 Low Voltage Patient Television Drop Cable
2.3.2 Category 6 Drop Cable
2.3.3 Category 6 Patch Cords
2.3.4 Terminators
2.3.5 Splitters/Combiners
2.3.6 Line Taps
2.3.7 Coaxial Outlets
2.3.8 Coaxial Connectors
2.3.9 Tilt Compensator

2.4 BACKBOARDS

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Distribution System
3.1.1.1 Trunk, Feeder, and Drop Cable
3.1.1.2 Splitters, Directional Couplers, Attenuators, Amplifiers
3.2 FIELD QUALITY CONTROL
3.2.1 System Pretest
3.2.2 Acceptance Tests
3.3 OPERATION AND MAINTENANCE MANUALS

-- End of Section Table of Contents --

SECTION 27 05 13.43

TELEVISION DISTRIBUTION SYSTEM

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE C2	(2023) National Electrical Safety Code
IEEE C62.41.1	(2002; R 2008) Guide on the Surges Environment in Low-Voltage (1000 V and Less) AC Power Circuits
IEEE C62.41.2	(2002) Recommended Practice on Characterization of Surges in Low-Voltage (1000 V and Less) AC Power Circuits

NATIONAL CABLE AND TELECOMMUNICATIONS ASSOCIATION (NCTA)

NCTA RP	(1989) NCTA Recommended Practices for Measurements on Cable Television Systems

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2023) National Electrical Code

U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)

47 CFR 76.605	Technical Standards

UNDERWRITERS LABORATORIES (UL)

UL 969	(2017; Reprint Mar 2018) UL Standard for Safety Marking and Labeling Systems
UL 1581	(2001; Reprint Jun 2021) UL Standard for Safety Reference Standard for Electrical Wires, Cables, and Flexible Cords
UL 1666	(2007; Reprint Sep 2021) UL Standard for Safety Test for Flame Propagation Height of Electrical and Optical-Fiber Cables Installed Vertically in Shafts

1.2 DEFINITIONS

1.2.1 Television Distribution System

The television distribution system system, commonly referred to as cable

television, is a network of cables, headend, electronic and passive components that process and amplify television (TV) signals for distribution of adequate signals to each receiver from the headend equipment to the individual television outlets and provides distortion-free signal to TV sets by isolating each receiver from the system an providing the proper amount of signal to each set.

1.2.2 Headend

The connection point between television distribution system equipment and equipment provided by the local television service provider.

1.2.3 Distribution System

Distribution system transports and delivers adequate signals to each receiver. Provides distortion-free signal to TV sets by isolating each receiver from the system and by providing proper amount of signal to each set.

1.2.4 Cable

Trunk and feeder cables are low-loss cables used to transport the desired signal from the headend equipment to the telecommunications room in the area to be served. These cables are used to transport signal from the telecommunications room into close proximity to a number of user locations in excess of 200 feet from the telecommunications room. Drop cables are used to transport the desired signal used from the telecommunications closet room to the wall outlet.

1.3 SYSTEM DESCRIPTION

1.3.1 Headend

Contractor shall provide interior equipment up to headend located at the interior television distribution system rack.

1.3.2 Distribution System

Distribution system shall be a star topology utilizing a coaxial trunk cable and category 6 UTP drop cables.

1.3.3 Cable

Provide drop cables to transport the desired signal from the telecommunications room to the outlet.

1.3.4 System Components

System shall provide high quality TV signals to all outlets. Provide any combination of items specified herein to achieve required performance, subject to approvals, limitations, acceptance test, and other requirements specified herein. System shall include amplifiers, splitters, combiners, line taps, cables, outlets, tilt compensators and all other parts, components, and equipment necessary to provide a complete and usable system.

1.3.4.1 System Bandwidth

a. Downstream: 50-1000 MHz minimum.

b. Upstream 5-40 MHz minimum.

1.3.5 System Performance

System shall be in compliance with 47 CFR 76.605.

1.3.5.1 Receiver Termination Signal Level

Each termination for a TV receiver must have a minimum signal level of 0 decibel millivolts (dBmV) (1000 microvolts) at 55 MHz and of 0 dBmV (1000 microvolts) at 1000 MHz and a maximum signal of 15 dBmV or a level not to overload the receiver for the entire system bandwidth.

1.3.5.2 Distribution System

a. Modulation distortion at power frequencies: 4 percent or less hum distortion;

b. Composite third order distortion for:

(1) CW carriers: 53 dB.

(2) Modulated carriers: 59 dB.

c. Subscriber terminal isolation: 18 dB or greater.

d. Carrier to second order beat ratio: 60 dB.

e. Amplitude characteristic:within a range of plus or minus 2 decibels from 0.75 MHz to 5.0 MHz above the lower boundary frequency of the cable television channel, referenced to the average of the highest and lowest amplitudes within these frequency boundaries.

f. Visual, aural carrier level, 24-hour variation: 47 CFR 76.605, subpart (a), rules (4), (5), and (6).

g. Frequency determination: 47 CFR 76.605, subpart (a), rules (1),(2), and (3).

1.3.5.3 System Tolerance

The system must not show a serious loss of carrier to noise when the system levels are lowered 3 dB below normal or a significant distortion when the levels are increased 3 dB above normal, as observed on a TV set located at the far end extremities of the system.

1.4 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Television Distribution System Wiring Diagrams And Installation Details; G

Television Distribution System Components; G

SD-03 Product Data

Attenuators; G

Cables, including Trunk, Feeder, and Drop; G

Terminators; G

Splitters/Combiners; G

Line Taps; G

Coaxial Outlets; G

Coaxial Connectors; G

Tilt Compensator; G

Submittals for each manufactured item must be the current manufacturer's descriptive literature of catalog products, equipment drawings, diagrams, performance and characteristics curves, and catalog cuts.

SD-05 Design Data

Television Distribution System Loss Calculations; G

SD-06 Test Reports

Operational Test Plan; G

Operational Test Procedures; G

System Pretest; G

Acceptance Tests; G

SD-08 Manufacturer's Instructions

Connector Installation; G

SD-10 Operation and Maintenance Data

Operation and Maintenance Manuals; G

Submit Data Package 5 for each component in accordance with requirements of Section 01 78 23 OPERATION AND MAINTENANCE DATA.

1.5 QUALITY ASSURANCE

1.5.1 Wiring Diagrams and Installation Details

Illustrate how each item of equipment functions in the system and include an overall system schematic indicating the relationship of television distribution system units on one diagram. Drawings must include wiring diagrams and installation details of equipment indicating proposed locations, layout and arrangements, and other items that must be shown to

ensure coordinated installation.

1.5.2 Television Distribution System Loss Calculations

Calculations must verify that the system does not exceed the loss values specified in dBmV at the input of all active devices and the receiver terminations. Provide a drawing displaying all distribution network calculations. The drawing should accurately show taps, splitters, outlets, and the type and length of all trunk, feeder, and drop cables. The drawing must show how many taps, splitters, or outlets are served by each tap or splitter.

1.5.3 Operational Test Plan

Test plan must define tests required to ensure that the system meets technical, operational, and performance specifications. Test plan must be based on NCTA RP and be in accordance with FCC proof of performance requirements. Test plan must include plan for testing for signal leakage. Provide test requirements and guidelines.

1.5.4 Operational Test Procedures

Use test plan and design documents to develop test procedures. Procedures must consist of detailed instructions for a test setup, execution, and evaluation of test results.

1.5.5 Connector Installation

Provide manufacturer's instructions for installing connectors.

PART 2 PRODUCTS

2.1 ELECTRONIC EQUIPMENT

Electronic components of similar type must be produced and designed by the same manufacturer as major components of the equipment and must have the manufacturer's name and model permanently attached. Equipment must function properly as a complete integrated system. Equipment must be shielded. The system must be designed to operate within 5 to 1000 MHz bandwidth using 1000 MHz passive devices and a minimum of 1000 MHz active devices.

2.2 HEADEND EQUIPMENT

2.2.1 Headend Amplifiers

Provide broadband distribution amplifiers. Amplifiers must amplify broadband signals from 40 to 1000 MHz. Amplifiers must be bidirectional with variable slope and gain control.

2.2.2 Attenuators

Provide attenuators to equalize signal levels, when required. Variable attenuators are not permitted.

2.2.3 Power Supplies

Power supplies must contain a current limiter circuit to protect against short circuits on the radio frequency (RF) line. Provide overvoltage

protection to protect solid state equipment from line surges and induced voltages, in accordance with IEEE C62.41.1 and IEEE C62.41.2.

2.3 DISTRIBUTION EQUIPMENT

2.3.1 Cables and Associated Hardware

Cabling shall be UL listed for the application and shall comply with NFPA 70. Provide a labeling system for cabling as required by UL 969. Cabling manufactured more than 12 months prior to date of installation shall not be used.

2.3.1.1 Trunk Cable

UL 1666. Provide trunk cable with an NFPA 70 rating of CATVR.

a. Provide RG-11 coaxial cable with the following characteristics:

(1) 14 AWG copper-clad steel center conductor.

(2) Gas injected foam polyethylene dielectric with nominal 0.28 inches outer diameter.

(3) Bonded foil inner-shield and 60 percent aluminum braid.

(4) 75 ohms impedance.

(5) 82 to 85 percent nominal velocity of propagation.

(6) Black PVC jacket

(7) Maximum attenuation characteristics:

MHz	DB/100 ft
5	0.38
55	0.96
300	2.25
350	2.42
450	2.86
500	2.90
600	3.18
750	3.65
1000	4.35

b. Provide 625 Series cable with an NFPA 70 rating of CATVR and the following characteristics:

(1) Copper-clad aluminum center conductor

(2) Seamless aluminum tubing shield

(3) Expanded polyethylene dielectric

(4) 75 ohms impedance

(5) Nominal diameter over outer conductor: 0.625 inches.

(6) Maximum attenuation at 20 degrees C and 1000 MHz: 2.07 dB/100 feet

(7) Black medium density polyethylene jacket

(8) Nominal 87 percent velocity of propagation

2.3.1.2 Drop Cable

UL 1581. Provide RG 6 coaxial cable with an NFPA 70 rating of CATV and with the following characteristics:

a. No. 18 AWG copper-clad steel center conductor.

b. Bonded foil inner-shield and 90 percent aluminum braid.

c. Characteristic impedance of 75 ohms.

d. Foam FEP dielectric

e. Nominal capacitance, conductor to shield, of 16.2 pf per 100 ft .

f. Maximum operating voltage of 350 V RMS.

g. Maximum attenuation:

CATV	
MHz	DB/100 ft
10	0.81
50	1.46
100	2.05
200	2.83
400	4.0
500	4.53
700	6.0
1000	7.3

h. PVC low smoke polymer or FEP jacket.

i. 100 percent sweep testing from 5 MHz to a minimum of 1000 MHz.

2.3.1.3 Low Voltage Patient Television Drop Cable

UL 1581. Provide RG 6 coaxial cable with an NFPA 70 rating of CATV and with the following characteristics:

a. No. 18 AWG solid copper center conductor.

b. Aluminum/Polyesetr/Aluminum tape 100 percent coverage inner-shield and tinned copper outer braid with 60 percent coverage.

c. Characteristic impedance of 75 ohms.

d. Foam FEP dielectric

e. Nominal capacitance, conductor to shield, of 16.2 pf per ft.

f. Maximum operating voltage of 300 V RMS.

g. Maximum attenuation:

CATV	
MHz	DB/100 ft
10	0.70
50	1.5
100	2.0
200	2.8
400	4.0
700	5.3
900	6.1
1000	6.5
1500	8.3

h. PVC low smoke polymer or FEP jacket.

i. 100 percent sweep testing from 5 MHz to a minimum of 1000 MHz.

2.3.2 Category 6 Drop Cable

Provide as indicated on the drawings and 27 10 00 BUILDING TELECOMMUNICATIONS CABLING SYSTEM.

2.3.3 Category 6 Patch Cords

Provide patch cords, as complete assemblies, with matching connectors as specified in 27 10 00 BUILDING TELECOMMUNICATIONS CABLING SYSTEM. Patch cords shall meet minimum performance requirements specified in 27 10 00 BUILDING TELECOMMUNICATIONS CABLING SYSTEM for cables, cable length and hardware specified.

2.3.4 Terminators

Coaxial terminators shall be rated for 75 ohms and 1/4 watt. Category 6 port terminators shawl be plug-in hub type and shall have integral 8-pin modular connector.

2.3.5 Splitters/Combiners

Use splitters/combiners with characteristics equal to or exceeding the characteristics listed in this paragraph over the entire operating band. All unused outlets must be terminated with 75-ohm terminators.

a. Peak to Valley: Not to exceed 1 dB across bandwidth of device.

b. Return loss: 18 dB minimum.

c. Bandwidth: 5-1000 Mh

2.3.6 Line Taps

Line taps shall have 18 dB minimum isolation from each tap to the thru-line.Pressure tapoffs are not permitted. Taps shall be rated from 5 to 1000 MHz and shall have a peak to valley not to exceed 1 dB to 1 GHz.

2.3.7 Coaxial Outlets

Provide flush mounted, 75-ohm, F-type connector outlets rated from 5 to 1000 MHz in standard electrical outlet boxes.

2.3.8 Coaxial Connectors

Provide one piece connectors. Trunk and feeder cable connectors shall be pin type. Drop cable connectors shall be feed thru type.

2.3.9 Tilt Compensator

Provide tilt compensators as required.

2.4 BACKBOARDS

Provide void-free, fire rated interior grade plywood, 3/4 inch thick, 4 by 8 feet. Backboards shall be painted with a gray, nonconductive fire-resistant overcoat. Do not cover the fire stamp on the backboard.

PART 3 EXECUTION

3.1 INSTALLATION

3.1.1 Distribution System

Distribution system shall conform to requirements specified herein. Installation shall be in accordance with IEEE C2 and NFPA 70.

3.1.1.1 Trunk, Feeder, and Drop Cable

Provide cable to grounding blocks, to line taps, and to outlets.

3.1.1.2 Splitters, Directional Couplers, Attenuators, Amplifiers

Install in accordance with manufacturer's written instructions.

3.2 FIELD QUALITY CONTROL

3.2.1 System Pretest

Upon completing installation of the television distribution system, the Contractor shall align and balance the system and shall perform complete pretesting. During the system pretest, Contractor, utilizing the approved spectrum analyzer or signal level meter, shall verify that the system is fully operational and meets all the system performance requirements of the specification. Contractor shall test the signal loss in dBmV at 55, 151, 547, and 1000 MHz. The signal levels shall be 0 dBmV (1000 microvolts), minimum. The signal shall not exceed 15 dBmV over the entire system bandwidth. Any deficiencies found shall be corrected and revalidated by follow up testing. Contractor shall measure and record the video and audio carrier levels at each of the frequency levels specified at each of the following points in the system:

a. Furthest outlet from communications room.

b. A random sampling of 25 percent of the outletsfrom communications room.

c. At each outlet.

3.2.2 Acceptance Tests

Contractor shall notify the Contracting Officer of system readiness 10 days prior to the date of acceptance testing. Contractor shall also coordinate with the local television service provider and allow them to attend witness tests. The television distribution system shall be tested in accordance with the approved test plan in the presence of the Contracting Officer's representative to certify acceptable performance. System test shall verify that the total system meets all the requirements of the specification and complies with the specified standards. Contractor shall verify that no signal leakage exists in conformance with NCTA RP and 47 CFR 76.605. System leakage shall also be tested at the headend location with signal applied to system. Deficiencies revealed by the testing shall be corrected on the housing units sampled as well as on the outlets not sampled and revalidated by follow-up testing. Contractor shall conduct testing at each of the following points in the system:

a. Furthest outlet from communications room.

b. A random sampling of 25 percent of the outlets from telecommunications room as designated by the Contracting Officer.

c. At each outlet.

3.3 OPERATION AND MAINTENANCE MANUALS

Submit commercial, off-the-shelf manuals for operation, installation, configuration, and maintenance of products provided as a part of the cable television premises distribution system.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 27 - COMMUNICATIONS

SECTION 27 05 28.36 40

CABLE TRAYS FOR COMMUNICATIONS SYSTEMS

PART 1 GENERAL

1.1 REFERENCES
1.2 ADMINISTRATIVE REQUIREMENTS
1.2.1 Pre-Installation Meetings
1.3 SUBMITTALS
1.4 QUALITY CONTROL

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION
2.2 FABRICATION
2.3 COMPONENTS
2.3.1 Supports
2.4 MATERIALS

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Manufacturer's Instructions
3.1.2 Installation Drawings
3.1.3 Grounding

-- End of Section Table of Contents --

SECTION 27 05 28.36 40

CABLE TRAYS FOR COMMUNICATIONS SYSTEMS

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ASTM INTERNATIONAL (ASTM)

ASTM A1008/A1008M	(2021a) Standard Specification for Steel, Sheet, Cold-Rolled, Carbon, Structural, High-Strength Low-Alloy, High-Strength Low-Alloy with Improved Formability, Solution Hardened, and Bake Hardenable

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA VE 1	(2017) Metal Cable Tray Systems
NEMA VE 2	(2018; ERTA 1-2 2018) Cable Tray Installation Guidelines

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2023) National Electrical Code

1.2 ADMINISTRATIVE REQUIREMENTS

1.2.1 Pre-Installation Meetings

The Contracting Officer will schedule a pre-installation meeting within 30 days of contract award. Submit fabrication drawings for review and approval.

Submit manufacturer's product data for the following items:

a. Cable Trays

b. Supports

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Fabrication Drawings; G

Installation Drawings; G

SD-03 Product Data

Cable Trays; G

Supports; G

SD-08 Manufacturer's Instructions

Manufacturer's Instructions

1.4 QUALITY CONTROL

Comply with NEMA VE 1.

Comply with NEC, requirements that apply to the construction and installation of cable tray and cable channel systems (Article 392 NEC).

Provide products that are UL-classified and labeled with the UL classification mark.

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION

Provide ladder cable trays consisting of two longitudinal side members connected by individual transverse members.

Provide trough cable trays consisting of continuous one-piece ventilated-bottom sections contained within longitudinal side members.

Provide channel cable trays consisting of one-piece ventilated channel sections.

2.2 FABRICATION

Submit fabrication drawings for cable trays. Ensure the drawings contain details showing the fabrication and assembly details performed in the factory.

Before assembly, use an antioxidant compound to coat the contact surfaces of trays. Ensure that the finishes of edges, fittings, and hardware are free from burrs and sharp edges. Include splice and end plates, dropouts, and miscellaneous hardware.

2.3 COMPONENTS

2.3.1 Supports

Permit both vertical and horizontal adjustment, where possible on supports and hangers. Provide an adequate bearing surface for the tray on the horizontal and vertical tray supports, and ensure that the surface can accommodate holddown clamps or fasteners. Provide a means, other than friction, for securely fastening cable trays to supports.

Provide support for cable trays at intervals of no more than 6 -foot. Place supports for horizontal-elbow tray fittings within 2 -feet of each fitting extremity and as recommended by the cable tray manufacturer.

Ensure that the cable trays can carry at least 150 pounds per linear foot when supported at 6 -foot intervals. Ensure that the tray fittings have a load-carrying capacity that is equal to or greater than that of straight tray sections. Ensure that the radius of tray fittings is based on the minimum bending radius of the cables, as specified by the cable manufacturer.

2.4 MATERIALS

Provide cable trays constructed of high-strength corrosion-resistant aluminum Alloy No. 5052-H32 in accordance with ASTM A1008/A1008M and that has a zinc coating which was applied after fabrication.

PART 3 EXECUTION

Comply with NEMA VE 2 for cable tray installation.

3.1 INSTALLATION

3.1.1 Manufacturer's Instructions

Submit the manufacturer's instructions for cable trays, including special provisions required to install equipment components and system packages. Ensure that the instructions specify impedances, hazards and safety precautions.

3.1.2 Installation Drawings

No later than 30 calendar days before shipment, submit installation drawings to the Contracting Officer for approval. Coordinate drawings with those being used for all other work in the immediate area to ensure that this other work does not conflict with the installation. Include the layout of the cable tray work and details on both horizontal and vertical supports as specified in the paragraph SUPPORTS.

3.1.3 Grounding

Provide properly grounded cable trays by means that has a low-resistance conductor of sufficient capacity, and that is no smaller than No. 3/0 AWG aluminum. Bond the grounding conductor to cable tray sections and fittings by compatible bolted connections. Consider cable tray sections in tandem assembly as having electrical continuity when these sections are bonded with appropriate high-strength bolts. Provide permanent and continuous effective grounding with an impedance that is low enough to limit the potential above ground and to facilitate operation of overcurrent devices in the circuit. Provide grounding and bonding for cable trays in accordance with NFPA 70.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 27 - COMMUNICATIONS

SECTION 27 10 00

BUILDING TELECOMMUNICATIONS CABLING SYSTEM

PART 1 GENERAL

1.1 REFERENCES
1.2 DEFINITIONS
1.2.1 Campus Distributor (CD)
1.2.2 Building Distributor (BD)
1.2.3 Floor Distributor (FD)
1.2.4 Telecommunications Room (TR)
1.2.5 Entrance Facility (EF) (Telecommunications)
1.2.6 Equipment Room (ER) (Telecommunications)
1.2.7 Open Cable
1.2.8 Open Office
1.2.9 Pathway
1.3 SYSTEM DESCRIPTION
1.4 SUBMITTALS
1.5 QUALITY ASSURANCE
1.5.1 Shop Drawings
1.5.1.1 Telecommunications Drawings
1.5.1.2 Telecommunications Space Drawings
1.5.2 Telecommunications Qualifications
1.5.2.1 Telecommunications Contractor
1.5.2.2 Key Personnel
1.5.2.3 Minimum Manufacturer Qualifications
1.5.3 Test Plan
1.5.4 Regulatory Requirements
1.5.5 Standard Products
1.5.5.1 Alternative Qualifications
1.5.5.2 Material and Equipment Manufacturing Date
1.6 DELIVERY AND STORAGE
1.7 ENVIRONMENTAL REQUIREMENTS
1.8 WARRANTY
1.9 MAINTENANCE
1.9.1 Operation and Maintenance Manuals
1.9.2 Record Documentation

PART 2 PRODUCTS

2.1 COMPONENTS
2.2 TELECOMMUNICATIONS PATHWAY
2.3 TELECOMMUNICATIONS CABLING
2.3.1 Backbone Cabling
2.3.1.1 Backbone Optical Fiber
2.3.2 Horizontal Cabling
2.3.2.1 Horizontal Copper
2.3.2.2 Horizontal Optical Fiber
2.3.3 Work Area Cabling

2.3.3.1 Work Area Copper
2.4 TELECOMMUNICATIONS SPACES
2.4.1 Backboards
2.4.2 Equipment Support Frame
2.4.3 Cable Guides
2.4.4 Patch Panels
2.4.4.1 Modular to 110 Block Patch Panel
2.4.4.2 Fiber Optic Patch Panel
2.4.5 Optical Fiber Distribution Panel
2.5 TELECOMMUNICATIONS OUTLET/CONNECTOR ASSEMBLIES
2.5.1 Outlet/Connector Copper
2.5.2 Optical Fiber Adapters(Couplers)
2.5.3 Optical Fiber Connectors
2.5.4 Cover Plates
2.6 GROUNDING AND BONDING PRODUCTS
2.7 FIRESTOPPING MATERIAL
2.8 TESTS, INSPECTIONS, AND VERIFICATIONS
2.8.1 Factory Reel Tests

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Cabling
3.1.1.1 Open Cable
3.1.1.2 Horizontal Cabling
3.1.2 Pathway Installations
3.1.3 Service Entrance Conduit, Underground
3.1.4 Cable Tray Installation
3.1.5 Work Area Outlets
3.1.5.1 Terminations
3.1.5.2 Cover Plates
3.1.5.3 Cables
3.1.5.4 Pull Cords
3.1.6 Telecommunications Space Termination
3.1.6.1 Patch Panels
3.1.6.2 Equipment Support Frames
3.1.7 Electrical Penetrations
3.1.8 Grounding and Bonding
3.2 LABELING
3.2.1 Labels
3.2.2 Cable
3.2.3 Termination Hardware
3.3 FIELD APPLIED PAINTING
3.3.1 Painting Backboards
3.4 FIELD FABRICATED NAMEPLATE MOUNTING
3.5 TESTING
3.5.1 Telecommunications Cabling Testing
3.5.1.1 Inspection
3.5.1.2 Verification Tests
3.5.1.3 Performance Tests

-- End of Section Table of Contents --

SECTION 27 10 00

BUILDING TELECOMMUNICATIONS CABLING SYSTEM

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ELECTRONIC COMPONENTS INDUSTRY ASSOCIATION (ECIA)

ECIA EIA/ECA 310-E	(2005) Cabinets, Racks, Panels, and Associated Equipment

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 100	(2000; Archived) The Authoritative Dictionary of IEEE Standards Terms

INSULATED CABLE ENGINEERS ASSOCIATION (ICEA)

ICEA S-83-596	(2021) Indoor Optical Cable
ICEA S-90-661	(2021) Category 3 and 5E Individually Unshielded Twisted Pairs, Indoor Cables (With or Without an Overall Shield) for Use in General Purpose and LAN Communications Wiring Systems

NATIONAL ELECTRICAL CONTRACTORS ASSOCIATION (NECA)

NECA/BICSI 568	(2006) Standard for Installing Building Telecommunications Cabling

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

ANSI/NEMA WC 66	(2019) Performance Standard for Category 6 and Category 7 100 Ohm Shielded and Unshielded Twisted Pairs

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2023) National Electrical Code

TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)

TIA-455-21	(1988a; R 2012) FOTP-21 - Mating Durability of Fiber Optic Interconnecting Devices
TIA-526-7	(2015a; R 2022) Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant, Adoption of IEC 61280-4-2

	edition 2: Fibre-Optic Communications Subsystem Test Procedures - Part 4-2: Installed Cable Plant - Single-Mode Attenuation and Optical Return Loss Measurement
TIA-526-14	(2015c) OFSTP-14A Optical Power Loss Measurements of Installed Multimode Fiber Cable Plant
TIA-568.0	(2020e) Generic Telecommunications Cabling for Customer Premises
TIA-568.1	(2020e) Commercial Building Telecommunications Infrastructure Standard
TIA-568.2	(2018d) Balanced Twisted-Pair Telecommunications Cabling and Components Standards
TIA-568.3	(2016d; Add 1 2019) Optical Fiber Cabling Components Standard
TIA-569	(2019e; Add 1 2022) Telecommunications Pathways and Spaces
TIA-606	(2021d) Administration Standard for Telecommunications Infrastructure
TIA-607	(2019d) Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises
TIA-1152	(2016; R 2021) Requirements for Field Test Instruments and Measurements for Balanced Twisted-Pair Cabling
TIA/EIA-598	(2014D; Add 2 2018) Optical Fiber Cable Color Coding
TIA/EIA-604-10	(2002a) FOCIS 10 Fiber Optic Connector Intermateability Standard - Type LC

U.S. FEDERAL COMMUNICATIONS COMMISSION (FCC)

FCC Part 68	Connection of Terminal Equipment to the Telephone Network (47 CFR 68)

UNDERWRITERS LABORATORIES (UL)

UL 50	(2015) UL Standard for Safety Enclosures for Electrical Equipment, Non-Environmental Considerations
UL 444	(2017; Reprint Jun 2021) UL Standard for Safety Communications Cables
UL 467	(2022) UL Standard for Safety Grounding and Bonding Equipment

UL 514C	(2014; Reprint Feb 2020) UL Standard for Safety Nonmetallic Outlet Boxes, Flush-Device Boxes, and Covers
UL 723	(2018) UL Standard for Safety Test for Surface Burning Characteristics of Building Materials
UL 969	(2017; Reprint Mar 2018) UL Standard for Safety Marking and Labeling Systems
UL 1286	(2022) UL Standard for Safety Office Furnishings
UL 1666	(2007; Reprint Sep 2021) UL Standard for Safety Test for Flame Propagation Height of Electrical and Optical-Fiber Cables Installed Vertically in Shafts
UL 1863	(2004; Reprint Oct 2019) UL Standard for Safety Communication Circuit Accessories

1.2 DEFINITIONS

Unless otherwise specified or indicated, electrical and electronics terms used in this specification shall be as defined in TIA-568.1, TIA-568.2, TIA-568.3, TIA-569, TIA-606 and IEEE 100 and herein.

1.2.1 Campus Distributor (CD)

A distributor from which the campus backbone cabling emanates. (International expression for main cross-connect (MC).)

1.2.2 Building Distributor (BD)

A distributor in which the building backbone cables terminate and at which connections to the campus backbone cables may be made. (International expression for intermediate cross-connect (IC).)

1.2.3 Floor Distributor (FD)

A distributor used to connect horizontal cable and cabling subsystems or equipment. (International expression for horizontal cross-connect (HC).)

1.2.4 Telecommunications Room (TR)

An enclosed space for housing telecommunications equipment, cable, terminations, and cross-connects. The room is the recognized cross-connect between the backbone cable and the horizontal cabling.

1.2.5 Entrance Facility (EF) (Telecommunications)

An entrance to the building for both private and public network service cables (including wireless) including the entrance point at the building wall and continuing to the equipment room.

1.2.6 Equipment Room (ER) (Telecommunications)

An environmentally controlled centralized space for telecommunications equipment that serves the occupants of a building. Equipment housed therein is considered distinct from a telecommunications room because of the nature of its complexity.

1.2.7 Open Cable

Cabling that is not run in a raceway as defined by NFPA 70. This refers to cabling that is "open" to the space in which the cable has been installed and is therefore exposed to the environmental conditions associated with that space.

1.2.8 Open Office

A floor space division provided by furniture, moveable partitions, or other means instead of by building walls.

1.2.9 Pathway

A physical infrastructure utilized for the placement and routing of telecommunications cable.

1.3 SYSTEM DESCRIPTION

The building telecommunications cabling and pathway system shall include permanently installed backbone and horizontal cabling, horizontal and backbone pathways, service entrance facilities, work area pathways, telecommunications outlet assemblies, conduit, raceway, and hardware for splicing, terminating, and interconnecting cabling necessary to transport telephone and data (including LAN) between equipment items in a building. The horizontal system shall be wired in a star topology from the telecommunications work area to the floor distributor or campus distributor at the center or hub of the star. The backbone cabling and pathway system includes intrabuilding and interbuilding interconnecting cabling, pathway, and terminal hardware. The intrabuilding backbone provides connectivity from the floor distributors to the building distributors or to the campus distributor and from the building distributors to the campus distributor as required. The backbone system shall be wired in a star topology with the campus distributor at the center or hub of the star. The telecommunications contractor must coordinate with the NMCI/COSC/NGEN contractor concerning access to and configuration of telecommunications spaces. The telecommunications contractor may be required to coordinate work effort within the telecommunications spaces with the NMCI/COSC/NGEN contractor.

1.4 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Telecommunications Drawings; G

Telecommunications Space Drawings; G

In addition to Section 01 33 00 SUBMITTAL PROCEDURES, provide shop drawings in accordance with paragraph SHOP DRAWINGS.

SD-03 Product Data

Telecommunications Cabling (backbone and horizontal); G

Patch Panels; G

Telecommunications Outlet/Connector Assemblies; G

Equipment Support Frame; G

Submittals shall include the manufacturer's name, trade name, place of manufacture, and catalog model or number. Include performance and characteristic curves. Submittals shall also include applicable federal, military, industry, and technical society publication references. Should manufacturer's data require supplemental information for clarification, the supplemental information shall be submitted as specified in paragraph REGULATORY REQUIREMENTS and as required in Section 01 33 00 SUBMITTAL PROCEDURES.

SD-06 Test Reports

Telecommunications Cabling Testing; G

SD-07 Certificates

Telecommunications Contractor Qualifications; G

Key Personnel Qualifications; G

Manufacturer Qualifications; G

Test Plan; G

SD-09 Manufacturer's Field Reports

Factory Reel Tests; G

SD-10 Operation and Maintenance Data

Telecommunications Cabling and Pathway System Data Package 5; G

SD-11 Closeout Submittals

Record Documentation; G

1.5 QUALITY ASSURANCE

1.5.1 Shop Drawings

In exception to Section 01 33 00 SUBMITTAL PROCEDURES, submitted plan drawings shall be a minimum of 11 by 17 inches in size using a minimum scale of 1/8 inch per foot. Include wiring diagrams and installation details of equipment indicating proposed location, layout and arrangement, control panels, accessories, piping, ductwork, and other items that must

be shown to ensure a coordinated installation. Wiring diagrams shall identify circuit terminals and indicate the internal wiring for each item of equipment and the interconnection between each item of equipment. Drawings shall indicate adequate clearance for operation, maintenance, and replacement of operating equipment devices. Submittals shall include the nameplate data, size, and capacity. Submittals shall also include applicable federal, military, industry, and technical society publication references.

1.5.1.1 Telecommunications Drawings

Provide registered communications distribution designer (RCDD) approved, drawings in accordance with TIA-606. The identifier for each termination and cable shall appear on the drawings. Drawings shall depict final telecommunications installed wiring system infrastructure in accordance with TIA-606. The drawings should provide details required to prove that the distribution system shall properly support connectivity from the EF telecommunications and ER telecommunications, CD's, BD's, and FD's to the telecommunications work area outlets. Provide a plastic laminated schematic of the as-installed telecommunications cable system showing cabling, CD's, BD's, FD's, and the EF and ER for telecommunications keyed to floor plans by room number. Mount the laminated schematic in the EF telecommunications space as directed by the Contracting Officer. The following drawings shall be provided as a minimum:

a. Layout of complete building per floor - Building Area/Serving Zone Boundaries, Backbone Systems, and Horizontal Pathways. Layout of complete building per floor. The drawing indicates location of building areas, serving zones, vertical backbone diagrams, telecommunications rooms, access points, pathways, grounding system, and other systems that need to be viewed from the complete building perspective.

b. Serving Zones/Building Area Drawings - Drop Locations and Cable Identification (ID’S). Shows a building area or serving zone. These drawings show drop locations, telecommunications rooms, access points and detail call outs for common equipment rooms and other congested areas.

c. Typical Detail Drawings - Faceplate Labeling, Firestopping, Americans with Disabilities Act (ADA), Safety, Department of Transportation (DOT). Detailed drawings of symbols and typicals such as faceplate labeling, faceplate types, faceplate population installation procedures, detail racking, and raceways.

1.5.1.2 Telecommunications Space Drawings

Provide drawings in accordance with TIA-606 that include telecommunications rooms plan views, pathway layout (cable tray, racks, ladder-racks, etc.), mechanical/electrical layout, and cabinet, backboard and wall elevations. Drawings shall show layout of applicable equipment including incoming cable stub or connector blocks, building protector assembly, outgoing cable connector blocks, patch panels and equipment spaces and cabinet/racks. Drawings shall include a complete list of equipment and material, equipment rack details, proposed layout and anchorage of equipment and appurtenances, and equipment relationship to other parts of the work including clearance for maintenance and operation. Drawings may also be an enlargement of a congested area of drawings.

1.5.2 Telecommunications Qualifications

Work under this section shall be performed by and the equipment shall be provided by the approved telecommunications contractor and key personnel. Qualifications shall be provided for: the telecommunications system contractor, the telecommunications system installer, and the supervisor (if different from the installer). A minimum of 30 days prior to installation, submit documentation of the experience of the telecommunications contractor and of the key personnel.

1.5.2.1 Telecommunications Contractor

The telecommunications contractor shall be a firm which is regularly and professionally engaged in the business of the applications, installation, and testing of the specified telecommunications systems and equipment. The telecommunications contractor shall demonstrate experience in providing successful telecommunications systems within the past 3 years of similar scope and size. Submit documentation for a minimum of three and a maximum of five successful telecommunication system installations for the telecommunications contractor.

1.5.2.2 Key Personnel

Provide key personnel who are regularly and professionally engaged in the business of the application, installation and testing of the specified telecommunications systems and equipment. There may be one key person or more key persons proposed for this solicitation depending upon how many of the key roles each has successfully provided. Each of the key personnel shall demonstrate experience in providing successful telecommunications systems within the past 3 years.

Supervisors and installers assigned to the installation of this system or any of its components shall be Building Industry Consulting Services International (BICSI) Registered Cabling Installers, Technician Level. Submit documentation of current BICSI certification for each of the key personnel.

In lieu of BICSI certification, supervisors and installers assigned to the installation of this system or any of its components shall have a minimum of 3 years experience in the installation of the specified copper and fiber optic cable and components. They shall have factory or factory approved certification from each equipment manufacturer indicating that they are qualified to install and test the provided products. Submit documentation for a minimum of three and a maximum of five successful telecommunication system installations for each of the key personnel. Documentation for each key person shall include at least two successful system installations provided that are equivalent in system size and in construction complexity to the telecommunications system proposed for this solicitation. Include specific experience in installing and testing telecommunications systems and provide the names and locations of at least two project installations successfully completed using optical fiber and copper telecommunications cabling systems. All of the existing telecommunications system installations offered by the key persons as successful experience shall have been in successful full-time service for at least 18 months prior to the issuance date for this solicitation. Provide the name and role of the key person, the title, location, and completed installation date of the referenced project, the referenced project owner point of contact information including name, organization,

title, and telephone number, and generally, the referenced project description including system size and construction complexity.

Indicate that all key persons are currently employed by the telecommunications contractor, or have a commitment to the telecommunications contractor to work on this project. All key persons shall be employed by the telecommunications contractor at the date of issuance of this solicitation, or if not, have a commitment to the telecommunications contractor to work on this project by the date that the bid was due to the Contracting Officer.

Note that only the key personnel approved by the Contracting Officer in the successful proposal shall do work on this solicitation's telecommunications system. Key personnel shall function in the same roles in this contract, as they functioned in the offered successful experience. Any substitutions for the telecommunications contractor's key personnel requires approval from The Contracting Officer.

1.5.2.3 Minimum Manufacturer Qualifications

Cabling, equipment and hardware manufacturers shall have a minimum of 3 years experience in the manufacturing, assembly, and factory testing of components which comply with TIA-568.1, TIA-568.2 and TIA-568.3.

1.5.3 Test Plan

Provide a complete and detailed test plan for the telecommunications cabling system including a complete list of test equipment for the components and accessories for each cable type specified, 60 days prior to the proposed test date. Include procedures for certification, validation, and testing.

1.5.4 Regulatory Requirements

In each of the publications referred to herein, consider the advisory provisions to be mandatory, as though the word, "shall" had been substituted for "should" wherever it appears. Interpret references in these publications to the "authority having jurisdiction," or words of similar meaning, to mean the Contracting Officer. Equipment, materials, installation, and workmanship shall be in accordance with the mandatory and advisory provisions of NFPA 70 unless more stringent requirements are specified or indicated.

1.5.5 Standard Products

Provide materials and equipment that are products of manufacturers regularly engaged in the production of such products which are of equal material, design and workmanship. Products shall have been in satisfactory commercial or industrial use for 2 years prior to bid opening. The 2-year period shall include applications of equipment and materials under similar circumstances and of similar size. The product shall have been on sale on the commercial market through advertisements, manufacturers' catalogs, or brochures during the 2-year period. Where two or more items of the same class of equipment are required, these items shall be products of a single manufacturer; however, the component parts of the item need not be the products of the same manufacturer unless stated in this section.

1.5.5.1 Alternative Qualifications

Products having less than a 2-year field service record will be acceptable if a certified record of satisfactory field operation for not less than 6000 hours, exclusive of the manufacturers' factory or laboratory tests, is furnished.

1.5.5.2 Material and Equipment Manufacturing Date

Products manufactured more than 1 year prior to date of delivery to site shall not be used, unless specified otherwise.

1.6 DELIVERY AND STORAGE

Provide protection from weather, moisture, extreme heat and cold, dirt, dust, and other contaminants for telecommunications cabling and equipment placed in storage.

1.7 ENVIRONMENTAL REQUIREMENTS

Connecting hardware shall be rated for operation under ambient conditions of 32 to 140 degrees F and in the range of 0 to 95 percent relative humidity, noncondensing.

1.8 WARRANTY

The equipment items shall be supported by service organizations which are reasonably convenient to the equipment installation in order to render satisfactory service to the equipment on a regular and emergency basis during the warranty period of the contract.

1.9 MAINTENANCE

1.9.1 Operation and Maintenance Manuals

Commercial off the shelf manuals shall be furnished for operation, installation, configuration, and maintenance of products provided as a part of the telecommunications cabling and pathway system, Data Package 5. Submit operations and maintenance data in accordance with Section 01 78 23 OPERATION AND MAINTENANCE DATA and as specified herein not later than 2 months prior to the date of beneficial occupancy. In addition to requirements of Data Package 5, include the requirements of paragraphs TELECOMMUNICATIONS DRAWINGS, TELECOMMUNICATIONS SPACE DRAWINGS, and RECORD DOCUMENTATION. Ensure that these drawings and documents depict the as-built configuration.

1.9.2 Record Documentation

Provide Drawings including documentation on cables and termination hardware in accordance with TIA-606. Drawings shall include schedules to show information for cut-overs and cable plant management, patch panel layouts and cover plate assignments, cross-connect information and connecting terminal layout as a minimum. Drawings shall be provided in hard copy format and on electronic media using Windows based computer cable management software. A licensed copy of the cable management software including documentation, shall be provided. Provide the following drawing documentation as a minimum:

a. Cables - A record of installed cable shall be provided in accordance

with TIA-606. The cable records shall include only the required data fieldsin accordance with TIA-606. Include manufacture date of cable with submittal.

b. Termination Hardware - A record of installed patch panels, cross-connect points, distribution frames, terminating block arrangements and type, and outlets shall be provided in accordance with TIA-606. Documentation shall include the required data fields as a minimum in accordance with TIA-606.

PART 2 PRODUCTS

2.1 COMPONENTS

Components shall be UL or third party certified. Where equipment or materials are specified to conform to industry and technical society reference standards of the organizations, submit proof of such compliance. The label or listing by the specified organization will be acceptable evidence of compliance. In lieu of the label or listing, submit a certificate from an independent testing organization, competent to perform testing, and approved by the Contracting Officer. The certificate shall state that the item has been tested in accordance with the specified organization's test methods and that the item complies with the specified organization's reference standard. Provide a complete system of telecommunications cabling and pathway components using star topology. Provide support structures and pathways, complete with outlets, cables, connecting hardware and telecommunications cabinets/racks. Cabling and interconnecting hardware and components for telecommunications systems shall be UL listed or third party independent testing laboratory certified, and shall comply with NFPA 70 and conform to the requirements specified herein.

2.2 TELECOMMUNICATIONS PATHWAY

Provide telecommunications pathways in accordance with TIA-569 and as specified in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Provide system furniture pathways in accordance with UL 1286.

2.3 TELECOMMUNICATIONS CABLING

Cabling shall be UL listed for the application and shall comply with TIA-568.0, TIA-568.1, TIA-568.2, TIA-568.3 and NFPA 70. Provide a labeling system for cabling as required by TIA-606 and UL 969. Ship cable on reels or in boxes bearing manufacture date for for unshielded twisted pair (UTP) in accordance with ICEA S-90-661 and optical fiber cables in accordance with ICEA S-83-596 for all cable used on this project. Cabling manufactured more than 12 months prior to date of installation shall not be used.

2.3.1 Backbone Cabling

2.3.1.1 Backbone Optical Fiber

Provide in accordance with ICEA S-83-596, TIA-568.3, UL 1666 and NFPA 70. Cable shall be imprinted with fiber count, fiber type and aggregate length at regular intervals not to exceed 40 inches.

Provide the number of strands indicated, (but not less than 12 strands between the main telecommunication room and each of the other

telecommunication rooms), of single-mode(OS1), tight buffered fiber optic cable.

Provide tight buffered fiber optic multimode, 50/125-um diameter laser optimized(OM3) cable as indicated.

Provide plenum (OFNP) rated non-conductive, fiber optic cable in accordance with NFPA 70. Substitution of a higher rated cable shall be permitted in accordance with NFPA 70. The cable cordage jacket, fiber, unit, and group color shall be in accordance with TIA/EIA-598.

2.3.2 Horizontal Cabling

Provide horizontal cable in compliance with NFPA 70 and performance characteristics in accordance with TIA-568.1.

2.3.2.1 Horizontal Copper

Provide horizontal copper cable, UTP, 100 ohm in accordance with TIA-568.2, UL 444, ANSI/NEMA WC 66, ICEA S-90-661 . Provide four each individually twisted pair, minimum size 24 AWG conductors, Category 6A, with a blue thermoplastic jacket. Cable shall be imprinted with manufacturers name or identifier, flammability rating, gauge of conductor, transmission performance rating (category designation) and length marking at regular intervals in accordance with ICEA S-90-661. Provide plenum (CMP) communications rated cabling in accordance with NFPA 70. Substitution of a higher rated cable shall be permitted in accordance with NFPA 70. Cables installed in conduit within and under slabs shall be UL listed and labeled for wet locations in accordance with NFPA 70.

2.3.2.2 Horizontal Optical Fiber

Provide optical fiber horizontal cable in accordance with ICEA S-83-596and TIA-568.3. Cable shall be tight buffered, multimode, 50/125-um diameter laser optimized, OM, OM1, or single-mode, 8/125-um diameter, OS1. Cable shall be imprinted with manufacturer, flammability rating and fiber count at regular intervals not to exceed 40 inches.

Provide plenum (OFNP) rated non-conductive, fiber optic cable in accordance with NFPA 70. Substitution of a higher rated cable shall be permitted in accordance with NFPA 70.Cables installed in conduit within and under slabs be UL listed and labeled for wet locations in accordance with NFPA 70. The cable jacket shall be of single jacket construction with color coding of cordage jacket, fiber, unit, and group in accordance with TIA/EIA-598.

2.3.3 Work Area Cabling

2.3.3.1 Work Area Copper

Provide work area copper cable in accordance with TIA-568.2, with a blue, thermoplastic jacket.

2.4 TELECOMMUNICATIONS SPACES

Provide connecting hardware and termination equipment in the telecommunications entrance facility and telecommunication room to facilitate installation as shown on design drawings for terminating and cross-connecting permanent cabling. Provide telecommunications

interconnecting hardware color coding in accordance with TIA-606.

2.4.1 Backboards

Provide void-free, interior grade A-C plywood 3/4 inch thick 4 by 8 feet. Backboards shall be fire rated by manufacturing process. Fire stamp shall be clearly visible. Paint applied over fire retardant backboard shall be UL 723 fire retardant paint. Provide label including paint manufacturer, date painted, UL listing and name of Installer. When painted, paint label and fire stamp shall be clearly visible. Backboards shall be provided on a minimum of two adjacent walls in the telecommunication spaces.

2.4.2 Equipment Support Frame

Provide in accordance with ECIA EIA/ECA 310-E and UL 50.

2.4.3 Cable Guides

Provide cable guides specifically manufactured for the purpose of routing cables, wires and patch cords horizontally and vertically on 19 inches equipment cabinets and telecommunications backboards. Cable guides of ring or bracket type devices mounted on cabinet backboard for horizontal cable management and individually mounted for vertical cable management. Mount cable guides with screws, and or nuts and lockwashers.

2.4.4 Patch Panels

Provide ports for the number of horizontal and backbone cables terminated on the panel plus 25 percent spare. Provide patch cords for patch panels. Provide patch cords, as complete assemblies, with matching connectors as specified. Patch cords shall meet minimum performance requirements specified in TIA-568.1, TIA-568.2 for cables, cable length and hardware specified.

2.4.4.1 Modular to 110 Block Patch Panel

Provide in accordance with TIA-568.1 and TIA-568.2. Panels shall be third party verified and shall comply with EIA/TIA Category 6A requirements. Panel shall be constructed of 0.09 inches minimum aluminum and shall be rack mounted and compatible with an ECIA EIA/ECA 310-E 19 inches equipment rack. Panel shall provide 48 non-keyed, 8-pin modular ports, wired to T568B. Patch panels shall terminate the building cabling on Type 110 IDCs and shall utilize a printed circuit board interface. The rear of each panel shall have incoming cable strain-relief and routing guides. Panels shall have each port factory numbered and be equipped with laminated plastic nameplates above each port.

2.4.4.2 Fiber Optic Patch Panel

Provide panel for maintenance and cross-connecting of optical fiber cables. Panel shall be constructed of 16 gauge steel or 11 gauge aluminum minimum and shall be rack mounted and compatible with a ECIA EIA/ECA 310-E 19 inches equipment rack. Each panel shall provide 36/72 multimode single-mode adapters as duplex LC in accordance with TIA/EIA-604-10 with zirconia ceramic alignment sleeves. Provide dust cover for unused adapters. The rear of each panel shall have a cable management tray a minimum of 8 inches deep with removable cover, incoming cable strain-relief and routing guides. Panels shall have each adapter factory numbered and be equipped with laminated plastic nameplates above each

adapter.

2.4.5 Optical Fiber Distribution Panel

Rack mounted optical fiber distribution panel (OFDP) shall be constructed in accordance with ECIA EIA/ECA 310-E utilizing 16 gauge steel or 11 gauge aluminum minimum. Panel shall be divided into two sections, distribution and user. Distribution section shall have strain relief, routing guides, splice tray and shall be lockable, user section shall have a cover for patch cord protection. Each panel shall provide 36/72 multimode and 36/72 single-mode pigtails and adapters. Provide adapters as duplex LC with zirconia ceramic alignment sleeves. Provide dust covers for adapters. Provide patch cords as specified in the paragraph PATCH PANELS.

2.5 TELECOMMUNICATIONS OUTLET/CONNECTOR ASSEMBLIES

2.5.1 Outlet/Connector Copper

Outlet/connectors shall comply with FCC Part 68, TIA-568.1, and TIA-568.2. UTP outlet/connectors shall be UL 1863 listed, non-keyed, 8-pin modular, constructed of high impact rated thermoplastic housing and shall be third party verified and shall comply with TIA-568.2 Category 6A requirements. Outlet/connectors provided for UTP cabling shall meet or exceed the requirements for the cable provided. Outlet/connectors shall be terminated using a Type 110 IDC PC board connector, color-coded for both T568A and T568B wiring. Each outlet/connector shall be wired T568B. UTP outlet/connectors shall comply with TIA-568.2 for 200 mating cycles.

2.5.2 Optical Fiber Adapters(Couplers)

Provide optical fiber adapters suitable for duplex LC in accordance with TIA/EIA-604-10 with zirconia ceramic alignment sleeves, as indicated. Provide dust cover for adapters. Optical fiber adapters shall comply with TIA-455-21 for 500 mating cycles.

2.5.3 Optical Fiber Connectors

Provide in accordance with TIA-455-21. Optical fiber connectors shall be duplex LC in accordance with TIA/EIA-604-10 with zirconia ceramic alignment sleeves, ferrule, epoxyless crimp style compatible with 50/125 multimode and 8/125 single-mode fiber. The connectors shall provide a maximum attenuation of 0.3 dB at 850, 1300, 1310, 1550 nm with less than a 0.2 dB change after 500 mating cycles.

2.5.4 Cover Plates

Telecommunications cover plates shall comply with UL 514C, and TIA-568.1, TIA-568.2, TIA-568.3; flush design constructed of high impact thermoplastic material to match color of receptacle/switch cover plates specified in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Provide labeling in accordance with the paragraph LABELING in this section.

2.6 GROUNDING AND BONDING PRODUCTS

Provide in accordance with UL 467, TIA-607, and NFPA 70. Components shall be identified as required by TIA-606. Provide ground rods, bonding conductors, and grounding busbars as specified in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM.

2.7 FIRESTOPPING MATERIAL

Provide as specified in Section 07 84 00 FIRESTOPPING.

2.8 TESTS, INSPECTIONS, AND VERIFICATIONS

2.8.1 Factory Reel Tests

Provide documentation of the testing and verification actions taken by manufacturer to confirm compliance with TIA-568.1, TIA-568.2, TIA-568.3, TIA-526-7 for single mode optical fiber, and TIA-526-14 for multimode optical fiber cables.

PART 3 EXECUTION

3.1 INSTALLATION

Install telecommunications cabling and pathway systems, including the horizontal and backbone cable, pathway systems, telecommunications outlet/connector assemblies, and associated hardware in accordance with NECA/BICSI 568, TIA-568.1, TIA-568.2, TIA-568.3, TIA-569, NFPA 70, and UL standards as applicable. Provide cabling in a star topology network. Pathways and outlet boxes shall be installed as specified in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Install telecommunications cabling with copper media in accordance with the following criteria to avoid potential electromagnetic interference between power and telecommunications equipment. The interference ceiling shall not exceed 3.0 volts per meter measured over the usable bandwidth of the telecommunications cabling. Cabling shall be run with horizontal and vertical cable guides in telecommunications spaces with terminating hardware and interconnection equipment.

3.1.1 Cabling

Install UTP, and optical fiber telecommunications cabling system as detailed in TIA-568.1, TIA-568.2, and TIA-568.3. Screw terminals shall not be used except where specifically indicated on plans. Use an approved insulation displacement connection (IDC) tool kit for copper cable terminations. Do not exceed manufacturers' cable pull tensions for copper and optical fiber cables. Provide a device to monitor cable pull tensions. Do not exceed 25 pounds pull tension for four pair copper cables. Do not chafe or damage outer jacket materials. Use only lubricants approved by cable manufacturer. Do not over cinch cables, or crush cables with staples. For UTP cable, bend radii shall not be less than four times the cable diameter. Cables shall be terminated; no cable shall contain unterminated elements. Cables shall not be spliced. Label cabling in accordance with paragraph LABELING in this section.

3.1.1.1 Open Cable

Use only where specifically indicated on plans for use in cable trays, or below raised floors. Install in accordance with TIA-568.1, TIA-568.2 and TIA-568.3. Do not exceed cable pull tensions recommended by the manufacturer. Copper cable not in a wireway or pathway shall be suspended a minimum of 8 inches above ceilings by cable supports no greater than 60 inches apart. Cable shall not be run through structural members or in contact with pipes, ducts, or other potentially damaging items. Placement of cable parallel to power conductors shall be avoided, if possible; a minimum separation of 12 inches shall be maintained when such placement

cannot be avoided.

Plenum cable shall be used where open cables are routed through plenum areas. Cable routed exposed under raised floors shall be plenum rated. Plenum cables shall comply with flammability plenum requirements of NFPA 70. Install cabling after the flooring system has been installed in raised floor areas. Cable 6 feet long shall be neatly coiled not less than 12 inches in diameter below each feed point in raised floor areas.

3.1.1.2 Horizontal Cabling

Install horizontal cabling as indicated on drawings Do not untwist Category 6A UTP cables more than one half inch from the point of termination to maintain cable geometry. Provide slack cable in the form of a figure eight (not a service loop) on each end of the cable, 10 feet in the telecommunications room, and 12 inches in the work area outlet.

3.1.2 Pathway Installations

Provide in accordance with TIA-569 and NFPA 70.

3.1.3 Service Entrance Conduit, Underground

Provide service entrance underground as specified in Section 27 05 28.36 40 CABLE TRAYS FOR COMMUNICATION SYSTEMS.

3.1.4 Cable Tray Installation

Install cable tray as specified in Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM. Only CMP and OFNP type cable shall be installed in a plenum.

3.1.5 Work Area Outlets

3.1.5.1 Terminations

Terminate UTP cable in accordance with TIA-568.1, TIA-568.2 and wiring configuration as specified. Terminate fiber optic cables in accordance with TIA-568.3.

3.1.5.2 Cover Plates

As a minimum, each outlet/connector shall be labeled as to its function and a unique number to identify cable link in accordance with the paragraph LABELING in this section.

3.1.5.3 Cables

Unshielded twisted pair and fiber optic cables shall have a minimum of 12 inches of slack cable loosely coiled into the telecommunications outlet boxes. Minimum manufacturer's bend radius for each type of cable shall not be exceeded.

3.1.5.4 Pull Cords

Pull cords shall be installed in conduit serving telecommunications outlets that do not have cable installed.

3.1.6 Telecommunications Space Termination

Install termination hardware required for Category 6 or 6A and optical fiber system. An insulation displacement tool shall be used for terminating copper cable to insulation displacement connectors.

3.1.6.1 Patch Panels

Patch panels shall be mounted in equipment racks with sufficient ports to accommodate the installed cable plant plus 25 percent spares.

a. Copper Patch Panel. Copper cable entering a patch panel shall be secured to the panel as recommended by the manufacturer to prevent movement of the cable.

b. Fiber Optic Patch Panel. Fiber optic cable loop shall be 3 feet in length. The outer jacket of each cable entering a patch panel shall be secured to the panel to prevent movement of the fibers within the panel, using clamps or brackets specifically manufactured for that purpose.

3.1.6.2 Equipment Support Frames

Install in accordance with TIA-569:

a. Cabinets, freestanding modular type. When cabinets are connected together, remove adjoining side panels for cable routing between cabinets.

3.1.7 Electrical Penetrations

Seal openings around electrical penetrations through fire resistance-rated wall, partitions, floors, or ceilings as specified in Section 07 84 00 FIRESTOPPING.

3.1.8 Grounding and Bonding

Provide in accordance with TIA-607 and NFPA 70.

3.2 LABELING

3.2.1 Labels

Provide labeling in accordance with TIA-606. Handwritten labeling is unacceptable. Stenciled lettering for voice and data circuits shall be provided using thermal ink transfer process.

3.2.2 Cable

Cables shall be labeled using color labels on both ends with identifiers in accordance with TIA-606.

3.2.3 Termination Hardware

Workstation outlets and patch panel connections shall be labeled using color coded labels with identifiers in accordance with TIA-606.

3.3 FIELD APPLIED PAINTING

Paint electrical equipment as required to match finish of adjacent surfaces or to meet the indicated or specified safety criteria. Painting shall be as specified in Section 09 90 00 PAINTS AND COATINGS.

3.3.1 Painting Backboards

If backboards are required to be painted, then the manufactured fire retardant backboard must be painted with fire retardant paint, so as not to increase flame spread and smoke density and must be appropriately labeled. Label and fire rating stamp must be unpainted.

3.4 FIELD FABRICATED NAMEPLATE MOUNTING

Provide number, location, and letter designation of nameplates as indicated. Fasten nameplates to the device with a minimum of two sheet-metal screws or two rivets.

3.5 TESTING

3.5.1 Telecommunications Cabling Testing

Perform telecommunications cabling inspection, verification, and performance tests in accordance with TIA-568.1, TIA-568.2, and TIA-568.3. Test equipment shall conform to TIA-1152. Perform optical fiber field inspection tests via attenuation measurements on factory reels and provide results along with manufacturer certification for factory reel tests. Remove failed cable reels from project site upon attenuation test failure.

3.5.1.1 Inspection

Visually inspect UTP and optical fiber jacket materials for UL or third party certification markings. Inspect cabling terminations in telecommunications rooms and at workstations to confirm color code for T568A or T568B pin assignments, and inspect cabling connections to confirm compliance with TIA-568.1, TIA-568.2, and TIA-568.3. Visually confirm Category 6 or 6A, marking of outlets, cover plates, outlet/connectors, and patch panels.

3.5.1.2 Verification Tests

UTP backbone copper cabling shall be tested for DC loop resistance, shorts, opens, intermittent faults, and polarity between conductors, and between conductors and shield, if cable has overall shield. Test operation of shorting bars in connection blocks. Test cables after termination but prior to being cross-connected.

For multimode optical fiber, perform optical fiber end-to-end attenuation tests in accordance with TIA-568.3 and TIA-526-14 using Method A, Optical Power Meter and Light Source for multimode optical fiber. For single-mode optical fiber, perform optical fiber end-to-end attenuation tests in accordance with TIA-568.3 and TIA-526-7 using Method A, Optical Power Meter and Light Source for single-mode optical fiber. Perform verification acceptance tests.

3.5.1.3 Performance Tests

Perform testing for each outlet and MUTOA as follows:

a. Optical fiber Links. Perform optical fiber end-to-end link tests in accordance with TIA-568.3.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 27 - COMMUNICATIONS

SECTION 27 13 23.00 40

COMMUNICATIONS OPTICAL BACKBONE CABLING

PART 1 GENERAL

1.1 REFERENCES
1.2 DEFINITIONS
1.3 ADMINISTRATIVE REQUIREMENTS
1.3.1 Pre-Installation Meetings
1.4 SUBMITTALS
1.5 QUALITY CONTROL
1.5.1 Fiber Optic Cable Installer and Splicer Qualifications
1.5.2 Quality Assurance Plan
1.5.3 Manufacturer's Qualifications
1.5.4 Fiber Optic Factory Test Plan
1.5.5 Fiber Optic Field Tests Plan
1.6 DELIVERY, STORAGE, AND HANDLING
1.7 PROJECT/SITE CONDITIONS

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION
2.1.1 Fiber Optic Cable Design
2.1.1.1 Fiber Optic Media Types
2.1.1.2 Cable Length
2.1.1.3 Construction
2.1.2 Cable Identification Symbol
2.1.3 Temperature Environment
2.1.4 Splice Compatibility Test
2.2 EQUIPMENT
2.2.1 Replacement Cable
2.2.2 Splice Organizers
2.2.3 Pre-Connected Cable Assembly
2.2.4 Optical Patch Panel Assemblies
2.2.5 Fiber Optic Terminations And Connectors
2.2.6 Fiber Optic Pathway System
2.2.7 FO Media Tags
2.3 MATERIALS
2.3.1 Central Core Member
2.3.2 Optical Fibers
2.3.3 Fiber Primary Protective Coating
2.3.4 Optical Fiber Color-Code Coating
2.3.5 Loose Tube Buffering
2.3.6 Colorants
2.3.7 Filling Compound
2.4 TESTS, INSPECTIONS, AND VERIFICATIONS
2.4.1 Factory FO Quality Control
2.4.2 Factory Test Certificates
2.4.2.1 Optical Performance

2.4.2.2 Mechanical Performance
2.4.3 Factory Reel Test

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Fiber Splices
3.1.2 Contractor Damage
3.1.3 Underground Cable
3.1.3.1 Securing Cable
3.1.3.2 Bending
3.1.3.3 Pulling
3.1.3.4 Lubricant
3.1.3.5 Damage and Defects
3.1.3.6 Seal
3.1.4 Cable Installation in Cable Trays
3.1.5 Grounding Systems
3.1.6 Reconditioning of Surfaces
3.1.6.1 Unpaved Surface Treatment
3.1.6.2 Paving Repairs
3.1.7 Cable Pulling
3.1.7.1 FO Media Tensions
3.1.7.2 Pulling Eyes
3.1.7.3 Media in Maintenance Manholes, Handholes, and Vaults
3.2 FIELD QUALITY CONTROL
3.2.1 Test Requirements
3.2.1.1 Single and Multi-Mode OTDR Test
3.2.1.2 End-to-End Attenuation Tests
3.2.1.3 End-to-End Bandwidth Tests
3.2.2 Field Reel Tests
3.2.2.1 Reel Test Reports
3.2.3 Final Acceptance Tests
3.2.3.1 Test Results
3.3 CLOSEOUT ACTIVITIES

-- End of Section Table of Contents --

SECTION 27 13 23.00 40

COMMUNICATIONS OPTICAL BACKBONE CABLING

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ASTM INTERNATIONAL (ASTM)

ASTM C338	(1993; R 2013) Standard Test Method Softening Point of Glass
ASTM D4976	(2012a) Standard Specification for Polyethylene Plastics Molding and Extrusion Materials

ELECTRONIC INDUSTRIES ALLIANCE (EIA)

ANSI/TIA-455-80C	(2003) FOTP-80 - IEC 60793-1-144 Optical fibres Part 1-44: Measurement Methods and Test Procedures - Cut-off Wavelength
TIA/EIA 455-41-A	(1993a; R 2001) FOTP-41 - Compressive Loading Resistance of Fiber Optic Cables

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE C2	(2023) National Electrical Safety Code

INSULATED CABLE ENGINEERS ASSOCIATION (ICEA)

ICEA S-87-640	(2016) Optical Fiber Outside Plant Communications Cable; 4th Edition

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA RN 1	(2005; R 2013) Polyvinyl-Chloride (PVC) Externally Coated Galvanized Rigid Steel Conduit and Intermediate Metal Conduit
NEMA TC 2	(2020) Standard for Electrical Polyvinyl Chloride (PVC) Conduit
NEMA TC 3	(2021) Polyvinyl Chloride (PVC) Fittings for Use With Rigid PVC Conduit and Tubing
NEMA TC 6 & 8	(2020) Standard for Polyvinyl Chloride (PVC) Plastic Utilities Duct for Underground Installations
NEMA TC 9	(2020) Standard for Fittings for Polyvinyl

	Chloride (PVC) Plastic Utilities Duct for Underground Installation

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2023) National Electrical Code

TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)

EIA/TIA 455-165A	(1993) Standard for Mode-Field Diameter Measurement by Near-Field Scanning Technique
TIA-455-33	(2005b; R 2013) Optical Cable Tensile Loading and Bending Test
TIA-455-78-B	(2020c) FOTP-78 Optical Fibres - Part 1-40: Measurement Methods and Test Procedures - Attenuation
TIA-455-82	(2020c) FOTP-82 Fluid Penetration Test for Fluid-Blocked Fiber Optic Cable
TIA-455-104	(2016b) Standard for FOTP-104 Fiber Optic Cable Cyclic Flexing Test
TIA-455-175	(2020c) FOTP-175 IEC-60793-1-42: Measurement Methods and Test Procedures – Chromatic Dispersion
TIA-455-177	(2020c) FOTP-177 IEC-60793-1-43: Measurement Methods and Test Procedures - Numerical Aperture
TIA-472D000	(2007b) Fiber Optic Communications Cable for Outside Plant Use
TIA-526-7	(2015a; R 2022) Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant, Adoption of IEC 61280-4-2 edition 2: Fibre-Optic Communications Subsystem Test Procedures - Part 4-2: Installed Cable Plant - Single-Mode Attenuation and Optical Return Loss Measurement
TIA-526-14	(2015c) OFSTP-14A Optical Power Loss Measurements of Installed Multimode Fiber Cable Plant
TIA-568.1	(2020e) Commercial Building Telecommunications Infrastructure Standard
TIA-568.3	(2016d; Add 1 2019) Optical Fiber Cabling Components Standard
TIA-569	(2019e; Add 1 2022) Telecommunications Pathways and Spaces

TIA-590	(1997a) Standard for Physical Location and Protection of Below Ground Fiber Optic Cable Plant
TIA-758	(2012b) Customer-Owned Outside Plant Telecommunications Infrastructure Standard
TIA/EIA-455	(1998b) Standard Test Procedure for Fiber Optic Fibers, Cables, Transducers, Sensors, Connecting and Terminating Devices, and Other Fiber Optic Components
TIA/EIA-455-25	(2016d) FOTP-25 Impact Testing of Optical Fiber Cables
TIA/EIA-455-81	(2000b) FOTP-81 Compound Flow (Drip) Test for Filled Fiber Optic Cable
TIA/EIA-472DAAA	(1993) Detail Specification for All Dielectric Fiber Optic Communications Cable for Outside Plant Use Containing Class 1a 62.5 Um Core Diameter/125 um Cladding Diameter/250 um Coating Diameter Fiber(s).
TIA/EIA-598	(2014D; Add 2 2018) Optical Fiber Cable Color Coding
TIA/EIA-604-3	(2004b; R 2014) Fiber Optic Connector Intermateability Standard (FOCIS), Type SC and SC-APC, FOCIS-3
TIA/EIA-4750000-C	(1996) Generic Specifications for Fiber Optic Connectors (ANSI)

U.S. DEPARTMENT OF AGRICULTURE (USDA)

RUS Bull 1753F-601	(1994) Specifications for Filled Fiber Optic Cables (PE-90)

U.S. DEPARTMENT OF DEFENSE (DOD)

MIL-STD-188-176	(1996; Notice 1) Standardized Profile for Asynchronous Transfer Mode (ATM)

1.2 DEFINITIONS

References in this section to cable refer to fiber optic ("FO") cable. Fiber optic cable consists of optical fibers, strength members, and jacketing. Associated components include optical fiber connectors, optical patch panels, terminal bay cabinets, and splice closures as indicated.

1.3 ADMINISTRATIVE REQUIREMENTS

1.3.1 Pre-Installation Meetings

Within 30 calendar days after date of receipt by him of notice of award, submit for the approval of the Contracting Officer six (6) copies of

outline drawings of all equipment to be furnished under this contract, together with pre-construction and installation drawings and documents. Ensure drawings show the general arrangement and overall dimensions of the cable installation, control centers, space requirements, details of any hidden floor supports or ceiling systems and provisions for conduits for external cables. Submit the following for review and approval:

a. Fiber Optic System Contract Drawings

b. Detailed Shop Drawings

c. Qualifications

d. Quality Assurance Plan

Submit a quality assurance plan for fiber optic cable systems consisting of detailed procedures defining methods to ensure compliance to contract drawings and specifications by drawing control, inspection and procurement records, and test plan showing when and how each system will be tested, material testing, and certification records. Submit test plan to the Technical Representative for approval at least 30 calendar days prior to the start of testing.

Submit manufacturer's product data for the following items. Ensure data includes a complete list of parts, special tools, and supplies with current unit prices and source of supply:.

a. Optical Fibers

b. Fiber Optic Cable Design

c. Splice Organizers

d. Pre-Connected Cable Assembly

e. Fiber Optic Terminal Cabinets

f. Optical Patch Panel Assemblies

g. Fiber Optic Media Types

h. Fiber Optic Terminations and Connectors

i. Fiber Optic Enclosures

j. Fiber Optic Cable Installer and Splicer Qualifications

k. Manufacturer's Qualifications

l. Fiber Optic System Instructions

1.4 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Qualifications

Quality Assurance Plan

SD-02 Shop Drawings

Fiber Optic System Contract Drawings

Detailed Shop Drawings

Record (As-Built) Drawings

SD-03 Product Data

Optical Fibers

Fiber Optic Cable Design

Splice Organizers

Pre-Connected Cable Assembly

Fiber Optic Terminal Cabinets

Optical Patch Panel Assemblies

Fiber Optic Media Types

Fiber Optic Terminations and Connectors

Fiber Optic Enclosures

SD-06 Test Reports

Factory Test Certificates

Single and Multi-Mode OTDR Test

End-to-End Attenuation Tests

End-to-End Bandwidth Tests

Fiber Optic Factory Test Plan

Fiber Optic Field Tests Plan

SD-07 Certificates

Fiber Optic Cable Installer and Splicer Qualifications

Manufacturer's Qualifications

SD-08 Manufacturer's Instructions

Fiber Optic System Instructions

1.5 QUALITY CONTROL

1.5.1 Fiber Optic Cable Installer and Splicer Qualifications

Provide technicians installing FO media, splices and performing system tests who are certified and trained in accordance with an approved manufacturers training program, with a minimum of 3 years FO experience in installing equivalent FO systems. Submit data for approval to the Contracting Officer. Submit FO technician qualifications for approval 30 days before splices are to be made on the cable. Certification includes the training, and experience of the individual on specific type and classification of FO media to be provided under this contract.

Contracting officer may require each person who is to perform fiber optic cable splicing to perform a minimum of one acceptable sample splice and termination. Do not incorporate sample splices and terminations in the job.

1.5.2 Quality Assurance Plan

Prepare a quality assurance plan which provides a detailed outline of all testing to be accomplished, addresses whether cladding modes have been stripped prior to testing, source wavelength (peak), spectral width full width/half maximum (FWHM), mode structure, fiber end preparation, and bandwidth measurements of fiber links both greater and less than 1 kilometer. Quality assurance plan includes, as a minimum, a schedule of when tests will be performed relative to installation milestones, specific test procedure that will be used, a list of test equipment that will be used including manufacturer, model number, range, resolution accuracy and conformance to the specified requirements.

1.5.3 Manufacturer's Qualifications

Ensure FO media manufacturer has a minimum of 3 years experience in the manufacturing, assembly, and factory testing of FO media which comply with RUS Bull 1753F-601. Ensure manufacturer provides a list of customers with 3 years of maintenance logs documenting experience with government customers.

1.5.4 Fiber Optic Factory Test Plan

Prepare and provide to the Government for review a test plan for factory and field tests of the FO media. Provide factory Optical Time Domain Reflectometer(OTDR) test data as part of the test report. Provide a list of factory test equipment. Include a FO link performance test plan. Submit the plan at least 30 days prior to tests for government approval. Refer to TIA-569 for performance measurement criteria. Conduct tests at all operating bandwidths. Provide calculations for optical power budget and bandwidth as required by RUS Bull 1753F-601 using test method TIA-455-78-B or TIA/EIA-455. Submit test plans and reports to the Government for review and approval.

1.5.5 Fiber Optic Field Tests Plan

Prepare and provide technicians and test equipment for field tests of FO media. Conduct OTDR reel tests at the job site prior to installation. Perform OTDR and end to end tests of all installed media. Conduct tests on single mode fiber in accordance with TIA-526-7 for single mode fiber and EIA TIA/EIA-526-14A for multi mode fiber.

1.6 DELIVERY, STORAGE, AND HANDLING

Ship media to job site on factory reels in custom lengths or in factory cartons. Provide a reel drum radius no smaller than the minimum bend radius recommended by the manufacturer for the media. Wind cable on the reel so that unwinding can be done without kinking the cable. Provide 6 1/2-feet pigtails of cable at each end of the reel readily accessible for testing. Attach a permanent label on each reel showing length, media, identification number, and date of manufacture. Provide water resistant label and ink on the labels. Apply end seals to each end of the media after testing and before terminating to prevent moisture from entering the cable while stored at the job site. Ensure reels are suitable for outside storage conditions when temperature ranges from minus 40 degrees F to plus 150 degrees F, with relative humidity from zero to 100 percent. Store equipment, other than FO media, delivered and placed in storage with protection from weather, humidity and temperature variation, dirt and dust, or other contaminants.

1.7 PROJECT/SITE CONDITIONS

Ensure that the buried cable is fed through the plow into the ground at zero tension. Do not allow tension to develop in the cable.

Whenever the plow is stopped, unreel sufficient cable to guard against sudden jerks when the plow is started.

Exercise caution to ensure that the plow is not backed up while the blade is in the ground. Cable can be severely damaged by the plow backing up even a slight amount. During the plowing operation, the plow may strike a buried object or rock that would stop the equipment and necessitate removal of the plow from the ground. When this occurs, remove the plow carefully without backing up. When it is necessary to back the plow, uncover the cable a sufficient distance back from the plow for inspection by the Contracting Officer to determine if there is any damage. Immediately report any damage to the Contracting Officer. Repair or replace damages as directed by the Contracting Officer.

PART 2 PRODUCTS

2.1 SYSTEM DESCRIPTION

Provide fiber optic cables for the duct in the existing cable duct and manhole system.

Provide installation methods and procedures for installing the FO media and pathway system. Include methods and procedures for installing FO media, pathway, splices, and associated hardware. Submit installation procedures and equipment list to the Contracting Officer.

Provide detailed drawings for the fiber optic cable and pathway system. Provide single line schematic details of the fiber optic and pathway media, splices, and associated construction materials. Ensure drawings are in AUTOCAD.DXF or compatible format. Provide Registered Communications Distribution Designer (RCDD) approved drawings of the fiber optic system. Include drawing details of fiber optic terminations in equipment rooms. Show final configuration, including location, fiber pair count, pathway innerduct arrangement, and pathway assignment of outside plant. Verify FO system is compatible with MIL-STD-188-176.

2.1.1 Fiber Optic Cable Design

2.1.1.1 Fiber Optic Media Types

Verify FO media meets all performance requirements of TIA-568.1, TIA-568.3 and the physical requirements of ICEA S-87-640 and TIA/EIA-598.

a. Multi Mode Fiber Media

Provide FO media with outer sheath jacket, strength member, ripcords, water blocking material, optional steel shield, core tube, and core fibers as installed in a permanent underground pathway system as shown on the construction drawings. Provide FO media with an all glass, graded index material with a nominal core diameter of 50 microns OM4. Provide a cladding material for the fiber which is compatible with the core. Center media transmission window at 850 and 1300 nanometer wavelengths, with attenuation at 1300 nanometers less than 2.0 dB per kilometer, and minimum bandwidth of 500 mHz-Km.

b. Single Mode Fiber Media

Provide FO single mode media with outer sheath jacket, strength member, ripcords, water blocking material, optional steel shield, core tube, and core fibers as installed in a permanent underground pathway system as shown on the construction drawings. Provide media with all glass, dual window, graded index material with a core diameter of 8.7 microns. Coat fiber with a cladding material which is concentric with the core. Ensure fiber cladding diameter is a nominal 125 microns, and media has a transmission window centered at 1300 and 1550 nanometer wavelengths. Attenuation at 1550 nanometers is less than 0.5 dB per kilometer. Verify FO media complies with TIA/EIA-472DAAA,and TIA-758.

2.1.1.2 Cable Length

Ensure cable is manufactured continuous with no factory splices.

2.1.1.3 Construction

a. Number of Fibers Per Tube Per Cable

36-fiber cable and 72-fiber cable are required as follows:

(1) Provide 36-fiber cable containing multimode and single mode fibers, with cable core configuration comprised of six loose buffer tubes, each containing six fibers. Color code six fibers in each loose buffer tube using the first colors of the standard Munsell color code, Blue, Orange, Green, Brown, Slate, and White. Color code loose buffer tubes using the standard Munsell color code, Blue, Orange, Green, Brown and Slate. Ensure sixth buffer tube is Pink. Consider single mode fibers last in configuration.

(2) Provide 72-fiber cable containing multimode and single mode fibers, with cable core configuration comprised of 12 loose buffer tubes, each containing six fibers. Color code six fibers in each loose buffer tube using the first colors of the standard Munsell color code, Blue, Orange, Green, Brown, Slate and White. Color code loose buffer tubes using the standard Munsell color code, Blue, Orange, Green, Brown, Slate, Red, Black, Yellow, and

Violet. Ensure eleventh and twelfth buffer tubes are Blue/White and Orange/White, respectively. Consider single mode fibers last in configuration.

b. Inner Jacket

Locate buffer tubes concentrically around the cable central core member and covered with a polyethylene inner jacket. Ensure inner jacket is medium density polyethylene in accordance with ASTM D4976. Fill space between the buffer tubes and inner jacket with a gel compound to prevent air, moisture, or water intrusion in the inner jacket.

c. Pulling Strength Member

Use a ramid type material as pulling strength members in the cable to provide pulling strength of at least 400 pounds for the cable during installation.

d. Cable Outer Jacket

Apply black high density, high-molecular weight, polyethylene materials in accordance with ASTM D4976 longitudinally over all the inner jacket and sheathing strength member to form the cable outer jacket. Ensure outer jacket is smooth, concentric, non-nutrient to fungus, and free from holes, splits, blisters, or other imperfections. Overall outside cable diameter cannot exceed 0.75-inch.

2.1.2 Cable Identification Symbol

First of three lines on the ID symbol employ 5 characters.

First and second characters, from left to right, denotes the number of active optical fibers in the cable.

Third character is a slash.

Fourth and fifth characters denote optical transmission windows which the optical fiber can support. These windows are defined herein as follows:

a. Fourth character is an "A" or an "O." The "A" denotes a window at a wavelength of 850 nanometers (nm) with an attenuation of 4 dB/kilometer (km) and a bandwidth of 800 MHz-km. Use an "O" character if these requirements are not met.

b. Fifth character is a "B" or an "O." The "B" denotes a window at a wavelength of 1,300 nanometer (nm) with an attenuation of 1.0 dB/km and a bandwidth of 1,000 MHz-km. Use an "O" character if these requirements are not met.

Two lower lines of the cable ID symbol indicate multi-mode or single mode fibers, the cable number and the fiber count:

Example:

72/OB	Identifies the number of optical fibers (72) and the optical transmission window (OB - See preceding paragraph)

FM05 : 61-120	Identifies Multi-Mode Fiber Cable 05 with MM Fibers 61 through 120.
FS05 : 13-24	Identifies Single Mode Fiber Cable 05 with SM Fibers 13 through 24.

2.1.3 Temperature Environment

Provide fiber optical cable compliant with the mechanical performance requirements herein while used in duct applications where the temperature varies from 17.6 degrees F to 100 F. Ensure optical performance degradation is less than five percent of the optical performance requirements in the temperature range of minus 4 degrees F to 140 degrees F. Do not damage fiber optical cable in storage where the temperature may vary from minus 40 degrees F to 149 degrees F.

2.1.4 Splice Compatibility Test

When the material of the optic fiber is different from Cornings' Class Code No. 1517 for multi-mode graded index fiber and No. 1528 for single-mode fiber, perform and document the Splice Compatibility Test with Vendor as follows:

a. Fabricate and measure a minimum of 10 fusion splices using fiber from the different production lots and a sample of Corning fiber, Class Code No. 1517 and No. 1528, supplied by the Government.

b. Measure fusion splices using an Optical Time Domain Reflectometer (OTDR) operating in the region of 1250 through 1350 nm. Ensure the insertion loss of the fusion splice equals the average of two OTDR measurements, one taken with the OTDR installed on the Corning fiber, and the other with the OTDR installed on the vendor's fiber. Verify Vendor's fiber and the Corning fiber are each a minimum of 1 Km in length throughout the testing.

c. Consider vendor's fiber compatible with the Corning fiber if the maximum splice insertion loss of each of 10 fusion splices tested measures less than 0.2 dB.

   Allow a maximum of three retries on any one splice to obtain a loss of 0.2 dB or less.

Perform these tests under Government supervision.

2.2 EQUIPMENT

2.2.1 Replacement Cable

Provide not less than a 0.5 kilometer reel of each size and type of the manufacturer's furnished cable in addition to cable sections indicated.

Deliver replacement cable reels to the Government as directed by the Contracting Officer.

2.2.2 Splice Organizers

Provide fusion spliced single mode or multi-mode fibers with a protective sleeve covering, stored in an organizer with a minimum of 18-inches spare

coiled buffer tubing. Ensure single mode fibers are spliced last in the splice tray.

Complete a 72 fiber splice in an outer closure. Organizer assembly, with one tray containing 12 fusion splices each requires five extra trays, to form the section complete in the inner closure.

Fill space between the inner and outer closures with encapsulating fluid. Factory drill end plates to fit the cable(s) outer diameter.

2.2.3 Pre-Connected Cable Assembly

Provide factory assembled pre-connectorized cable assembly to interface with the patch panel bulkhead feed-through receptacle. Provide dust caps for all terminated fibers.

Ensure multi-mode fiber optic cable assembly is comprised of a single fiber connector, terminated on three (3) meter length of single fiber, multi-mode cable. Verify single fiber cable contains a buffered optical fiber the same as that provided in the multi-fiber cable.

Ensure single fiber optic cable assembly is comprised of a single fiber connector terminated on the three (3) meter length of single fiber, single mode cable. Single fiber cable contains a buffered optical fiber, the same as that provided in the multi-fiber cable. Ensure return loss for single mode connectors is a minimum of minus 30dB.

Provide connector/cable interface on both the single and multi-mode cable assemblies able to withstand a tensile force of 25 pounds without detrimental affects on the connector loss characteristics.

Verify each connectorized cable assembly has a loss of less than or equal to 0.5 dB .

2.2.4 Optical Patch Panel Assemblies

Provide all cable terminations in optical patch panel assemblies, with patch panel assemblies of the pre-assembled chassis type with associated rack-mounting hardware.

To facilitate the transition between outside plant cable and the preconnectorized cable assemblies, ensure the fibers are fusion spliced and housed in a splice tray. Position splice tray in the optical patch panel assembly as indicated. Ensure splice attenuation does not exceed 0.2 db. Cover splice with a protective sleeve.

2.2.5 Fiber Optic Terminations And Connectors

FO connectors to comply with TIA/EIA-4750000-C and TIA/EIA-604-3.

2.2.6 Fiber Optic Pathway System

Provide an FO pathway system including raceway conduit, duct system, and maintenance manholes and handholes as shown on the drawings. Provide pathway materials compliant with TIA-569, and the following commercial standards for construction materials, NEMA RN 1 (PVC), NEMA TC 2 (PVC), NEMA TC 3 (PVC), NEMA TC 6 & 8, and NEMA TC 9.

2.2.7 FO Media Tags

Provide stainless steel, 1 5/8-inches in diameter 1/16-inch thick, and circular in shape.

2.3 MATERIALS

Verify all materials used within a given cable are compatible with all other materials used in the same cable when such materials come into intimate contact. Ensure all cable components used have no adverse affect on optical transmission or on the mechanical integrity characteristics of the fiber placed in the cable, and all materials used are non-toxic, non-corrosive, and present no dermal hazard.

Minimum required material components applied to fiber optic cable construction are: central core member, color-coded optical fiber, color-coded loose tube buffer with gel-filling, gel-filling around loose tube, inner jacket, pulling strength members, and outer jacket. Variations in sequence and construction structural components will be considered when necessary.

2.3.1 Central Core Member

Include a central core member to serve as a cable core foundation to reduce strain on the fibers but not to serve as a pulling strength member. Ensure material of the central core member is non-metallic.

2.3.2 Optical Fibers

Provide two types of optical fibers, single-mode fiber and multi-mode fiber, within the cable as follows:

a. Provide Single-Mode (SM) fiber of equivalent graded index optical glass, with a fiber core diameter of approximately 8.7 micrometer. Cladding diameter is 125 plus or minus 3 micrometer with core cladding offset less than 1 micrometer. Ensure minimum tensile strength of the fiber after primary protective coating is greater than 50,000 psi.

b. Provide multi--Mode (MM) fiber of the graded index optical glass type, with a core diameter of 50 plus or minus 3 micrometers. Cladding diameter is 125 plus or minus 3 micrometers. Ensure the core-cladding offset is less than 3 micrometer, and the minimum tensile strength of the fiber after primary protective coating is greater than 50,000 psi.

Softening point of the optical fiber clad material is 1630 degrees C plus or minus 50 degrees C in accordance with ASTM C338, or the optical fiber meets the requirements in paragraph SPLICE COMPATIBILITY TEST.

2.3.3 Fiber Primary Protective Coating

Coat optical fiber with suitable material to preserve the intrinsic high tensile strength of the glass fiber. Ensure outside diameter of the coated optical fiber is 250 (plus or minus 15) micrometer. Provide coating material which is readily removable, mechanically or chemically, without damaging the optical fibers when the removal is desired.

2.3.4 Optical Fiber Color-Code Coating

Coat primary protective coated SM and MM fibers with a color-code coating

for individual fiber identification. Maximum outside diameter of color-code coated fiber is less than 300 micrometer.

2.3.5 Loose Tube Buffering

Surround color-code coated fibers with a loose tube buffering for protection from external mechanical and environmental influences. Fill interior of the tube with a suitable gel-fitting compound to prevent water migration. Color code loose tube buffering for the tube identification.

2.3.6 Colorants

Verify color concentrates or inks used to color code the optical fibers and the loose buffer tube are not susceptible to migration and chemical reaction with gel filling compound.

2.3.7 Filling Compound

Ensure inner jacket interior and loose tube buffer cavity contains a gel-type filling compound, of suitable viscosity so that it protects the optical fibers against the ingress of water and/or soluble chemicals, and not flow at the temperature of up to 149 degrees F. Verify gel filling compound is electrically non-conducting, inert gel-type, waterproof compound, non-toxic, with no dermal hazards, and compatible chemically and mechanically with all cable components and associated splice hardware materials to which it may make contact. Ensure gel filling compound is removable, as required, using commercially available products under field-type conditions.

2.4 TESTS, INSPECTIONS, AND VERIFICATIONS

2.4.1 Factory FO Quality Control

Provide conduit factory quality tests of FO media as required by TIA-472D000.

2.4.2 Factory Test Certificates

Provide fiber optical cable complying with the following optical and mechanical test requirements.

2.4.2.1 Optical Performance

a. Multi-Mode Fibers in the Cable

Verify optical attenuation of each optical fiber in the cable (reeled) is no greater than 1.0 dB/Km at 1300 plus or minus 50 nm optical spectrum window. Measure attenuation on completed cable reel length, and normalized linearly to 1 Km.

Verify bandwidth at minus 3 dB optical power of each optical fiber in the cable (reeled) is a bandwidth length product, gamma equals 1, greater than 1 GHz-Km at 1300 plus or minus 50 nm optical spectrum window.

Verify numerical aperture of each optical fiber is 0.2 plus or minus 0.015 at 1300 nm optical spectrum window. Ensure method of numerical aperture measurement is in accordance with TIA-455-177, at central wavelength 1300 nm nominal. When this requirement is not met, apply the fusion splice compatibility test.

b. Single-Mode Fibers in the Cable

Verify optical attenuation of each optical fiber in the cable (reeled) is no greater than 0.5 dB/Km at 1300 plus or minus 50 nm optical spectrum window. Measure attenuation on completed cable reel length, and normalized linearly to 1 Km. Ensure measurement method is in accordance with TIA-455-78-B, at central wavelength 1300 nm nominal.

Verify pulse dispersion of each optical fiber in the cable (reeled) is no greater than 3.5 picosecond/nm-Km within the emissive region of 1285-1330 nm. Ensure measurement method is in accordance with TIA-455-175.

Verify mode field diameter at 1300 nm optical spectrum window is within 10 plus or minus 1 micrometer. Ensure measurement method is in accordance with EIA/TIA 455-165A at central wavelength 1300 nm nominal. When this requirement is not met, apply the fusion splice compatibility test.

Verify cut-off wavelength for 1300 nm optical spectrum window is within 1200 plus or minus 70 nm. Ensure measurement method is in accordance with ANSI/TIA-455-80C.

2.4.2.2 Mechanical Performance

a. Minimum Bend Radius

Provide cable which withstands bending to a minimum radius of 10 times the cable outer diameter without tensile load applied, and of 20 times the cable outer diameter with maximum tensile load applied (during installation), without damage to cable components or degradation of the optical fiber performance at room temperature.

b. Tensile Strength

Provide fiber optical cable which withstands a pull force of at least 400 pounds to be applied to the pulling strength member during the installation, and a tensile load of at least 300 newtons during operation without incurring any damage or detriment to fiber optical cable and optical performance. Ensure tensile strength test is in accordance with TIA-455-33.

c. Flexing or Bending Cycles

Provide fiber optical cable which withstands at least 20 bending cycles at minimum bend radius without damage to the fiber optic cable components or degrading optical performance. Ensure cyclic flexing test is in accordance with TIA-455-104.

d. Crush Resistance

Provide minimum crush resistance of the fiber optical cable greater than 650 newton/centimeter (cm) without damage to cable components or degrading optical performance. Ensure crush resistance test is in accordance with TIA/EIA 455-41-A.

e. Impact Resistance

Provide fiber optical cable capable of withstanding 20 impacts, at five newton-meters force, without damage to cable components, or degradation of

optical performance. Ensure impact resistance test is in accordance with TIA/EIA-455-25.

f. Gel Filling Compound Drip Test

Test optical cable for the ability of the gel filling compound in the interior of the inner jacket and loose tube buffer to resist flow at the temperature range of minus 40 degrees C to 60 degrees C in accordance with TIA/EIA-455-81.

g. Fluid Penetration

Provide optical cable capable of preventing the entry and axial migration of pressurized water when subjected to fluid penetration testing in accordance with TIA-455-82.

2.4.3 Factory Reel Test

Test 100 percent OTDR test of FO media at the factory prior to shipment in accordance with TIA-568.1 and TIA-568.3. Use TIA-526-7 for single mode fiber and EIA TIA/EIA-526-14A Method B for multi mode fiber measurements. Calibrate OTDR to show anomalies of 0.2 dB minimum. Provide digitized or photographic traces to the Contracting Officer.

PART 3 EXECUTION

3.1 INSTALLATION

Install and test the FO media in accordance with contract drawings, specifications, IEEE C2, NFPA 70, and TIA-590. Provide all necessary power, utility services, technicians, test equipment, calibration equipment as required to perform reel and final acceptance tests of the media. Replace all media which fails the factory or reel tests or final acceptance field tests and re-test at the contractors expense.

3.1.1 Fiber Splices

Splices are not permitted unless shown on the construction drawings.

Field test splices within 24 hours after splice installation. Test splices to demonstrate a maximum 0.2 dB loss. Provide a minimum of 6 1/2-feet for routing and testing media. Provide fusion type outside plant fiber splices along the fiber route. Make all splice measurements at 1300 nm, plus or minus 5 nm. Mount all splices in trays. Do not increase number of splices.

Protect media ends of unspliced FO media during splicing operations. Cover completed splice with a protective sleeve heat shrink type to restore the protective properties of the fiber coating and buffering. Deviations to the splice, location and pulling plan will be permitted, upon approval by the Contracting Officer, at no additional cost to the Government.

Ensure all fiber colors are continuous from end to end. No switching or staggering of color scheme within the cable at splice points is allowed. Splice fibers in order with multi-mode fibers identified first and single mode fibers at the end.

Bring cables out of the manhole in a controlled environment to perform the

fiber fusion splice operation. Complete splice by returning the cable to the manhole such that the excess cable does not impede future entrance and utilization. Secure cable at regular intervals.

3.1.2 Contractor Damage

Promptly repair indicated utility and communications lines or systems damaged during site preparation and construction. When Contractor is advised in writing of the location of a non-indicated line or system, such notice provides that portion of the line or system with "indicated" status in determining liability for damages. In every event, immediately notify the Contracting Officer of damage.

3.1.3 Underground Cable

Provide inner duct assignment of individual cables as indicated. Do not place cables in ducts other than those specified.

Exercise adequate care when handling and storing reels of cable to prevent damage to the cable. Do not install cable with dents, flat spots, or other sheath distortions.

3.1.3.1 Securing Cable

Immediately after cable placement, attach a permanent identification tag as indicated to visible cable sections. Check cables to ensure that the markings are intact.

Support and secure cables and equipment as indicated. Where the specific method of support is not shown, use supports and fasteners to secure cables and equipment in position. Provide metallic supports and fasteners with a corrosion resistant finish. Rout all cables along the interior sides of manholes.

Provide two or more cable hooks per manhole.

Use clamps and straps as necessary to properly secure the cable.

3.1.3.2 Bending

Use caution when bending cable to avoid kinks or other damage to the sheath. Bend radius is as large as possible with a minimum of 10 -inches. Increase minimum radius when necessary to meet cable manufacturer's recommendation. Do not rest cables against any sharp edges.

Pull and splice cable in the manner and at the locations shown.

3.1.3.3 Pulling

Attach pulling lines to both cable ends when cable is destined for bi-directional pull, and fitted with factory-installed pulling eyes. Pull cables not equipped with a pulling eye using a pulling line attached to the cable end by means of a cable grip. Do not use core hitches.

Locate and align cable reels so that the cable is paid out from the top of the reel into the duct or conduit in a long, smooth bend without twisting. Do not pull cable from the bottom of the reel. Use a cable feeder guide of proper dimensions at the mouth to guide the cable into the duct or conduit.

Set up rigging at the pulling end so that the pulling line and cable exit on a line parallel with the duct or conduit to prevent either from rubbing against the edge or mouth. Do not pull cable ends around sheave wheels. When the sheave or pulley cannot be positioned to obtain sufficient cable end slack for proper racking and splicing with the pulling line attached to the end of the cable, a split cable grip may be used to obtain the necessary slack.

3.1.3.4 Lubricant

Use pulling lubricant to minimize pulling tension and prevent sheath damage when pulling cables into ducts and conduits. Apply lubricant to the cable sheath with a lubricator. When pulling has been completed, wipe the exposed cable ends clean of lubricant.

Ensure lubricants are compatible with and intended for use with plastic-sheathed cables. Do not allow soap and grease type lubricants.

Check all equipment and the pulling set to minimize interruptions once pulling begins. Pull cable without stopping until the required amount of the cable has been placed. When the pulling operation is halted before the pull is completed, do not release the tension of the pulling line. When pulling is resumed, overcome the inertia of the cable by increasing the tension in small steps a few seconds apart until the cable is in motion. Feed the cable from the top of the reel by rotating the reel in the feed direction at the rate of pull. Do not strip cable off the reel by pulling.

3.1.3.5 Damage and Defects

Use a tension monitoring device to ensure that the maximum pulling tension that may be applied to the cable to be pulled into a conduit section is not exceeded. Any damage to the cable due to exceeding the maximum tension will require a new cable furnished by the Contractor.

Carefully inspect cable for sheath defects or other irregularities as it is paid out form the reel. When defects are detected, stop pulling immediately and repair or replace the cable section at the discretion of the Contracting Officer. Maintain a system of communications between pulling and feed locations so that pulling can be stopped instantly, when required.

Hand guide cable through intermediate manholes and into the next duct section when making pull-throughs. Use proper rigging in the intermediate manhole to keep the pulling line and cable aligned with the exit duct to prevent the line or cable from rubbing against the edge of the duct. Set up cables in pull-through manholes and rack before the cable ends in adjacent manholes are set up and racked.

Tie cable ends pulled into manholes, vaults, or terminal locations that are not to be racked or otherwise permanently positioned immediately, in fixed positions to prevent damage to the cables and provide adequate working space.

3.1.3.6 Seal

Seal ducts or innerduct in which cable is placed with urethane foam duct seal. Insert this material between the cable and the duct or innerduct of

which it is in, between the innerduct and the duct, and in all unused innerduct, in order to prevent damage to the cable sheath and to prevent the entrance of dirt or water into the manhole or vault.

Provide cables in continuous lengths as required to accomplish the required installation without splices from termination to termination, except where field splices are specifically shown.

3.1.4 Cable Installation in Cable Trays

Do not install communication cables in the same cable tray with ac power cables.

Install cables placed in cable trays in a neat and orderly manner and not crossed or interlaced with other cables except at breakout points.

Individually retain cables in vertical trays with straps at a maximum of 6 -feet on center.

3.1.5 Grounding Systems

Ground cables at each termination point or as indicated.

3.1.6 Reconditioning of Surfaces

3.1.6.1 Unpaved Surface Treatment

Restore unpaved surfaces disturbed during the installation of duct or direct burial cable to their original elevation and condition. Carefully preserve existing sod and topsoil and replace after the back-filling is completed. Replace damaged sod with sod of quality equal to that removed. Where the surface is disturbed in a newly seeded area, re-seed the restored surface with the same quantity and formula of seed as that used in the original seeding.

3.1.6.2 Paving Repairs

a. Where trenches, pits, or other excavations are made in existing roadways and in other areas of pavement where surface treatment of any kind exists, restore such surface treatment or pavement to the same thickness and to the same kind as previously existed. Ensure surface treatment or pavement matches and ties into the adjacent and surrounding existing surfaces.

3.1.7 Cable Pulling

Test duct lines with a mandrel and swab out to remove foreign material before the pulling of FO media. Avoid damage to cables in setting up pulling apparatus or in placing tools or hardware. Do not step on media when entering or leaving the maintenance holes. Do not place media in ducts other than those shown without prior written approval of the Contracting Officer. Roll cable reels in the direction indicated by the arrows painted on the reel flanges. Set up media reels on the same side of the maintenance hole as the pathway section in which the media is to be placed. Level the reel and bring into proper alignment with the pathway section so that the media pays off from the top of the reel in a long smooth bend into the duct without twisting. Do not, under any circumstances roll the media off from the bottom of the reel. Check the equipment set up prior to beginning the media cable pulling to avoid an

interruption once pulling has started. Use a cable feeder guide of suitable dimensions between media reel and face of duct to protect media and guide cable into the duct as it is rolled off the reel. As media is rolled off the reel, lubricate and inspect media for sheath defects. When defects are noticed, stop pulling operations and notify the Contracting Officer to determine required corrective action. Stop media pulling if reel binds or does not roll off freely. Rectify cause of binding before resuming pulling operations. Provide media lubricants recommended by the cable manufacturer. Provide 3.3-feet of spare media in all manholes and enclosures for final termination and testing.

3.1.7.1 FO Media Tensions

Install FO media as shown on construction drawings. Provide devices to monitor media tension during installation. Do not exceed manufacturers recommended maximum FO tensions and bending radii during installation.

3.1.7.2 Pulling Eyes

Equip media 1-1/4-inches in diameter and larger with cable manufacturer's factory installed pulling-in eyes. Provide media with diameter smaller than 1-1/4-inches with heat shrinkable type end caps or seals on cable ends when using cable pulling grips. Do not beat rings to prevent grip from slipping into the cable sheath. Use a swivel grip of 3/4-inch links between pulling-in eyes or grips and pulling strand.

3.1.7.3 Media in Maintenance Manholes, Handholes, and Vaults

Do not install media utilizing the shortest route, but route along those walls providing the longest route and the maximum spare cable lengths. Form cables to closely parallel walls, not to interfere with duct entrances. Support media on brackets and cable insulators at a maximum of 4-feet. In existing maintenance manholes, handholes, and vaults where new ducts are to be terminated, or where new media are to be installed, modify the existing installation of media, cable supports, and grounding as required with cables arranged and supported as specified for new media.

3.2 FIELD QUALITY CONTROL

3.2.1 Test Requirements

Ensure test equipment used for verifying installation testing is calibrated by a certified testing company within 3 weeks of use.

3.2.1.1 Single and Multi-Mode OTDR Test

Ensure the Optical Time Domain Reflectometer (OTDR) conforms to the following minimum requirements:

a. Operating wavelengths: 1,300 plus or minus 20 nanometers

b. Attenuation Range (one way): minimum 15 dB at 1,300 nm

c. Attenuation Resolution: 0.01 dB

d. Accuracy: plus 0.5 dB

Use OTDRs with digital readout capability and a means of providing a permanent record in the form of a strip chart.

3.2.1.2 End-to-End Attenuation Tests

An attenuation measurement test set consists of an optical power meter and an optical power source. Provide attenuation measurement test set in accordance with the applicable National Bureau of Standards (NBS) standards for a stable optical source. Meter may be analog or digital. Include end-to-end attenuation test reading on the test reference loss. Ensure measurement test set conforms to the following minimum requirements:

a. Operating wavelengths: 1,300 plus or minus 10 nanometers

b. Attenuation Range: at least 30 dB at 1,300 nm

c. Attenuation Resolution: 0.01 dB

d. Accuracy: The accuracy of the attenuation measurement test set is plus or minus 5 percent.

Ensure optical source is capable of coupling sufficient power into the fiber so that the light received at the meter is within the meter delectability limits.

3.2.1.3 End-to-End Bandwidth Tests

Ensure bandwidth test conforms to the following minimum requirements:

a. Operating wavelengths: 1,300 plus or minus 10 nanometers

b. Bandwidth range: minimum 1000 megahertz

c. Bandwidth Resolution: 1 megahertz

d. Accuracy: plus or minus 0.5 megahertz, Measurement Method: Swept Frequency

As a minimum, test each fiber cable before and after installation for any faults or attenuations using an Optical Time Domain Reflectometer (OTDR). Conduct end-to-end attenuation tests after complete installation.

Clearly state all test equipment, test procedures, and testing techniques in the quality assurance plan. Conduct tests in accordance with the approved Quality Assurance Plan. Ensure all field tests are witnessed by the Contracting Officer. Give Contracting Officer at least 20 calendar days notice prior to performing each test.

Provide each test sheet with a sign-off blank for both Contractor and the Contracting Officer. Deliver copies of the completed test forms and test results as indicated.

Record sequential cable markings along the cable on the sequential cable form, prior to and after each end of splice point,and submit for approval.

Submit test results on all installed fiber cabling before and after each pre-connectorized cable assembly splice is completed.

Maintain an accurate test record during all field tests.

3.2.2 Field Reel Tests

Perform the following tests on FO media at the job site before it is removed from the cable reel. For cables with factory installed pulling eyes, perform these tests at the factory and submit certified test results with the media. Perform OTDR tests with media on reels and compare factory and field test data.

3.2.2.1 Reel Test Reports

Provide results of reel tests to the Contracting Officer within 5 working days before installation is to commence. Verify results indicate reel number of the media, manufacturer, type and number of fiber tested, and recorded readings in the report. When reel tests indicate that the media does not comply with factory reel test reports remove the media from the job site and replace with compliant media.

3.2.3 Final Acceptance Tests

Perform end-to-end tests including power meter light source and OTDR tests. Perform OTDR measurements as required by TIA-568.1 and TIA-568.3. Test single mode fiber in accordance with TIA-526-7 (Optical Power Loss). Test multi mode fiber in accordance with TIA-526-14(Optical Power Loss).

3.2.3.1 Test Results

Provide results of final acceptance tests (attenuation tests, OTDR traces, etc.), to the Contracting Officer within 5 working days after completion of tests.

3.3 CLOSEOUT ACTIVITIES

Submit 5 copies of the Record (As-Built) Drawings to the Contracting Officer.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 28 - ELECTRONIC SAFETY AND SECURITY

SECTION 28 31 76

INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE

PART 1 GENERAL

1.1 REFERENCES
1.2 RELATED SECTIONS
1.3 SUMMARY
1.3.1 Scope
1.3.2 Qualified Fire Protection Engineer (QFPE)
1.4 DEFINITIONS
1.4.1 Interface Device
1.4.2 Fire Alarm and Mass Notification Control Unit (FMCU)
1.4.3 Local Operating Console (LOC)
1.4.4 Terminal Cabinet
1.4.5 Control Module and Relay Module
1.4.6 Designated Fire Protection Engineer (DFPE)
1.4.7 Qualified Fire Protection Engineer (QFPE)
1.4.8 Manufacturer's Technical Representative (MTR)
1.5 SUBMITTALS
1.6 SYSTEM OPERATION
1.6.1 Alarm Initiating Devices and Notification Appliances (Visual, Voice, Textual)
1.6.2 Functions and Operating Features
1.7 TECHNICAL DATA AND SITE-SPECIFIC SOFTWARE
1.8 QUALITY ASSURANCE
1.8.1 Submittal Documents
1.8.1.1 Preconstruction Submittals
1.8.1.2 Shop Drawings
1.8.1.3 Nameplates
1.8.1.4 Wiring Diagrams
1.8.1.5 System Layout
1.8.1.6 Notification Appliances
1.8.1.7 Initiating Devices
1.8.1.8 Amplifiers
1.8.1.9 Battery Power
1.8.1.10 Voltage Drop Calculations
1.8.1.11 Product Data
1.8.1.12 Operation and Maintenance (O&M) Instructions
1.8.1.13 As-Built Drawings
1.8.2 Qualifications
1.8.2.1 Fire Alarm System Designer
1.8.2.2 Supervisor
1.8.2.3 Technician
1.8.2.4 Installer
1.8.2.5 Test Technician
1.8.2.6 Manufacturer
1.8.2.7 Manufacturer's Representative
1.8.3 Regulatory Requirements

1.9 DELIVERY, STORAGE, AND HANDLING
1.10 MAINTENANCE
1.10.1 Spare Parts
1.10.2 Special Tools

PART 2 PRODUCTS

2.1 GENERAL PRODUCT REQUIREMENT
2.2 MATERIALS AND EQUIPMENT
2.2.1 Standard Products
2.2.2 Nameplates
2.2.3 Keys
2.2.4 Instructions
2.3 FIRE ALARM AND MASS NOTIFICATION CONTROL UNIT
2.3.1 Cabinet
2.3.2 Silencing Switches
2.3.2.1 Alarm Silencing Switch
2.3.2.2 Supervisory/Trouble Silencing Switch
2.3.3 Non-Interfering
2.3.4 Audible Notification System
2.3.4.1 Outputs and Operational Modules
2.3.4.2 Mass Notification
2.3.4.3 Installation-Wide Control
2.3.5 Memory
2.3.6 Field Programmability
2.3.7 Input/Output Modifications
2.3.8 Resetting
2.3.9 Walk Test
2.3.10 History Logging
2.3.11 Manual Access
2.4 LOCAL OPERATING CONSOLES (LOC)
2.4.1 General
2.5 AMPLIFIERS, PREAMPLIFIERS, TONE GENERATORS
2.5.1 Operation
2.5.2 Construction
2.5.3 Inputs
2.5.4 Tone Generator
2.5.5 Protection Circuits
2.6 REMOTE ANNUNCIATOR
2.6.1 LCD Annunciator
2.7 MANUAL STATIONS
2.8 ISOLATION MODULES
2.9 SMOKE DETECTORS
2.9.1 Spot Type Detectors
2.9.2 Duct Smoke Detectors
2.10 ADDRESSABLE INTERFACE DEVICES
2.11 ADDRESSABLE CONTROL MODULES
2.12 NOTIFICATION APPLIANCES
2.12.1 Audible Notification Appliances
2.12.1.1 Speakers
2.12.2 Visual Notification Appliances
2.13 ELECTRIC POWER
2.13.1 Primary Power
2.14 SECONDARY POWER SUPPLY
2.14.1 Batteries
2.14.1.1 Capacity
2.14.1.2 Battery Power Calculations
2.14.2 Battery Chargers
2.15 SURGE PROTECTIVE DEVICES

2.16 WIRING
2.16.1 Alarm Wiring
2.17 INTERFACE TO THE BASE-WIDE MASS NOTIFICATION NETWORK
2.17.1 Radio
2.17.2 Secure Radio System
2.17.2.1 Communications Network
2.17.2.2 Radio Frequency Communications
2.17.2.3 Licensed Radio Frequency Systems
2.18 AUTOMATIC FIRE ALARM TRANSMITTERS
2.18.1 Radio Transmitter and Interface Panels
2.18.1.1 Operation
2.18.1.2 Battery Power
2.18.1.3 Transmitter Housing
2.18.1.4 Antenna
2.18.2 Signals to Be Transmitted to the Base Receiving Station
2.19 SYSTEM MONITORING
2.19.1 Valves
2.19.2 Room Low Temperature Supervisory Switch
2.19.3 Electromagnetic Door Holders
2.19.4 Knox Box Tamper Supervisory Switch
2.20 ENVIRONMENTAL ENCLOSURES OR GUARDS
2.21 TEXTUAL DISPLAY SIGNS

PART 3 EXECUTION

3.1 VERIFYING ACTUAL FIELD CONDITIONS
3.2 INSTALLATION
3.2.1 Fire Alarm and Mass Notification Control Unit (FMCU)
3.2.2 Battery Cabinets
3.2.3 Manual Stations
3.2.4 Notification Appliances
3.2.5 Smoke Detectors
3.2.6 LCD REMOTE Annunciator
3.2.7 Electromagnetic Door Holder Release
3.2.8 Local Operating Console (LOC)
3.3 SYSTEM FIELD WIRING
3.3.1 Wiring within Cabinets, Enclosures, and Boxes
3.3.2 Terminal Cabinets
3.3.3 Alarm Wiring
3.3.4 Back Boxes and Conduit
3.3.5 Conductor Terminations
3.4 FIRESTOPPING
3.5 PAINTING
3.6 FIELD QUALITY CONTROL
3.6.1 Test Procedures
3.6.2 Pre-Government Testing
3.6.2.1 Verification of Compliant Installation
3.6.2.2 Request for Government Final Test
3.6.3 Correction of Deficiencies
3.6.4 Government Final Tests
3.7 MINIMUM SYSTEM TESTS
3.7.1 System Tests
3.7.2 Audibility Tests
3.7.3 Intelligibility Tests
3.8 SYSTEM ACCEPTANCE
3.9 INSTRUCTION OF GOVERNMENT EMPLOYEES
3.9.1 Instructor
3.9.2 Required Instruction Time
3.9.2.1 Technical Training

3.9.3 Technical Training Manual
3.10 EXTRA MATERIALS
3.10.1 Repair Service/Replacement Parts
3.10.2 Spare Parts
3.10.3 Document Storage Cabinet

-- End of Section Table of Contents --

SECTION 28 31 76

INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ACOUSTICAL SOCIETY OF AMERICA (ASA)

ASA S3.2	(2020) American National Standard Method for Measuring the Intelligibility of Speech Over Communication Systems (ASA 85)

AIR NATIONAL GUARD ENGINEERING TECHNICAL LETTERS (ETL)

ANGETL-15-01-00	Air National Guard Design Policy
ANGETL 15-01-03	Fire Protection Design Guidance

FM GLOBAL (FM)

FM APP GUIDE	(updated on-line) Approval Guide http://www.approvalguide.com/

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE C62.41.1	(2002; R 2008) Guide on the Surges Environment in Low-Voltage (1000 V and Less) AC Power Circuits
IEEE C62.41.2	(2002) Recommended Practice on Characterization of Surges in Low-Voltage (1000 V and Less) AC Power Circuits

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 4	(2018) Standard for Integrated Fire Protection and Life Safety System Testing
NFPA 70	(2023) National Electrical Code
NFPA 72	(2022; ERTA 22-1) National Fire Alarm and Signaling Code
NFPA 90A	(2021) Standard for the Installation of Air Conditioning and Ventilating Systems
NFPA 170	(2021) Standard for Fire Safety and Emergency Symbols

U.S. DEPARTMENT OF DEFENSE (DOD)

UFC 3-601-02	(2021) Fire Protection Systems Inspection, Testing, and Maintenance
UFC 4-010-06	(2016; with Change 1, 2017) Cybersecurity of Facility-Related Control Systems

U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)

47 CFR 15	Radio Frequency Devices
47 CFR 90	Private Land Mobile Radio Services

UNDERWRITERS LABORATORIES (UL)

UL 228	(2006; Reprint Mar 2022) UL Standard for Safety Door Closers-Holders, With or Without Integral Smoke Detectors
UL 268	(2016; Reprint Nov 2021) UL Standard for Safety Smoke Detectors for Fire Alarm Systems
UL 268A	(2008; Reprint Oct 2014) Smoke Detectors for Duct Application
UL 464	(2016; Reprint Sep 2017) UL Standard for Safety Audible Signaling Devices for Fire Alarm and Signaling Systems, Including Accessories
UL 497B	(2004; Reprint Feb 2022) UL Standard for Safety Protectors for Data Communications and Fire Alarm Circuits
UL 864	(2014; Reprint May 2020) UL Standard for Safety Control Units and Accessories for Fire Alarm Systems
UL 1283	(2017) UL Standard for Safety Electromagnetic Interference Filters
UL 1449	(2021) UL Standard for Safety Surge Protective Devices
UL 1480	(2016; Reprint Sep 2017) UL Standard for Safety Speakers for Fire Alarm and Signaling Systems, Including Accessories
UL 1638	(2016; Reprint Sep 2017) UL Standard for Safety Visible Signaling Devices for Fire Alarm and Signaling Systems, Including Accessories
UL 1971	(2002; Reprint Oct 2008) Signaling Devices for the Hearing Impaired
UL 2017	(2008; Reprint Dec 2018) UL Standard for

	Safety General-Purpose Signaling Devices and Systems
UL 2572	(2016; Bul. 2018) UL Standard for Safety Mass Notification Systems
UL Fire Prot Dir	(2012) Fire Protection Equipment Directory

1.2 RELATED SECTIONS

Refer to the following sections for related work and coordination:

Section 21 13 13 WET PIPE SPRINKLER SYSTEM, FIRE PROTECTION
Section 08 71 00 DOOR HARDWARE for door release and additional work related to finish hardware.
Section 14 21 23 ELECTRIC TRACTION PASSENGER ELEVATORS for additional work related to elevators.
Section 07 84 00 FIRESTOPPING for additional work related to firestopping.

1.3 SUMMARY

1.3.1 Scope

a. This work includes designing and providing a new, complete, fire alarm and mass notification (MNS) system as described herein and on the contract drawings for the Noarth Carolina Air National Guard Security Forces Facility. Include system wiring, raceways, pull boxes, terminal cabinets, outlet and mounting boxes, control equipment, initiating devices, notification appliances, supervising station fire alarm transmitters/mass notification transceiver, and other accessories and miscellaneous items required for a complete operational system even though each item is not specifically mentioned or described. Provide system complete and ready for operation. Design and installation must comply with UFC 4-010-06, ANGETL-15-01-00, ANGETL 15-01-03 and AFGM 2019-320-02.

b. Provide equipment, materials, installation, workmanship, inspection, and testing in strict accordance with NFPA 72, except as modified herein. The system layout on the drawings show the intent of coverage and suggested locations. Final quantity, system layout, and coordination are the responsibility of the Contractor.

c. Each remote fire alarm control unit must be powered from a wiring riser specifically for that use or from a local emergency power panel located on the same floor as the remote fire alarm control unit. Where remote fire control units are provided, equipment for notification appliances may be located in the remote fire alarm control units.

e. Where an emergency generator provides standby power supply for life safety system circuits, the generator must be monitored by the FMCU and transmit emergency generator signals in accordance with NFPA 72.

f. The fire alarm and mass notification system must be independent of the building security, building management, and energy/utility monitoring systems other than for control functions.

1.3.2 Qualified Fire Protection Engineer (QFPE)

Services of the QFPE must include:

a. Reviewing SD-02, SD-03, and SD-05 submittal packages for completeness and compliance with the provisions of this specification. Construction (shop) drawings and calculations must be prepared by, or prepared under the immediate supervision of, the QFPE. The QFPE must affix their professional engineering stamp with signature to the shop drawings, calculations, and material data sheets, indicating approval prior to submitting the shop drawings to the DFPE.

b. Providing a letter documenting that the SD-02, SD-03, and SD-05 submittal package has been reviewed and noting any outstanding comments.

c. Performing in-progress construction surveillance prior to installation of ceilings (rough-in inspection).

d. Witnessing pre-Government and final Government functional performance testing and performing a final installation review.

e. Signing applicable certificates under SD-07.

1.4 DEFINITIONS

Wherever mentioned in this specification or on the drawings, the equipment, devices, and functions must be defined as follows:

1.4.1 Interface Device

An addressable device that interconnects hard wired systems or devices to an addressable system.

1.4.2 Fire Alarm and Mass Notification Control Unit (FMCU)

A master control unit having the features of a fire alarm control unit (FACU) and an autonomous control unit (ACU) where these units are interconnected to function as a combined fire alarm/mass notification system. The FACU and ACU functions may be contained in a single cabinet or in independent, interconnected, and co-located cabinets. The drawings represent this device(s) on the drawings as 'FACU'. The term 'FACU' shall be synonymous with the term 'FMCU' for this specification.

1.4.3 Local Operating Console (LOC)

A unit designed to allow emergency responders and/or building occupants to operate the MNS including delivery of recorded messages and/or live voice announcements, initiate visual, textual visual, and audible appliance operation and other relayed functions.

1.4.4 Terminal Cabinet

A steel cabinet with locking, hinge-mounted door where terminal strips are securely mounted inside the cabinet.

1.4.5 Control Module and Relay Module

Terms utilized to describe emergency control function interface devices as

defined by NFPA 72.

1.4.6 Designated Fire Protection Engineer (DFPE)

The DoD fire protection engineer that oversees that Area of Responsibility for that project. This is sometimes referred to as the "cognizant" fire protection engineer. Interpret reference to "authority having jurisdiction" and/or AHJ in referenced standards to mean the Designated Fire Protection Engineer (DFPE). The DFPE may be responsible for review of the contractor submittals having a "G" designation, and for witnessing final inspection and testing.

1.4.7 Qualified Fire Protection Engineer (QFPE)

A QFPE is an individual who is a licensed professional engineer (P.E.), who has passed the fire protection engineering written examination administered by the National Council of Examiners for Engineering and Surveying (NCEES) and has relevant fire protection engineering experience.

1.4.8 Manufacturer's Technical Representative (MTR)

A MTR is an individual who is an actual manufacturer employee trained in the technical programming, troubleshooting, testing of the fire alarm and mass notification system manufacturer. An employee who is a distributor/installer of a fire alarm system manufacturer shall not be considered a Manufacturer's Technical Representative.

1.5 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval.

Shop drawings (SD-02), product data (SD-03) and calculations (SD-05) must be prepared by the fire alarm designer and combined and submitted as one complete package. The QFPE must review the SD-02/SD-03/SD-05 submittal package for completeness and compliance with the Contract provisions prior to submission to the Government. The QFPE must provide a Letter of Confirmation that they have reviewed the submittal package for compliance with the contract provisions. This letter must include their registered professional engineer stamp and signature. Partial submittals and submittals not reviewed by the QFPE will be returned by the Government disapproved without review.

Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Qualified Fire Protection Engineer (QFPE); G

Fire alarm system designer; G

Supervisor; G

Technician; G

Installer; G

Test Technician; G

Fire Alarm System Site-Specific Software Acknowledgement; G

SD-02 Shop Drawings

Nameplates; G

Instructions; G

Wiring Diagrams; G

System Layout; G

Notification Appliances; G

Initiating devices; G

Amplifiers; G

Battery Power; G

Voltage Drop Calculations; G

SD-03 Product Data

Fire Alarm and Mass Notification Control Unit (FMCU); G

Local Operating Console (LOC); G

Amplifiers; G

Tone Generators; G

Digitalized voice generators; G

LCD Annunciator; G

Manual Stations; G

Smoke Detectors; G

Duct Smoke Detectors; G

Addressable Interface Devices; G

Addressable Control Modules; G

Notification Appliances; G

Batteries; G

Battery Chargers; G

Supplemental Notification Appliance Circuit Panels; G

Surge Protective Devices; G

Alarm Wiring; G

Back Boxes and Conduit; G

Terminal Cabinets; G

Automatic Fire Alarm Transmitters (including housing); G

Radio Transmitter and Interface Panels; G

Mass Notification Transceiver; G

Electromagnetic Door Holders; G

Environmental Enclosures or Guards; G

Document Storage Cabinet; G

SD-06 Test Reports

Test Procedures; G

SD-07 Certificates

Verification of Compliant Installation; G

Request for Government Final Test; G

SD-10 Operation and Maintenance Data

Operation and Maintenance (O&M) Instructions; G

Instruction of Government Employees; G

SD-11 Closeout Submittals

As-Built Drawings

Spare Parts

1.6 SYSTEM OPERATION

Fire alarm system/mass notification system including textual display sign control panel(s), components requiring power, except for the FMCU(s) power supply, must operate on 24 volts DC unless noted otherwise in this section.

The interior fire alarm and mass notification system must be a complete, supervised, noncoded, analog/addressable fire alarm and mass notification system conforming to NFPA 72, UL 864, and UL 2572. Systems meeting UL 2017 only are not acceptable. The system must be activated into the alarm mode by actuation of an alarm initiating device. The system must remain in the alarm mode until the initiating device is reset and the control unit is reset and restored to normal. The system may be placed in the alarm mode by local microphones, LOC, FMCU, or remotely from authorized locations/users.

1.6.1 Alarm Initiating Devices and Notification Appliances (Visual, Voice, Textual)

a. Connect alarm initiating devices to initiating device circuits (IDC)

Class "B", or to signaling line circuits (SLC) Class "A" with isolation modules installed between no more than 20 devices and installed in accordance with NFPA 72.

b. Connect notification appliances to notification appliance circuits (NAC) Class "A".

1.6.2 Functions and Operating Features

The system must provide the following functions and operating features:

a. Power, annunciation, supervision, and control for the system. Addressable systems must be microcomputer (microprocessor or microcontroller) based with a minimum word size of eight bits with sufficient memory to perform as specified.

b. Visual alarm notification appliances must be synchronized as required by NFPA 72.

c. Electrical supervision of the primary power (AC) supply, presence of the battery, battery voltage, and placement of system modules within the control unit.

d. An audible and visual trouble signal to activate upon a single break or open condition, or ground fault. The trouble signal must also operate upon loss of primary power (AC) supply, absence of a battery supply, low battery voltage, or removal of alarm or supervisory control unit modules. After the system returns to normal operating conditions, the trouble signal must again sound until the trouble is acknowledged. A smoke detector in the process of being verified for the actual presence of smoke must not initiate a trouble condition.

e. A trouble signal silence feature that must silence the audible trouble signal, without affecting the visual indicator.

f. Program capability via switches in a locked portion of the FMCU to bypass the automatic notification appliance circuits, fire reporting system, air handler shutdown, elevator recall, door release, door unlocking features. Operation of this programmed action must indicate on the FMCU display as a supervisory or trouble condition. Notification appliance bypass must be selectable by floor.

g. Alarm functions must override trouble or supervisory functions. Supervisory functions must override trouble functions.

h. The system must be capable of being programmed from the control unit keyboard. Programmed information must be stored in non-volatile memory.

i. The system must be capable of operating, supervising, and/or monitoring non-addressable alarm and supervisory devices.

j. There must be no limit, other than maximum system capacity, as to the number of addressable devices that may be in alarm simultaneously.

k. Where the fire alarm/mass notification system is responsible for initiating an action in another emergency control device or system, such as HVAC, elevator recall, releasing service, the addressable fire alarm relay must be located in the vicinity of the emergency control

device.

l. An alarm signal must automatically initiate the following functions:

(1) Transmission of an alarm signal to NC ANG Base Receiving Station(s). The base receiving station(s) software, hardware, graphics and programming shall be upgraded as part of this project.

(2) Visual indication of the device operated on the FMCU, Video Display unit (VDU), and on the graphic annunciator.

(3) Actuation of alarm notification appliances.

(4) Recording of the event electronically in the history log of the FMCU.

(5) Release of power to electric locks (delayed egress locks) on doors that are part of the means of egress.

m. A supervisory signal must automatically initiate the following functions:

(1) Visual indication of the device operated on the FMCU, Video Display unit (VDU), and on the graphic annunciator.

(2) Transmission of a supervisory signal to a NC ANG Base Receiving Station(s). The base receiving station(s) software, hardware, graphics and programming shall be upgraded as part of this project.

(3) Operation of a duct smoke detector must shut down the appropriate air handler in accordance with NFPA 90A in addition to other requirements of this paragraph and as allowed by NFPA 72.

(4) Recording of the event electronically in the history log of the FMCU.

n. A trouble condition must automatically initiate the following functions:

(1) Visual indication of the device operated on the FMCU, Video Display unit (VDU), and on the graphic annunciator.

(2) Transmission of a trouble signal to NC ANG Base Receiving Station(s). The base receiving station(s) software, hardware, graphics and programming shall be upgraded as part of this project.

(3) Recording of the event electronically in the history log of the FMCU.

o. System control equipment must be programmed to provide a 60-minute to 180-minute delay in transmission of trouble signals resulting from primary power failure.

p. Activation of a LOC pushbutton must activate the audible and visual alarms in the facility. The audible message must be the one associated with the pushbutton activated.

1.7 TECHNICAL DATA AND SITE-SPECIFIC SOFTWARE

Technical data and site-specific software (meaning technical data that relates to computer software) that are specifically identified in this project, and may be required in other specifications, must be delivered, strictly in accordance with the CONTRACT CLAUSES. The fire alarm system manufacturer must submit written confirmation of this contract provision as "Fire Alarm System Site-Specific Software Acknowledgement". Identify data delivered by reference to the specification paragraph against which it is furnished. Data to be submitted must include complete system, equipment, and software descriptions. Descriptions must show how the equipment will operate as a system to meet the performance requirements of this contract. A copy of the site-specific software for the fire alarm system shall be turned over the Government on-site at beneficial occupancy. The site-specific software data package must also include the following:

a. Items identified in NFPA 72, titled "Site-Specific Software".

b. Identification of programmable portions of the system equipment and capabilities.

c. Description of system revision and expansion capabilities and methods of implementation detailing both equipment and software requirements.

d. Provision of operational software data on all modes of programmable portions for fire alarm and mass notification.

e. Description of Fire Alarm and Mass Notification Control Unit equipment operation.

f. Description of auxiliary and remote equipment operations.

g. Library of application software.

h. Operation and maintenance manuals.

1.8 QUALITY ASSURANCE

1.8.1 Submittal Documents

All Submittal Documents shall be performed by a fire alarm designer that is a Registered FPE. A stamp of the Registered FPE shall be affixed to all documents.

1.8.1.1 Preconstruction Submittals

Within 36 days of contract award but not less than 14 days prior to commencing any work on site, the Contractor must submit the following for review and approval. SD-02, SD-03 and SD-05 submittals received prior to the review and approval of the qualifications of the fire alarm subcontractor and QFPE must be returned disapproved without review. All resultant delays must be the sole responsibility of the Contractor.

1.8.1.2 Shop Drawings

Shop drawings must not be smaller than the Contract Drawings. Drawings must comply with the requirements of NFPA 72 and NFPA 170. Minimum scale for floor plans must be 1/8"=1'.

1.8.1.3 Nameplates

Nameplate illustrations and data to obtain approval by the Contracting Officer before installation.

1.8.1.4 Wiring Diagrams

6 copies of point-to-point wiring diagrams showing the points of connection and terminals used for electrical field connections in the system, including interconnections between the equipment or systems that are supervised or controlled by the system. Diagrams must show connections from field devices to the FMCU and remote FMCU, initiating circuits, switches, relays and terminals, including pathway diagrams between the control unit and shared communications equipment within the protected premises. Point-to-point wiring diagrams must be job specific and must not indicate connections or circuits not being utilized. Provide complete riser diagrams indicating the wiring sequence of all devices and their connections to the control equipment. Include a color-code schedule for the wiring.

1.8.1.5 System Layout

Six copies of plan view drawing showing device locations, terminal cabinet locations, junction boxes, other related equipment, conduit routing, conduit sizes, wire counts, conduit fill calculations, wire color-coding, circuit identification in each conduit, and circuit layouts for all floors. Indicate candela rating of each visual notification appliance. Indicate the wattage of each speaker. Clearly identify the locations of isolation modules. Indicate the addresses of all devices, modules, relays, and similar. Show/identify all acoustically similar spaces. Indicate if the environment for the FMCU is within its environmental listing (e.g. temperature/humidity).

Provide a complete description of the system operation in matrix format similar to the "Typical Input/Output Matrix" included in the Annex of NFPA 72.

1.8.1.6 Notification Appliances

Calculations and supporting data on each circuit to indicate that there is at least 25 percent spare capacity for notification appliances. Annotate data for each circuit on the drawings.

1.8.1.7 Initiating Devices

Calculations and supporting data on each circuit to indicate that there is at least 25 percent spare capacity for initiating devices. Annotate data for each circuit on the drawings.

1.8.1.8 Amplifiers

Calculations and supporting data to indicate that amplifiers have sufficient capacity to simultaneously drive all notification speakers at tapped settings plus 25 percent spare capacity. Annotate data for each circuit on the drawings.

1.8.1.9 Battery Power

Calculations and supporting data as required in paragraph Battery Power

Calculations for alarm, alert, and supervisory power requirements. Calculations including ampere-hour requirements for each system component and each control unit component, and the battery recharging period, must be included on the drawings.

1.8.1.10 Voltage Drop Calculations

Voltage drop calculations for each notification circuit indicating that sufficient voltage is available for proper operation of the system and all components, at a minimum rated voltage of the system operating on batteries. Include the calculations on the system layout drawings.

1.8.1.11 Product Data

Six copies of annotated descriptive data to show the specific model, type, and size of each item. Catalog cuts must also indicate the NRTL listing. The data must be highlighted to show model, size, and options that are intended for consideration. Data must be adequate to demonstrate compliance with all contract requirements. Product data for all equipment must be combined into a single submittal.

Provide an equipment list identifying the type, quantity, make, and model number of each piece of equipment to be provided under this submittal. The equipment list must include the type, quantity, make and model of spare equipment. Types and quantities of equipment submitted must coincide with the types and quantities of equipment used in the battery calculations and those shown on the shop drawings.

1.8.1.12 Operation and Maintenance (O&M) Instructions

Six copies of the Operation and Maintenance Instructions. The O&M Instructions must be prepared in a single volume or in multiple volumes, with each volume indexed, and may be submitted as a Technical Data Package. Manuals must be approved prior to training. The Interior Fire Alarm and Mass Notification System Operation and Maintenance Instructions must include the following:

a. "Manufacturer Data Package five" as specified in Section 01 78 23 OPERATION AND MAINTENANCE DATA.

b. Operating manual outlining step-by-step procedures required for system startup, operation, and shutdown. The manual must include the manufacturer's name, model number, service manual, parts list, and preliminary equipment list complete with description of equipment and their basic operating features.

c. Maintenance manual listing routine maintenance procedures, possible breakdowns and repairs, and troubleshooting guide. The manuals must include conduit layout, equipment layout and simplified wiring, and control diagrams of the system as installed.

d. Complete procedures for system revision and expansion, detailing both equipment and software requirements.

e. Software submitted for this project on electronic storage media utilized.

f. Printouts of configuration settings for all devices.

g. Routine maintenance checklist. The routine maintenance checklist must be arranged in a columnar format. The first column must list all installed devices, the second column must state the maintenance activity or state no maintenance required, the third column must state the frequency of the maintenance activity, and the fourth column provided for additional comments or reference. All data (devices, testing frequencies, and similar) must comply with UFC 3-601-02.

h. A final Equipment List must be submitted with the Operating and Maintenance (O&M) manual.

1.8.1.13 As-Built Drawings

The drawings must show the system as installed, including deviations from both the project drawings and the approved shop drawings. These drawings must be submitted within two weeks after the final Government test of the system. At least one set of the as-built (marked-up) drawings must be provided at the time of, or prior to the final Government test.

1.8.2 Qualifications

1.8.2.1 Fire Alarm System Designer

The fire alarm system designer must be certified as a Level III (minimum) Technician by National Institute for Certification in Engineering Technologies (NICET) in the Fire Alarm Systems subfield of Fire Protection Engineering Technology or meet the qualifications for a QFPE.

1.8.2.2 Supervisor

A NICET Level III or IV fire alarm technician must supervise the installation of the fire alarm/mass notification system.A fire alarm technician with a minimum of eight years of experience must supervise the installation of the fire alarm/mass notification system. The fire alarm technicians supervising the installation of equipment must be factory trained in the installation, adjustment, testing, and operation of the equipment specified herein and on the drawings.

1.8.2.3 Technician

Fire alarm technicians with a minimum of four years of experience must be utilized to install and terminate fire alarm/mass notification devices, cabinets and control units. The fire alarm technicians installing the equipment must be factory trained in the installation, adjustment, testing, and operation of the equipment specified herein and on the drawings, and must be thoroughly experienced in the installation of air sampling detection systems.

1.8.2.4 Installer

Fire alarm installer with a minimum of two years of experience utilized to assist in the installation of fire alarm/mass notification devices, cabinets and control units or NICET Level II technician to assist in the installation of fire alarm/mass notification devices, cabinets, and panels. A licensed electrician must be allowed to install wire, cable, conduit and backboxes for the fire alarm system/mass notification system. The fire alarm installer must be factory trained in the installation, adjustment, testing, and operation of the equipment specified herein and on the drawings.

1.8.2.5 Test Technician

Fire alarm technicians with a minimum of eight years of experience and NICET Level III or IV utilized in testing and certification of the installation of the fire alarm/mass notification devices, cabinets and control units. The fire alarm technicians testing the equipment must be factory trained in the installation, adjustment, testing, and operation of the equipment installed as part of this project.

1.8.2.6 Manufacturer

Company specializing in manufacturing products specified in this section with minimum four years documented experience, and with service facilities within 100 miles of the project. Components must be of current design and must be in regular and recurrent production at the time of installation. Provide design, materials, and devices for a protected premises fire alarm system, complete, conforming to NFPA 72, except as specified herein.

1.8.2.7 Manufacturer's Representative

An individual directly employed or licensed by the manufacturer(s)of the products specified in this section with minimum four years documented experience, and assigned to the service facilities within 100 miles of the project. equipment must be factory trained in the installation, adjustment, testing, and operation of the equipment installed as part of this project. Provide design, installation, and testing services for the protected premises fire alarm system, conforming to NFPA 72, except as specified herein.

1.8.3 Regulatory Requirements

Equipment and material must be listed or approved. Listed or approved, as used in this section, means listed, labeled or approved by a Nationally Recognized Testing Laboratory (NRTL) such as UL Fire Prot Dir or FM APP GUIDE. The omission of these terms under the description of any item of equipment described must not be construed as waiving this requirement. All listings or approvals by testing laboratories must be from an existing ANSI or UL published standard. The recommended practices stated in the manufacturer's literature or documentation must be considered as mandatory requirements.

1.9 DELIVERY, STORAGE, AND HANDLING

Protect equipment delivered and placed in storage from the weather, humidity, and temperature variation, dirt and dust, and other contaminants.

1.10 MAINTENANCE

1.10.1 Spare Parts

Furnish the following spare parts in the manufacturers original unopened containers:

a. Five complete sets of system keys.

b. Two of each type of fuse required by the system.

c. One manual stations.

d. One of each type of detector installed.

e. One of each type of detector base and head installed.

f. Two of each type of audible and visual alarm device installed.

g. One textual visual notification appliance.

h. One of each type of addressable monitor module installed.

i. One of each type of addressable control module installed.

1.10.2 Special Tools

Software, connecting cables and proprietary equipment, necessary for the maintenance, testing, and reprogramming of the equipment must be furnished to the Contracting Officer, prior to the instruction of Government employees.

PART 2 PRODUCTS

2.1 GENERAL PRODUCT REQUIREMENT

All fire alarm and mass notification equipment must be listed for use under the applicable reference standards. Interfacing of UL 864 or similar approved industry listing with Mass Notification equipment listed to UL 2572 must be done in a laboratory listed configuration, if the software programming features cannot provide a listed interface control.

2.2 MATERIALS AND EQUIPMENT

2.2.1 Standard Products

Provide materials, equipment, and devices that have been tested by a nationally recognized testing laboratory and listed for fire protection service when so required by NFPA 72 or this specification. Select material from one manufacturer, where possible, and not a combination of manufacturers, for any particular classification of materials. Material and equipment must be the standard products of a manufacturer regularly engaged in the manufacture of the products for at least 2 years prior to bid opening.

2.2.2 Nameplates

Major components of equipment must have the manufacturer's name, address, type or style, model or serial number, catalog number, date of installation, installing Contractor's name and address, and the contract number provided on a new name plate permanently affixed to the item or equipment. Major components include, but are not limited to, the following:

a. FMCU

Nameplates must be etched metal or plastic, permanently attached by screws to control units or adjacent walls.

2.2.3 Keys

Keys and locks for equipment, control units and devices must be identical. Master all keys and locks to a single key as required by the Installation Fire Department. Keys must be CAT 60.

2.2.4 Instructions

Provide a typeset printed or typewritten instruction card mounted behind a Lexan plastic or glass cover in a stainless steel or aluminum frame. Install the instruction on the interior of the FMCU. The card must show those steps to be taken by an operator when a signal is received as well as the functional operation of the system under all conditions, normal, alarm, supervisory, and trouble. The instructions must also include procedures for operating live voice microphones. The instructions and their mounting location must be approved by the Contracting Officer before being posted.

2.3 FIRE ALARM AND MASS NOTIFICATION CONTROL UNIT

Provide a complete fire alarm and mass notification control unit (FMCU) fully enclosed in a lockable steel cabinet as specified herein. Operations required for testing or for normal care, maintenance, and use of the system must be performed from the front of the enclosure. If more than a single unit is required at a location to form a complete control unit, the unit cabinets must match exactly. If more than a single unit is required, and is located in the lobby/entrance, notify the Contracting Officer's Designated Representative (COR), prior to installing the equipment. The system must be capable of defining any module as an alarm module and report alarm trouble, loss of polling, or as a supervisory module, and reporting supervisory short, supervisory open or loss of polling such as waterflow switches, valve supervisory switches, fire pump monitoring, independent smoke detection systems, relays for output function actuation.

a. Each control unit must provide power, supervision, control, and logic for the entire system, utilizing solid state, modular components, internally mounted and arranged for easy access. Each control unit must be suitable for operation on a 120 volt, 60 hertz, normal building power supply. Provide each control unit with supervisory functions for power failure, internal component placement, and operation.

b. Visual indication of alarm, supervisory, or trouble initiation on the FMCU must be by liquid crystal display or similar means with a minimum of 80 characters. The mass notification control unit must have the capability of temporarily deactivate the fire alarm audible notification appliances while delivering voice messages.

c. Provide secure operator console for initiating recorded messages, strobes and displays; and for delivering live voice messages. Provide capacity for at least eight prerecorded messages. Provide the ability to automatically repeat prerecorded messages. Provide a secure microphone for delivering live messages. Provide adequate discrete outputs to temporarily deactivate fire alarm audible notification, initiate/synchronize strobes and initiate textual visual notification appliances. Provide a complete set of self-diagnostics for controller and appliance network. Provide local diagnostic information display and local diagnostic information and system event log file.

d. The fire alarm control unit shall report each point-to-point addressable device individually with distinct descriptions to the base receiving station and to the redundant receiving systems. A control unit that is only capable of providing generalized, non-addressable signal reporting must be pre-approved by the Contracting Officer during the pre-bid process.

2.3.1 Cabinet

Install control unit components in cabinets large enough to accommodate all components and also to allow ample gutter space for interconnection of control units as well as field wiring. The cabinet must be a sturdy steel housing, complete with back box, hinged steel door with cylinder lock, and surface mounting provisions. The enclosure must be identified by an engraved phenolic resin nameplate. Lettering on the nameplate must say "Fire Alarm and Mass Notification control unit" and must not be less than 1-inch high. Provide prominent rigid plastic or metal identification plates for lamps, circuits, meters, fuses, and switches.

2.3.2 Silencing Switches

2.3.2.1 Alarm Silencing Switch

Provide an alarm silencing switch at the FMCU that must silence the audible and visual notification appliances. Subsequent activation of initiating devices must cause the notification appliances to re-activate.

2.3.2.2 Supervisory/Trouble Silencing Switch

Provide supervisory and trouble silencing switch(es) that must silence the audible trouble and supervisory signal(s), but not extinguish the visual indicator. This switch must be overridden upon activation of a subsequent supervisory or trouble condition. Audible trouble indication must resound automatically every 24 hours after the silencing feature has been operated if the supervisory or trouble condition still exists.

2.3.3 Non-Interfering

Power and supervise each circuit such that a signal from one device does not prevent the receipt of signals from any other device. Initiating devices must be manually reset by switch from the FMCU after the initiating device or devices have been restored to normal.

2.3.4 Audible Notification System

The Audible Notification System must comply with the requirements of NFPA 72 for Emergency Voice/Alarm Communications System requirements, except as specified herein. The system must be a one-way, multi-channel voice notification system incorporating user selectability of a minimum eight distinct sounds for tone signaling, and the incorporation of a voice module for delivery of recorded messages. Audible appliances must produce a three-pulse temporal pattern for three cycles followed by a voice message that is repeated until the control unit is reset or silenced. Automatic messages must be broadcast through speakers throughout the building/facility but not in stairs or elevator cabs. A live voice message must override the automatic audible output through use of a microphone input at the control unit or the LOC.

a. When using the microphone, live messages must be broadcast throughout a selected floor or floors, or all call. The system must be capable of operating all speakers at the same time.

b. The microprocessor must actively interrogate circuitry, field wiring, and digital coding necessary for the immediate and accurate rebroadcasting of the stored voice data into the appropriate amplifier input. Loss of operating power, supervisory power, or any other malfunction that could render the digitalized voice module inoperative must automatically cause the three-pulse temporal pattern to take over all functions assigned to the failed unit in the event an alarm is activated.

2.3.4.1 Outputs and Operational Modules

All outputs and operational modules must be fully supervised with on-board diagnostics and trouble reporting circuits. Provide form "C" contacts for system alarm and trouble conditions. Provide circuits for operation of auxiliary appliance during trouble conditions. During a Mass Notification event, the control unit must not generate nor cause any trouble alarms to be generated with the Fire Alarm system.

2.3.4.2 Mass Notification

a. The system must have the capability of utilizing an LOC with redundant controls of the FMCU. Notification Appliance Circuits (NAC) must be provided for the activation of strobe appliances. Audio output must be selectable for line level. A hand-held microphone must be provided and, upon activation, must take priority over any tone signal, recorded message or PA microphone operation in progress, while maintaining the strobe NAC circuit activation.

b. The Mass Notification functions must override the manual or automatic fire alarm notification. Other fire alarm functions including transmission of a signal(s) to the fire department must remain operational. When a mass notification announcement is disengaged and a fire alarm condition still exists, the audible and visual notification appliances must resume activation for alarm conditions. The fire alarm message must be of lower priority that all other messages (except any "test" messages) and must not override any other messages.

c. Messages must be recorded professionally utilizing standard industry methods, in a professional female voice. Message and tone volumes must both be at the same decibel level. Messages recorded from the system microphone must not be accepted. A 1000 Hz tone (as required by NFPA 72) must precede messages and be similar to the following unless Installation or Facility specific messages are required:

(1) "May I have your attention please. May I have your attention please. A fire emergency has been reported in the building. Please leave the building by the nearest exit." (Provide a 2 second pause.) "May I have your attention please, (repeat the message).

(2) "Attention, Your attention please. This is a Tornado Warning. Please seek shelter in an interior room and stay out of hallways and away from exterior windows". Repeat 3 times.

(3) "Attention, Your attention please. The National Weather Service has issued a Severe Thunderstorm Warning for our area." Repeat 3 times.

(4) "Attention, attention. A bomb threat alert has been issued for this building. All personnel are to evacuate immediately using the nearest exit. Further instructions will be issued outside the building by emergency response teams." Repeat 3 times.

(5) "Attention, Your attention please. A Hazardous Material danger exists in the area. Remain in the building. Please keep all doors and windows closed. Please wait for further instructions from Emergency services." Repeat 3 times.

(6) "May I have your attention, please. All clear. The emergency has ended." Repeat 3 times.

(7) "Attention, Your attention please. This is a Test of the emergency audio system."

(8) "Attention, Your attention please. An Active Shooter danger exists in the area. Remain in the building and proceed to a room that all doors and windows can be locked. Lie flat on the floor so no one is visible from outside the room. Call 9-1-1 to report your location. Do not respond to any voice commands until you can verify they are from Emergency services." Repeat 3 times.

2.3.4.3 Installation-Wide Control

If an installation-wide control system for mass notification exists on the Base, the autonomous control unit must communicate with the central control unit of the Installation-wide system. The autonomous control unit must receive commands/messages from the central control unit and provide status information.

2.3.5 Memory

Provide each control unit with non-volatile memory and logic for all functions. The use of long life batteries, capacitors, or other age-dependent devices must not be considered as equal to non-volatile processors, PROMS, or EPROMS.

2.3.6 Field Programmability

Provide control units and control units that are fully field programmable for both input and output of control, initiation, notification, supervisory, and trouble functions. The system program configuration must be menu driven. System changes must be password protected. Any proprietary equipment and proprietary software needed by qualified technicians to implement future changes to the fire alarm system must be provided as part of this contract.

2.3.7 Input/Output Modifications

The FMCU must contain features that allow the bypassing of input devices from the system or the modification of system outputs. These control features must consist of a control unit mounted keypad. Any bypass or modification to the system must indicate a trouble condition on the FMCU.

2.3.8 Resetting

Provide the necessary controls to prevent the resetting of any alarm, supervisory, or trouble signal while the alarm, supervisory or trouble condition on the system still exists.

2.3.9 Walk Test

The FMCU must have a walk test feature. When using this feature, operation of initiating devices must result in limited system outputs, so that the notification appliances operate for only a few seconds and the event is indicated in the history log and on the system printer, but no other outputs occur.

2.3.10 History Logging

The control unit must have the ability to store a minimum of 400 events in a log. These events must be stored in a battery-protected memory and must remain in the memory until the memory is downloaded or cleared manually. Resetting of the control unit must not clear the memory.

2.3.11 Manual Access

An operator at the control unit, having a proper access level, must have the capability to manually access the following information for each initiating device.

a. Primary status.

b. Device type.

c. Present average value.

d. Present sensitivity selected.

e. Detector range (normal, dirty).

2.4 LOCAL OPERATING CONSOLES (LOC)

2.4.1 General

The LOC must consist of a remote microphone station incorporating a push-to-talk (PTT) hand-held microphone and system status indicators. The LOC must have the capability of being utilized to activate prerecorded messages. The unit must incorporate microphone override of any tone generation or recorded messages. The unit must be fully supervised from the FMCU. The housing for the LOC must not be lockable.

2.5 AMPLIFIERS, PREAMPLIFIERS, TONE GENERATORS

Any amplifiers, preamplifiers, tone generators, digitalized voice generators, and other hardware necessary for a complete, operational, textual audible circuit conforming to NFPA 72 must be housed in a remote FMCU, terminal cabinet, or in the FMCU. Individual amplifiers must be 100 watts maximum.

2.5.1 Operation

The system must automatically operate and control all building speakers

and must operate only when the microphone is used to deliver live messages.

2.5.2 Construction

Amplifiers must utilize computer grade solid state components and must be provided with output protection devices sufficient to protect the amplifier against any transient up to 10 times the highest rated voltage in the system.

2.5.3 Inputs

Equip each system with separate inputs for the tone generator, digitalized voice driver and control unit mounted microphone Public Address Paging Function . Microphone inputs must be of the low impedance, balanced line type. Both microphone and tone generator input must be operational on any amplifier.

2.5.4 Tone Generator

The tone generator must produce a three-pulse temporal pattern and must be constantly repeated until interrupted by either the digitalized voice message, the microphone input, or the alarm silence mode as specified. The tone generator must be single channel with an automatic backup generator per channel such that failure of the primary tone generator causes the backup generator to automatically take over the functions of the failed unit and also causes transfer of the common trouble relay. The tone generator must be provided with securely attached labels to identify the component as a tone generator and to identify the specific tone it produces.

2.5.5 Protection Circuits

Each amplifier must be constantly supervised for any condition that could render the amplifier inoperable at its maximum output. Failure of any component must cause illumination of a visual "amplifier trouble" indicator on the control unit, appropriate logging of the condition in the history log, and other actions for trouble conditions as specified.

2.6 REMOTE ANNUNCIATOR

2.6.1 LCD Annunciator

Provide a flush mounted annunciator that includes an LCD display. The display must indicate the device in trouble/alarm or any supervisory device. Display the device name, address, and actual building location. The remote annunciator must duplicate functions of the FMCU for message display, fire alarm, supervisory alarm, and trouble conditions, visual and audible notification, and system reset functions. Remote annunciator must require the use of a key for accessing the reset, control and other functions.

A building floor plan must be provided and mounted (behind Plexiglass or similar protective material) at the annunciator location. The floor plan must indicate all rooms by name and number including the locations of stairs and elevators. The floor plan must show all devices and their programmed address to facilitate identification of their physical location from the LCD display information.

2.7 MANUAL STATIONS

Provide metal or plastic, semi-flush mounted, double-action, addressable manual stations, that are not subject to operation by jarring or vibration. Stations must be equipped with screw terminals for each conductor. Stations that require the replacement of any portion of the device after activation are not permitted. Stations must be finished in red with molded raised lettering operating instructions of contrasting color. The use of a key must be required to reset the station.

2.8 ISOLATION MODULES

Provide isolation modules to subdivide each signaling line circuit into groups not more than 20 addressable devices between adjacent isolation modules. For this project, provide no less than two isolation modules and place them so addressable devices are evenly isolated by quantity. As an example, if there are 30 addressable devices for the project, the two isolation modules would be placed near the 10th devices and 20th device on the SLC loop.

2.9 SMOKE DETECTORS

2.9.1 Spot Type Detectors

Provide addressable photoelectric smoke detectors as follows:

a. Provide analog/addressable photoelectric smoke detectors utilizing the photoelectric light scattering principle for operation in accordance with UL 268. Smoke detectors must be listed for use with the FMCU.

b. Provide self-restoring type detectors that do not require any readjustment after actuation at the FMCU to restore them to normal operation. The detector must have a visual indicator to show actuation.

c. Vibration must have no effect on the detector's operation. Protect the detection chamber with a fine mesh metallic screen that prevents the entrance of insects or airborne materials. The screen must not inhibit the movement of smoke particles into the chamber.

d. Provide twist lock bases with screw terminals for each conductor. The detectors must maintain contact with their bases without the use of springs.

e. The detector address must identify the particular unit, its location within the system, and its sensitivity setting. Detectors must be of the low voltage type rated for use on a 24 VDC system.

f. Provide indicating lights for all concealed detectors and initiating devices.

2.9.2 Duct Smoke Detectors

Duct-mounted addressable photoelectric smoke detectors must consist of a smoke detector, as specified in paragraph Spot Type Detectors, mounted in a special housing fitted with duct sampling tubes. Detector circuitry must be mounted in a metallic or plastic enclosure exterior to the duct. Detectors must be listed for operation over the complete range of air velocities, temperature and humidity expected at the detector when the

air-handling system is operating. Detectors must be powered from the FMCU.

a. Sampling tubes must run the full width of the duct. The duct detector package must conform to the requirements of NFPA 90A, UL 268A, and must be listed for use in air-handling systems. The control functions, operation, reset, and bypass must be controlled from the FMCU.

b. Lights to indicate the operation and alarm condition must be visible and accessible with the unit installed and the cover in place. Remote indicators must be provided where required by NFPA 72 for every duct mounted smoke detector. Remote indicators as well as the affected fan units must be properly identified in etched plastic placards. Indicators shall have integral testing stations.

c. Detectors must provide for control of auxiliary contacts that provide control, interlock, and shutdown functions specified in Section 23 09 00INSTRUMENTATION AND CONTROL FOR HVAC. Auxiliary contacts provide for this function must be located within 3 feet of the controlled circuit or appliance. The auxiliary contacts must be supplied by the fire alarm system manufacturer to ensure complete system compatibility.

2.10 ADDRESSABLE INTERFACE DEVICES

The initiating device being monitored must be configured as a Class "A" initiating device circuits. The module must be listed as compatible with the control unit. The module must provide address setting means compatible with the control unit's SLC supervision and store an internal identifying code. Monitor module must contain an integral LED that flashes each time the monitor module is polled and is visible through the device cover plate. Pull stations with a monitor module in a common backbox are not required to have an LED. Modules must be listed for the environmental conditions in which they will be installed.

2.11 ADDRESSABLE CONTROL MODULES

The control module must be capable of operating as a relay (dry contact form C) for interfacing the control unit with other systems, and to control door holders. The module must be listed as compatible with the control unit. The indicating device or the external load being controlled must be configured as Class B notification appliance circuits. The system must be capable of supervising, audible, visual and dry contact circuits. The control module must have both an input and output address. The supervision must detect a short on the supervised circuit and must prevent power from being applied to the circuit. The control module must provide address setting means compatible with the control unit's SLC supervision and store an internal identifying code. The control module must contain an integral LED that flashes each time the control module is polled and is visible through the device cover plate. Control Modules must be listed for the environmental conditions in which they will be installed.

2.12 NOTIFICATION APPLIANCES

2.12.1 Audible Notification Appliances

Audible appliances must conform to the applicable requirements of UL 464. Appliances must be connected into notification appliance circuits. Surface mounted audible appliances must be painted red. Recessed audible

appliances must be installed with a grill that is painted red with a factory finish to match the surface to which it is mounted.

2.12.1.1 Speakers

a. Speakers must conform to the applicable requirements of UL 1480. Speakers must have six different sound output levels and operate with audio line input levels of 70.7 VRMs and 25 VRMs, by means of selectable tap settings. Interior speaker tap settings must include taps of 1/4, 1/2, 1, and 2 watt, at a minimum. Exterior speakers must also be multi-tapped with no more than 15 watt maximum setting. Speakers must incorporate a high efficiency speaker for maximum output at minimum power across a frequency range of 400 Hz to 4,000 Hz, and must have a sealed back construction. Speakers must be capable of installation on standard 4-inch square electrical boxes. Where speakers and strobes are provided in the same location, they may be combined into a single wall mounted unit. All inputs must be polarized for compatibility with standard reverse polarity supervision of circuit wiring via the FMCU.

b. Provide speaker mounting plates constructed of cold rolled steel having a minimum thickness of 16 gage or molded high impact plastic and equipped with mounting holes and other openings as needed for a complete installation. Fabrication marks and holes must be ground and finished to provide a smooth and neat appearance for each plate. Each plate must be primed and painted.

c. Speakers must utilize screw terminals for termination of all field wiring.

d. Speakers that are located within 20 feet of the LOC or any other FA/MNS microphone shall be controlled so that when the microphone key is pressed-to-talk, then those adjacent speakers are de-activated until the microphone key button is depressed-to-stop-talking.

2.12.2 Visual Notification Appliances

Visual notification appliances must conform to the applicable requirements of UL 1638, UL 1971 and conform to the Architectural Barriers Act (ABA). Visual Notification Appliances must have clear high intensity optic lens, xenon flash tubes, or light emitting diode (LED) and be marked "Alert" in letters of contrasting color. The light pattern must be dispersed so that it is visible above and below the strobe and from a 90 degree angle on both sides of the strobe. Strobe flash rate must be 1 flash per second and a minimum of 30 candela based on the UL 1971 test. Strobe must be semi-flush mounted.

2.13 ELECTRIC POWER

2.13.1 Primary Power

Power must be 120 VAC 60 Hz service for the FMCU from the AC service to the building in accordance with NFPA 72.

2.14 SECONDARY POWER SUPPLY

Provide for system operation in the event of primary power source failure. Transfer from normal to auxiliary (secondary) power or restoration from auxiliary to normal power must be automatic and must not

cause transmission of a false alarm.

2.14.1 Batteries

Provide sealed, maintenance-free, lead-calcium batteries as the source for emergency power to the FMCU. Batteries must contain suspended electrolyte. The battery system must be maintained in a fully charged condition by means of a solid state battery charger. Provide an automatic transfer switch to transfer the load to the batteries in the event of the failure of primary power.

2.14.1.1 Capacity

Battery size must be the greater of the following two capacities. This capacity applies to every control unit associated with this system, including supplemental notification appliance circuit panels, fire alarm transmitters, and Base-wide mass notification transceivers. When determining the required capacity under alarm condition, visual notification appliances must include both textual and non-textual type appliances.

a. Sufficient capacity to operate the fire alarm system under supervisory and trouble conditions, including audible trouble signal devices for 48 hours and audible and visual signal devices under alarm conditions for an additional 15 minutes.

b. Sufficient capacity to operate the mass notification for 60 minutes after loss of AC power.

2.14.1.2 Battery Power Calculations

a. Verify that battery capacity exceeds supervisory and alarm power requirements for the criteria noted in the paragraph "Capacity" above.

   (1) Substantiate the battery calculations for alarm and supervisory power requirements. Include ampere-hour requirements for each system component and each control unit component, and compliance with UL 864.

   (2) Provide complete battery calculations for both the alarm and supervisory power requirements. Submit ampere-hour requirements for each system component with the calculations.

   (3) Provide voltage drop calculations to indicate that sufficient voltage is available for proper operation of the system and all components. Calculations must be performed using the minimum rated voltage of each component.

b. For battery calculations assume a starting voltage of 24 VDC for starting the calculations to size the batteries. Calculate the required Amp-Hours for the specified standby time, and then calculate the required Amp-Hours for the specified alarm time. Using 20.4 VDC as starting voltage, perform a voltage drop calculation for circuits containing device and/or appliances remote from the power sources.

2.14.2 Battery Chargers

Provide a solid state, fully automatic, variable charging rate battery charger. The charger must be capable of providing 120 percent of the

connected system load and must maintain the batteries at full charge. In the event the batteries are fully discharged (20.4 Volts dc), the charger must recharge the batteries back to 95 percent of full charge within 48 hours after a single discharge cycle as described in paragraph CAPACITY above. Provide pilot light to indicate when batteries are manually placed on a high rate of charge as part of the unit assembly if a high rate switch is provided.

2.15 SURGE PROTECTIVE DEVICES

Surge protective devices must be provided to suppress all voltage transients which might damage fire alarm control unit components. Systems having circuits located outdoors, communications equipment must be protected against surges induced on any signaling line circuit. Cables and conductors, that serve as communications links, must have surge protection circuits installed at each end. The surge protective device must wire in series to the power supply of the protected equipment with screw terminations. Line voltage surge arrestor must be installed directly adjacent to the power panel where the FMCU breaker is located.

a. Surge protective devices for nominal 120 VAC must be UL 1449 listed with a maximum 500 volt suppression level and have a maximum response time of 5 nanoseconds. The surge protective device must also meet IEEE C62.41.1 and IEEE C62.41.2 category B tests for surge capacity. The surge protective device must feature multi-stage construction and be provided with a long-life indicator lamp (either light emitting diode or neon) which extinguishes upon failure of protected components. Any unit fusing must be externally accessible.

b. Surge protective devices for nominal 24 VAC, fire alarm telephone dialer, or ethernet connection must be UL 497B listed, meet IEEE C62.41.1 and have a maximum response time of 1-nanosecond. The surge protective device must feature multi-stage construction and be self-resetting. The surge protective device must be a base and plug style. The base assembly must have screw terminals for fire alarm wiring. The base assembly must accept "plug-in" surge protective module.

c. All surge protective devices (SPD) must be the standard product of a single manufacturer and be equal or better than the following:

(1) Install surge protection recommended by FACU and NAC power supply manufacturer(s). Install on all 120 volt system wiring for all fire alarm panels, located outside of the fire alarm cabinet.

(2) For 120 VAC nominal line voltage: UL 1449 and UL 1283 listed, series connected 120 VAC, 20A rated, surge protective device in a NEMA 4x enclosure. Minimum 50,000 amp surge current rating with EMI/RFI filtering and a dry contact circuit for remote monitoring of surge protection status.

(3) For 24-volt nominal line voltage: UL 497B listed, series connected low voltage, 24-volt, 5A rated, loop circuit protector, base and replaceable module.

2.16 WIRING

Provide wiring materials under this section as specified herein.

2.16.1 Alarm Wiring

IDC and SLC wiring must be solid copper cable in accordance with the manufacturer's requirements. Copper signaling line circuits and initiating device circuit field wiring must be No. 14 AWG size conductors at a minimum. Visual notification appliance circuit conductors, that contain audible alarm appliances, must be copper No. 14 AWG size conductors at a minimum. Speaker circuits must be copper No. 16 AWG size twisted and shielded conductors at a minimum. Wiring for textual notification appliance circuits must be in accordance with manufacturer's requirements but must be supervised by the FMCU. Wire size must be sufficient to prevent voltage drop problems. Circuits operating at 24 VDC must not operate at less than the listed voltages for the detectors and/or appliances. Power wiring, operating at 120 VAC minimum, must be a minimum No. 12 AWG solid copper having similar insulation. Acceptable power-limited cables are FPL, FPLR or FPLP as appropriate with red colored covering. Nonpower-limited cables must comply with NFPA 70. All fire alarm wiring shall be in a conduit system. SLC wiring shall be provided in its own conduit network separate from IDC and NAC circuits.

2.17 INTERFACE TO THE BASE-WIDE MASS NOTIFICATION NETWORK

2.17.1 Radio

The mass notification transceiver must be bi-direction and meet all the requirements of paragraph, RADIO TRANSMITTER AND INTERFACE PANELS as specified in this specification section. The transceiver utilized in the mass notification system must be capable of the following:

a. Communication with the central control/monitoring system to provide supervision of communication link and status changes are reported by automatic and manual poll/reply/acknowledge routines.

b. All monitored points/status changes are transmitted immediately and at programmed intervals until acknowledged by the central control/monitoring system.

c. Each transceiver must transmits a unique identity code as part of all messages; the code is set by the user at the transceiver.

2.17.2 Secure Radio System

2.17.2.1 Communications Network

The communications network provides two-way signals between central control units and autonomous control units (in individual building systems), and should include redundant (primary and backup) communication links. The system must incorporate technology to prevent easy interruption of the radio traffic for MNS alerting.

2.17.2.2 Radio Frequency Communications

Use of radio frequency-type communications systems must comply with National Telecommunications and Information Administration (NTIA) requirements. The systems must be designed to minimize the potential for interference, jamming, eavesdropping, and spoofing.

2.17.2.3 Licensed Radio Frequency Systems

An approved DD Form 1494 for the system is required prior to operation.

2.18 AUTOMATIC FIRE ALARM TRANSMITTERS

2.18.1 Radio Transmitter and Interface Panels

Transmitters must be compatible with proprietary supervising station receiving equipment. Each radio alarm transmitter must be the manufacturer's recognized commercial product, completely assembled, wired, factory tested, and delivered ready for installation and operation. Transmitters must be provided in accordance with applicable portions of NFPA 72, Federal Communications Commission (FCC) 47 CFR 90 and Federal Communications Commission (FCC) 47 CFR 15. Transmitter electronics module must be contained within the physical housing as an integral, removable assembly. The proprietary supervising station receiving equipment is Monaco D21 and the transmitter must be fully compatible with the existing equipment. At the contractor's option, and if listed, the transmitter may be housed in the same control unit as the FMCU. The transmitter must be narrowband radio, with FCC certification for narrowband operation and meets the requirements of the NTIA (National Telecommunications and Information Administration) Manual of Regulations and Procedures for Federal Frequency Management.

2.18.1.1 Operation

Operate each transmitter from 120-volt ac power. In the event of 120-volt ac power loss, the transmitter must automatically switch to battery operation. Switchover must be accomplished with no interruption of protective service, and must automatically transmit a trouble message. Upon restoration of ac power, transfer back to normal ac power supply must also be automatic.

2.18.1.2 Battery Power

Transmitter standby battery capacity must provide sufficient power to operate the transmitter in a normal standby status for a minimum of 72 hours and be capable of transmitting alarms during that period.

2.18.1.3 Transmitter Housing

Use NEMA Type 1 for housing. The housing must contain a lock that is keyed identical to radio alarm transmitter housings on the Installation. Radio alarm transmitter housing must be factory painted with a suitable priming coat and not less than two coats of a hard, durable weatherproof enamel.

2.18.1.4 Antenna

Antenna must be omnidirectional, coaxial, halfwave dipole antennas for radio alarm transmitters with a driving point impedance to match transmitter output. The antenna and antenna mounts must be corrosion resistant and designed to withstand wind velocities of 100 mph. Do not mount antennas to any portion of the building roofing system. Protect the antenna from physical damage.

2.18.2 Signals to Be Transmitted to the Base Receiving Station

The following signals must be sent to the base receiving station in a point-by-point addressable arrangement:

a. Sprinkler waterflow

b. Manual pull stations

c. Smoke detectors

d. Duct smoke detectors

e. Sprinkler valve supervision

f. Knox Box tamper supervision

2.19 SYSTEM MONITORING

2.19.1 Valves

Each valve affecting the proper operation of a fire protection system, including automatic sprinkler control valves, sprinkler service entrance valve, isolating valves for pressure type waterflow or supervision switches, and valves at backflow preventers, whether supplied under this contract or existing, must be electrically monitored to ensure its proper position. Provide each tamper switch with a separate address.

2.19.2 Room Low Temperature Supervisory Switch

Provide listed supervisory air temperature switch for the fire pump and sprinkler riser rooms. Switch must cause a supervisory signal to be transmitted to the FMCU whenever the temperature in the room drops to below 40 degrees F. Device must reset when temperature rises above 40 degrees F.

2.19.3 Electromagnetic Door Holders

Electromagnetic holding devices must operate on 24 VDC, and require not more than 3 watts of power to develop 25 psi of holding force. Under normal conditions, the magnets must attract and hold the doors open. Operation must be fail safe with no moving parts. Electromagnetic door hold-open devices must not be required to be held open during building power failure. The device must be listed based on UL 228 tests.

2.19.4 Knox Box Tamper Supervisory Switch

Each Knox box is equipped with a supervisory switch at the entrances. These supervisory contacts must be electronically monitored by the fire alarm system to ensure notification of tampering of the Knox box to a monitored location. Provide a separate address for each monitored device.

2.20 ENVIRONMENTAL ENCLOSURES OR GUARDS

Environmental enclosures must be provided to permit fire alarm/mass notification components to be used in areas that exceed the environmental limits of the listing. The enclosure must be listed for the device or appliance as either a manufactured part number or as a listed compatible accessory for the component is currently listed. Guards required to deter

mechanical damage must be either a listed manufactured part or a listed accessory for the category of the initiating device or notification appliance.

2.21 TEXTUAL DISPLAY SIGNS

Textual displays signs must be LED Scrolling and must not exceed 400 mm long by 150 mm high by 75 mm deep. The text display must spell out the word 'EVACUATE' or 'ANNOUNCEMENT'. The design of the text display must be such that it cannot be read when not illuminated. Basis of design is Monaco MAAP-X Text Display (PN# 710-075-01) or equivalent.

PART 3 EXECUTION

3.1 VERIFYING ACTUAL FIELD CONDITIONS

Before commencing work, examine all adjoining work on which the contractor's work is in any way dependent for perfect workmanship according to the intent of this specification section, and report to the Contracting Officer's Representative any condition which prevents performance of first class work. No "waiver of responsibility" for incomplete, inadequate or defective adjoining work will be considered unless notice has been filed before submittal of a proposal.

3.2 INSTALLATION

3.2.1 Fire Alarm and Mass Notification Control Unit (FMCU)

Locate the FMCU where indicated on the drawings. Recess the enclosure with the top of the cabinet 6 feet above the finished floor or center the cabinet at 5 feet, whichever is lower. Ensure MNS microphone and message buttons are within 44" AFF to satisfy ADA requirements. Conductor terminations must be labeled and a drawing containing conductors, their labels, their circuits, and their interconnection must be permanently mounted in the FMCU. Locate the document storage cabinet adjacent to the FMCU unless the Contracting Officer directs otherwise.

3.2.2 Battery Cabinets

When batteries will not fit in the FMCU, locate battery cabinets below or adjacent to the FMCU. Battery cabinets must be installed at an accessible location when standing at floor level. Battery cabinets must not be installed lower than 12 inches above finished floor, measured to the bottom of the cabinet, nor higher than 36 inches above the floor, measured to the top of the cabinet. Installing batteries above drop ceilings or in inaccessible locations is prohibited. Battery cabinets must be large enough to accommodate batteries and also to allow ample gutter space for interconnection of control units as well as field wiring. The cabinet must be provided in a sturdy steel housing, complete with back box, hinged steel door with cylinder lock, and surface mounting provisions. The cabinet must be identified by an engraved phenolic resin nameplate. Lettering on the nameplate must indicate the control unit(s) the batteries power and must not be less than 1-inch high.

3.2.3 Manual Stations

Locate manual stations as required by NFPA 72 and as indicated on the drawings. Mount stations so they are located no farther than 5 feet from the exit door they serve, measured horizontally. Manual stations must be

mounted at 44 inches measured to the operating handle.

3.2.4 Notification Appliances

a. Locate notification appliance devices where indicated and to meet the intelligibility requirements. Where more than two visual notification appliances are located in the same room or corridor or field of view, provide synchronized operation. Devices must use screw terminals for all field wiring. Audible and visual notification appliances mounted in acoustical ceiling tiles must be centered in the tiles plus or minus 2 inches. The Contractor is responsible for meeting all intelligibility requirements of this Contract and UFC Standards. If additional speakers are required to achieve intelligibility, they shall be provided, installed and tested at no additional cost to the Government.

b. Audible and visual notification appliances mounted on the exterior of the building, within unconditioned spaces, or in the vicinity of showers must be listed weatherproof appliances installed on weatherproof backboxes.

c. Speakers must not be located in close proximity to the FMCU or LOC so as to cause feedback when the microphone is in use.

3.2.5 Smoke Detectors

Locate detectors as required by NFPA 72 and their listing on a 4-inch mounting box. Install heat detectors not less than 4 inches from a side wall to the near edge. Heat detectors located on the wall must have the top of the detector at least 4 inches below the ceiling, but not more than 12 inches below the ceiling. Smoke detectors are permitted to be on the wall no lower than 12 inches from the ceiling with no minimum distance from the ceiling. Install smoke detectors no closer than 3 feet from air handling supply diffusers. Detectors installed in acoustical ceiling tiles must be centered in the tiles plus or minus 2 inches. All concealed detectors shall have indicating lamps in an accessible location that indicates the location of the concealed device.

3.2.6 LCD REMOTE Annunciator

Locate the LCD annunciator as shown on the drawings. Mount the annunciator, with the top 6 feet above the finished floor or center the annunciator at 5 feet, whichever is lower.

3.2.7 Electromagnetic Door Holder Release

Doors must be held open at a minimum of 90 degrees so as not to impede egress from the space. Mount the armature portion on the door and have an adjusting screw for seating the angle of the contact plate. Wall-mount the electromagnetic release, with a total horizontal projection not exceeding 4 inches. Ensure all doors release to close upon first stage (pre-discharge) alarm. Electrical supervision of wiring external of control unit for magnetic door holding circuits is not required.

3.2.8 Local Operating Console (LOC)

Locate the LOC(s) as required by NFPA 72 and as indicated. Mount the console so that the top message button and microphone is no higher than 4 feet above the floor and the bottom (lowest) message button and microphone

is at least 3 feet above the finished floor.

3.3 SYSTEM FIELD WIRING

3.3.1 Wiring within Cabinets, Enclosures, and Boxes

Provide wiring installed in a neat and workmanlike manner and installed parallel with or at right angles to the sides and back of any box, enclosure, or cabinet. Conductors that are terminated, spliced, or otherwise interrupted in any enclosure, cabinet, mounting, or junction box must be connected to screw-type terminal blocks. Mark each terminal in accordance with the wiring diagrams of the system. The use of wire nuts or similar devices is prohibited. Wiring to conform with NFPA 70. T-tapping is prohibited.

Indicate the following in the wiring diagrams:

a. Point-to-point wiring diagrams showing the points of connection and terminals used for electrical field connections in the system, including interconnections between the equipment or systems that are supervised or controlled by the system. Diagrams must show connections from field devices to the FMCU and remote fire alarm/mass notification control units, initiating circuits, switches, relays and terminals.

b. Complete riser diagrams indicating the wiring sequence of devices and their connections to the control equipment. Include a color code schedule for the wiring. Include floor plans showing the locations of devices and equipment.

3.3.2 Terminal Cabinets

Provide a terminal cabinet at the base of any circuit riser, on each floor at each riser, and where indicated on the drawings. Terminal size must be appropriate for the size of the wiring to be connected. Conductor terminations must be labeled and a drawing containing conductors, their labels, their circuits, and their interconnection must be permanently mounted in the terminal cabinet. Minimum size is 8 inches by 8 inches. Only screw-type terminals are permitted. Provide an identification label, that displays "FIRE ALARM TERMINAL CABINET" with 2-inch lettering, on the front of the terminal cabinet.

3.3.3 Alarm Wiring

a. Voltages must not be mixed in any junction box, housing or device, except those containing power supplies and control relays.

b. Utilize shielded wiring where recommended by the manufacturer. For shielded wiring, ground the shield at only one point, in or adjacent to the FMCU.

c. Pigtail or T-tap connections to signal line circuits, initiating device circuits, supervisory alarm circuits, and notification appliance circuits are prohibited.

d. Color coding is required for circuits and must be maintained throughout the circuit. Conductors used for the same functions must be similarly color coded. Conform wiring to NFPA 70.

e. Pull all conductors splice free. The use of wire nuts, crimped connectors, or twisting of conductors is prohibited.

f. All SLC circuits shall be run in a separate conduit from the notification appliance circuits. The SLC circuit's outgoing and return conductors are to be separated by 1 foot in the vertical orientation and 4 feet in the horizontal orientation.

3.3.4 Back Boxes and Conduit

In addition to the requirements of Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM, provide all wiring in rigid metal conduit or intermediate metal conduit unless specifically indicated otherwise. Minimum conduit size must be 3/4-inch in diameter. Do not use electrical non-metallic tubing (ENT) or flexible non-metallic tubing and associated fittings.

a. Galvanized rigid steel (GRS) conduit must be utilized where exposed to weather, where subject to physical damage, and where exposed on exterior of buildings. Intermediate metal conduit (IMC) may be used in lieu of GRS as allowed by NFPA 70.

b. Electrical metallic tubing (EMT) is permitted above suspended ceilings or exposed where not subject to physical damage. Do not use EMT underground, encased in concrete, mortar, or grout, in hazardous locations, where exposed to physical damage, outdoors or in fire pump rooms. Use die-cast compression connectors.

c. For rigid metallic conduit (RMC), only threaded type fitting are permitted for wet or damp locations.

d. Flexible metal conduit is permitted for initiating device circuits 6 feet in length or less. Flexible metal conduit is prohibited for notification appliance circuits and signaling line circuits. Use liquid tight flexible metal conduit in damp and wet locations.

e. Schedule 40 (minimum) polyvinyl chloride (PVC) is permitted where conduit is routed underground or underground below floor slabs. Convert non-metallic conduit, other than PVC Schedule 40 or 80, to plastic-coated rigid, or IMC, steel conduit before turning up through floor slab.

f. Exterior wall penetrations must be weathertight. Conduit must be sealed to prevent the infiltration of moisture.

g. All conduits shall be minimum size of 3/4 inches.

h. All conduits shall be installed as concealed in the walls and ceilings unless referenced as ceiling mounted device.

3.3.5 Conductor Terminations

Labeling of conductors at terminal blocks in terminal cabinets, FMCU and the LOC must be provided at each conductor connection. Each conductor or cable must have a shrink-wrap label to provide a unique and specific designation. Each terminal cabinet, FMCU, and remote FMCU must contain a laminated drawing that indicates each conductor, its label, circuit, and terminal. The laminated drawing must be neat, using 12 point lettering minimum size, and mounted within each cabinet, control unit, or unit so that it does not interfere with the wiring or terminals. Maintain

existing color code scheme where connecting to existing equipment.

3.4 FIRESTOPPING

Provide firestopping for holes at conduit penetrations through floor slabs, fire-rated walls, partitions with fire-rated doors, corridor walls, and vertical service shafts in accordance with Section 07 84 00 FIRESTOPPING.

3.5 PAINTING

a. In unfinished areas (including areas above drop ceilings), paint all exposed electrical conduit (serving fire alarm equipment), fire alarm conduit, surface metal raceway, junction boxes and covers red. In lieu of painting conduit, the contractor may utilize red conduit with a factory applied finish.

b. In finished areas, paint exposed electrical conduit (serving fire alarm equipment), fire alarm conduit, surface metal raceways, junction boxes, and electrical boxes to match adjacent finishes. The inside cover of the junction box must be identified as "Fire Alarm" and the conduit must have painted red bands 3/4-inch wide at 10-foot centers and at each side of a floor, wall, or ceiling penetration.

c. Painting must comply with Section 09 90 00 PAINTS AND COATINGS.

3.6 FIELD QUALITY CONTROL

3.6.1 Test Procedures

Submit detailed test procedures, prepared and signed by the NICET Level III or IV Fire Alarm Technician, and the representative of the installing company, and reviewed by the QFPE 60 days prior to performing system tests. Detailed test procedures must list all components of the installed system such as initiating devices and circuits, notification appliances and circuits, signaling line devices and circuits, control devices/equipment, batteries, transmitting and receiving equipment, power sources/supply, annunciators, special hazard equipment, emergency communication equipment, interface equipment, and surge protective devices. Test procedures must include sequence of testing, time estimate for each test, and sample test data forms. The test data forms must be in a check-off format (pass/fail with space to add applicable test data; similar to the forms in NFPA 72 and NFPA 4.) The test procedures and accompanying test data forms must be used for the pre-Government testing and the Government testing. The test data forms must record the test results and must:

a. Identify the NFPA Class of all Initiating Device Circuits (IDC), and Notification Appliance Circuits (NAC), Voice Notification System Circuits (NAC Audio), and Signaling Line Circuits (SLC).

b. Identify each test required by NFPA 72 Test Methods and required test herein to be performed on each component, and describe how these tests must be performed.

c. Identify each component and circuit as to type, location within the facility, and unique identity within the installed system. Provide necessary floor plan sheets showing each component location, test location, and alphanumeric identity.

d. Identify all test equipment and personnel required to perform each test (including equipment necessary for smoke detector testing. The use of magnets is not permitted.

e. Provide space to identify the date and time of each test. Provide space to identify the names and signatures of the individuals conducting and witnessing each test.

3.6.2 Pre-Government Testing

3.6.2.1 Verification of Compliant Installation

Conduct inspections and tests to ensure that devices and circuits are functioning properly. Tests must meet the requirements of paragraph entitled "Minimum System Tests" as required by NFPA 72. The contractor and an authorized representative from each supplier of equipment must be in attendance at the pre-Government testing to make necessary adjustments. After inspection and testing is complete, provide a signed Verification of Compliant Installation letter by the QFPE that the installation is complete, compliant with the specification and fully operable. The letter must include the names and titles of the witnesses to the pre-Government tests. Provide all completion documentation as required by NFPA 72 including all referenced annex sections and the test reports noted below.

a. NFPA 72 Record of Completion.

b. NFPA 72 Record of Inspection and Testing.

c. Fire Alarm and Emergency Communication System Inspection and Testing Form.

d. Audibility test results with marked-up test floor plans.

e. Intelligibility test results with marked-up floor plans.

f. Documentation that all tests identified in the paragraph "Minimum System Tests" are complete.

3.6.2.2 Request for Government Final Test

When the verification of compliant installation has been completed, submit a formal request for Government final test to the Contracting Officer's Representative (COR). Government final testing will not be scheduled until the DFPE has received copies of the request for Government final testing and Verification of Compliant Installation letter with all required reports. Government final testing will not be performed until after the connections to the installation-wide fire reporting system and the installation-wide mass notification system have been completed and tested to confirm communications are fully functional. Submit request for test at least 15 calendar days prior to the requested test date.

3.6.3 Correction of Deficiencies

If equipment was found to be defective or non-compliant with contract requirements, perform corrective actions and repeat the tests. Tests must be conducted and repeated if necessary until the system has been demonstrated to comply with all contract requirements.

3.6.4 Government Final Tests

The tests must be performed in accordance with the approved test procedures in the presence of the DFPE. Furnish instruments and personnel required for the tests. The contractor shall provide all time necessary for the manufacturer's technical representative to fully test, program, and troubleshoot the entire system until system testing has been approved by the Contracting Officer's Representative (COR). The following must be provided at the job site for Government Final Testing:

a. The manufacturer's technical representative.

b. The contractor's Qualified Fire Protection Engineer (QFPE).

c. Marked-up red line drawings of the system as actually installed.

d. Loop resistance test results.

e. Complete program printout including input/output addresses.

f. Copy of pre-Government Test Certificate, test procedures and completed test data forms.

g. Audibility test results with marked-up floor plans.

h. Intelligibility test results with marked-up floor plans.

Government Final Tests will be witnessed by the Contracting Officer's Representative (COR) and Qualified Fire Protection Engineer (QFPE). At this time, any and all required tests noted in the paragraph "Minimum System Tests" must be repeated at their discretion.

3.7 MINIMUM SYSTEM TESTS

3.7.1 System Tests

Test the system in accordance with the procedures outlined in NFPA 72. The required tests are as follows:

a. Loop Resistance Tests: Measure and record the resistance of each circuit with each pair of conductors in the circuit short-circuited at the farthest point from the circuit origin. The tests must be witnessed by the Contracting Officer and test results recorded for use at the final Government test.

b. Verify the absence of unwanted voltages between circuit conductors and ground. The tests must be accomplished at the pre-Government test with results available at the final system test.

c. Verify that the control unit is in the normal condition as detailed in the manufacturer's O&M manual.

d. Test each initiating device and notification appliance and circuit for proper operation and response at the control unit. Smoke detectors must be tested in accordance with manufacturer's recommended calibrated test method. Use of magnets is prohibited. Testing of duct smoke detectors must comply with the requirements of NFPA 72 except disconnect at least 20 percent of devices. If there is a failure at

these devices, then supervision must be tested at each device.

f. Test the system for specified functions in accordance with the contract drawings and specifications and the manufacturer's O&M manual.

g. Test both primary power and secondary power. Verify, by test, the secondary power system is capable of operating the system for the time period and in the manner specified.

h. Determine that the system is operable under trouble conditions as specified.

i. Visually inspect wiring.

j. Test the battery charger and batteries.

k. Verify that software control and data files have been entered or programmed into the FMCU. Hard copy records of the software must be provided to the Contracting Officer.

l. Verify that red-line drawings are accurate.

m. Measure the current in circuits to ensure there is the calculated spare capacity for the circuits.

n. Measure voltage readings for circuits to ensure that voltage drop is not excessive.

o. Disconnect the verification feature for smoke detectors during tests to minimize the amount of smoke needed to activate the sensor. Testing of smoke detectors must be conducted using real smoke or the use of canned smoke which is permitted.

p. Measure the voltage drop at the most remote appliance (based on wire length) on each notification appliance circuit.

q. Verify the documentation cabinet is installed and contains all as-built shop drawings, product data sheets, design calculations, site-specific software data package, and all documentation required by paragraph titled "Test Reports".

3.7.2 Audibility Tests

Sound pressure levels from audible notification appliances must be a minimum of 15 dBa over ambient with a maximum of 110 dBa in any occupiable area. The provisions for audible notification (audibility and intelligibility) must be met with doors, fire shutters, movable partitions, and similar devices closed.

3.7.3 Intelligibility Tests

Intelligibility testing of the System must be accomplished in accordance with NFPA 72 for Voice Evacuation Systems, and ASA S3.2. Following are the specific requirements for intelligibility tests:

a. Intelligibility Requirements: Verify intelligibility by measurement after installation.

b. Ensure that a CIS value greater than the required minimum value is

provided in each area where building occupants typically could be found. The minimum required value for CIS is .7. Rounding of values is permitted.

c. Areas of the building provided with hard wall and ceiling surfaces (such as metal or concrete) that are found to cause excessive sound reflections may be permitted to have a CIS score less than the minimum required value if approved by the DFPE, and if building occupants in these areas can determine that a voice signal is being broadcast and they must walk no more than 33 feet to find a location with at least the minimum required CIS value within the same area.

d. Areas of the building where occupants are not expected to be normally present are permitted to have a CIS score less than the minimum required value if personnel can determine that a voice signal is being broadcast and they must walk no more than 50 feet to a location with at least the minimum required CIS value within the same area.

e. Take measurements near the head level applicable for most personnel in the space under normal conditions (e.g., standing, sitting, sleeping, as appropriate).

f. The distance the occupant must walk to the location meeting the minimum required CIS value must be measured on the floor or other walking surface as follows:

(1) Along the centerline of the natural path of travel, starting from any point subject to occupancy with less than the minimum required CIS value.

(2) Curving around any corners or obstructions, with a 12 inches clearance there from.

(3) Terminating directly below the location where the minimum required CIS value has been obtained.

Use commercially available test instrumentation to measure intelligibility as specified by NFPA 72 as applicable. Use the mean value of at least three readings to compute the intelligibility score at each test location.

3.8 SYSTEM ACCEPTANCE

Following acceptance of the system, as-built drawings and O&M manuals must be delivered to the Contracting Officer for review and acceptance. The drawings must show the system as installed, including deviations from both the project drawings and the approved shop drawings. These drawings must be submitted within two weeks after the final Government test of the system. At least one set of as-built (marked-up) drawings must be provided at the time of, or prior to the Final Government Test.

a. The drawings must be prepared electronically and sized no less than the contract drawings. Furnish one set of electronic storage media containing software back-up and CAD based drawings in latest version of AutoCAD, DXF and portable document formats of as-built drawings and schematics.

b. Include complete wiring diagrams showing connections between devices and equipment, both factory and field wired.

c. Include a riser diagram and drawings showing the as-built location of devices and equipment.

d. Provide Operation and Maintenance (O&M) Instructions.

3.9 INSTRUCTION OF GOVERNMENT EMPLOYEES

3.9.1 Instructor

Provide the services of an instructor, who has received specific training from the manufacturer for the training of other persons regarding the operation, inspection, testing, and maintenance of the system provided. The instructor must train the Government employees designated by the Contracting Officer, in the care, adjustment, maintenance, and operation of the fire alarm system. The instructor must be thoroughly familiar with all parts of this installation. The instructor must be trained in operating theory as well as in practical O&M work. Submit the instructor's information and qualifications including the training history.

3.9.2 Required Instruction Time

Provide 8 hours of instruction after final acceptance of the system. The instruction must be given during regular working hours on such dates and times selected by the Contracting Officer. The instruction may be divided into two or more periods at the discretion of the Contracting Officer. The training must allow for rescheduling for unforeseen maintenance and/or fire department responses.

3.9.2.1 Technical Training

Equipment manufacturer or a factory representative must provide 3 days of on site technical training. Training must allow for classroom instruction as well as individual hands on programming, troubleshooting and diagnostics exercises. Factory training must occur within 6 months of system acceptance.

3.9.3 Technical Training Manual

Provide, in manual format, lesson plans, operating instructions, maintenance procedures, and training data for the training courses. The operations training must familiarize designated government personnel with proper operation of the installed system. The maintenance training course must provide the designated government personnel adequate knowledge required to diagnose, repair, maintain, and expand functions inherent to the system.

3.10 EXTRA MATERIALS

3.10.1 Repair Service/Replacement Parts

Repair services and replacement parts for the system must be available for a period of 10 years after the date of final acceptance of this work by the Contracting Officer. During the warranty period, the service technician must be on-site within 24 hours after notification. All repairs must be completed within 24 hours of arrival on-site.

During the warranty period, the installing fire alarm contractor is responsible for conducting all required testing and maintenance in accordance with the requirements and recommended practices of NFPA 72 and

the system manufacturer. Installing fire alarm contractor is NOT responsible for any damage resulting from abuse, misuse, or neglect of equipment by the end user.

3.10.2 Spare Parts

Spare parts furnished must be directly interchangeable with the corresponding components of the installed system. Spare parts must be suitably packaged and identified by nameplate, tagging, or stamping. Spare parts must be delivered to the Contracting Officer at the time of the Government testing and must be accompanied by an inventory list.

In the bid, provide additional speakers at an amount of 15 percent more than shown on the plans. Include the extra costs of conduit, wire, installation, pretesting and final testing for these extra speakers and the relocation of installed speakers as required. If speakers are left over after the CIS scores are met for the entire facility, turn equipment over to Contracting Officer. . In addition one of each: smoke detector with base, pull station, duct detector with remote test, monitor module, mini module, relay module, control module, Text display, isolation module.

3.10.3 Document Storage Cabinet

Upon completion of the project, but prior to project close-out, place in the document storage cabinet copies of the following record documentation:

a. As-built shop drawings

b. Product data sheets

c. Design calculations

d. Site-specific software data package

e. All documentation required by SD-06.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 31 - EARTHWORK

SECTION 31 00 00

EARTHWORK

PART 1 GENERAL

1.1 PAYMENT PROCEDURES
1.2 CRITERIA FOR BIDDING
1.2.1 Geotechnical Data
1.3 REFERENCES
1.4 DEFINITIONS
1.4.1 Satisfactory Materials
1.4.2 Unsatisfactory Materials
1.4.3 Cohesionless and Cohesive Materials
1.4.4 Degree of Compaction
1.4.5 Topsoil
1.4.6 Hard/Unyielding Materials
1.4.7 Rock
1.4.8 Unstable Material
1.4.9 Select Granular Material
1.4.9.1 General Requirements
1.4.10 Initial Backfill Material
1.4.11 Expansive Soils
1.4.12 Nonfrost Susceptible (NFS) Material
1.5 SYSTEM DESCRIPTION
1.5.1 Classification of Excavation
1.5.2 Dewatering Work Plan
1.6 SUBMITTALS

PART 2 PRODUCTS

2.1 REQUIREMENTS FOR OFFSITE SOILS
2.2 BURIED WARNING AND IDENTIFICATION TAPE
2.2.1 Warning Tape for Metallic Piping
2.2.2 Detectable Warning Tape for Non-Metallic Piping
2.3 DETECTION WIRE FOR NON-METALLIC PIPING
2.4 CAPILLARY WATER BARRIER

PART 3 EXECUTION

3.1 STRIPPING OF TOPSOIL
3.2 GENERAL EXCAVATION
3.2.1 Ditches, Gutters, and Channel Changes
3.2.2 Drainage Structures
3.2.3 Drainage
3.2.4 Dewatering
3.2.5 Trench Excavation Requirements
3.2.5.1 Bottom Preparation
3.2.5.2 Removal of Unyielding Material
3.2.5.3 Removal of Unstable Material

3.2.5.4 Excavation for Appurtenances
3.2.5.5 Jacking, Boring, and Tunneling
3.2.6 Underground Utilities
3.2.7 Structural Excavation
3.3 SELECTION OF BORROW MATERIAL
3.4 OPENING AND DRAINAGE OF EXCAVATION AND BORROW PITS
3.5 SHORING
3.5.1 General Requirements
3.5.2 Geotechnical Engineer
3.6 GRADING AREAS
3.7 FINAL GRADE OF SURFACES TO SUPPORT CONCRETE
3.8 GROUND SURFACE PREPARATION
3.8.1 General Requirements
3.8.2 Frozen Material
3.9 UTILIZATION OF EXCAVATED MATERIALS
3.10 BURIED TAPE AND DETECTION WIRE
3.10.1 Buried Warning and Identification Tape
3.10.2 Buried Detection Wire
3.11 FILLING, BACKFILLING AND COMPACTION
3.11.1 Trench Backfill
3.11.1.1 Replacement of Unyielding Material
3.11.1.2 Replacement of Unstable Material
3.11.1.3 Bedding and Initial Backfill
3.11.1.3.1 Class I
3.11.1.3.2 Class II
3.11.1.3.3 Sand
3.11.1.3.4 Gravel and Crushed Stone
3.11.1.4 Final Backfill
3.11.1.4.1 Roadways, Railroads, and Airfields
3.11.1.4.2 Sidewalks, Turfed or Seeded Areas and Miscellaneous Areas
3.11.2 Backfill for Appurtenances
3.12 SPECIAL REQUIREMENTS
3.12.1 Gas Distribution
3.12.2 Water Lines
3.12.3 Heat Distribution System
3.12.4 Electrical Distribution System
3.13 EMBANKMENTS
3.13.1 Earth Embankments
3.14 SUBGRADE PREPARATION
3.14.1 Proof Rolling
3.14.2 Construction
3.14.3 Compaction
3.14.3.1 Subgrade for Pavements
3.15 FINISHING
3.15.1 Subgrade and Embankments
3.15.2 Capillary Water Barrier
3.15.3 Grading Around Structures
3.16 PLACING TOPSOIL
3.17 TESTING
3.17.1 Fill and Backfill Material Gradation
3.17.2 In-Place Densities
3.17.3 Check Tests on In-Place Densities
3.17.4 Moisture Contents
3.17.5 Optimum Moisture and Laboratory Maximum Density
3.17.6 Tolerance Tests for Subgrades
3.17.7 Displacement of Sewers
3.18 DISPOSITION OF SURPLUS MATERIAL

-- End of Section Table of Contents --

SECTION 31 00 00

EARTHWORK

PART 1 GENERAL

1.1 PAYMENT PROCEDURES

Payment will constitute full compensation for all labor, equipment, tools, supplies, and incidentals necessary to complete the work.

1.2 CRITERIA FOR BIDDING

Base bids on the following criteria:

a. Surface elevations are as indicated.

b. Pipes or other artificial obstructions, except those indicated, will not be encountered.

c. Ground water elevations indicated by the boring log were those existing at the time subsurface investigations were made and do not necessarily represent ground water elevation at the time of construction.

d. Material character is indicated by the boring logs.

e. Hard materials and rock will not be encountered.

f. Over-excavation under slabs on grade and building foundations will be required as described on the structural drawings.

1.2.1 Geotechnical Data

Geotechnical Investigation Report for this Project, prepared by Intertek PSI, dated March 16, 2023, is appended to this section. The opinions expressed in this report are those of a geotechnical engineer and represent interpretations of subsoil conditions, tests, and results of analyses conducted by a geotechnical engineer. Government is not responsible for interpretations or conclusions drawn from the data. Any party using information described in the geotechnical report will make additional test borings and conduct other exploratory operations that may be required to determine the character of subsurface materials that may be encountered.

Because subsurface conditions indicated by the soil borings are a sampling in relation to the entire construction area, and for other reasons, Owner, Architect, Architect's consultants, and the firm reporting the subsurface conditions do not warranty the conditions below the depths of the borings or that the strata logged from the borings are necessarily typical of the entire site. Any party using the information described in the soil borings and geotechnical report accepts full responsibility for its use.

1.3 REFERENCES

The publications listed below form a part of this specification to the

extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN ASSOCIATION OF STATE HIGHWAY AND TRANSPORTATION OFFICIALS (AASHTO)

AASHTO T 180	(2017) Standard Method of Test for Moisture-Density Relations of Soils Using a 4.54-kg (10-lb) Rammer and a 457-mm (18-in.) Drop

AMERICAN WATER WORKS ASSOCIATION (AWWA)

AWWA C600	(2017) Installation of Ductile-Iron Mains and Their Appurtenances

ASTM INTERNATIONAL (ASTM)

ASTM C33/C33M	(2018) Standard Specification for Concrete Aggregates
ASTM C136/C136M	(2019) Standard Test Method for Sieve Analysis of Fine and Coarse Aggregates
ASTM D698	(2012; E 2014; E 2015) Laboratory Compaction Characteristics of Soil Using Standard Effort (12,400 ft-lbf/cu. ft. (600 kN-m/cu. m.))
ASTM D1140	(2017) Standard Test Methods for Determining the Amount of Material Finer than 75-µm (No. 200) Sieve in Soils by Washing
ASTM D1556/D1556M	(2015; E 2016) Standard Test Method for Density and Unit Weight of Soil in Place by Sand-Cone Method
ASTM D1557	(2012; E 2015) Standard Test Methods for Laboratory Compaction Characteristics of Soil Using Modified Effort (56,000 ft-lbf/ft3) (2700 kN-m/m3)
ASTM D2487	(2017; E 2020) Standard Practice for Classification of Soils for Engineering Purposes (Unified Soil Classification System)
ASTM D4318	(2017; E 2018) Standard Test Methods for Liquid Limit, Plastic Limit, and Plasticity Index of Soils
ASTM D4718/D4718M	(2015) Standard Practice for Correction of Unit Weight and Water Content for Soils Containing Oversize Particles
ASTM D6938	(2017a) Standard Test Method for In-Place Density and Water Content of Soil and Soil-Aggregate by Nuclear Methods (Shallow

Depth)

U.S. ARMY CORPS OF ENGINEERS (USACE)

EM 385-1-1	(2014) Safety -- Safety and Health Requirements Manual

U.S. ENVIRONMENTAL PROTECTION AGENCY (EPA)

EPA 600/4-79/020	(1983) Methods for Chemical Analysis of Water and Wastes
EPA SW-846.3-3	(1999, Third Edition, Update III-A) Test Methods for Evaluating Solid Waste: Physical/Chemical Methods

1.4 DEFINITIONS

1.4.1 Satisfactory Materials

Satisfactory materials comprise any materials classified by ASTM D2487 as GW, GP, GM, GP-GM, GW-GM, GC, GP-GC, GM-GC, SW, SM, or SP. Satisfactory materials shall not contain rocks greater than 3 inches in any dimension or have greater than 30 percent retained on the 1/4-inch sieve. Organic content shall be no greater than 3 percent by weight and no roots larger than 1/4-inch in diameter are permitted. Organic material shall not be intentionally mixed into the material. The fill material shall have a Standard Proctor (ASTM D698) maximum dry density of at least 100 pcf. Material shall have a maximum liquid limit of 45 and a plasticity index of 20 or less.

Replacement material under building footings and slabs shall be SM, ML, CL material or lean concrete. Open graded stone and gravel shall not be used as replacement material under footings and slabs as it will allow water to accumulate.

1.4.2 Unsatisfactory Materials

Materials which do not comply with the requirements for satisfactory materials are unsatisfactory. Unsatisfactory materials also include man-made fills; trash; refuse; backfills from previous construction; and material classified as satisfactory which contains root and other organic matter or frozen material. Notify the Contracting Officer when encountering any contaminated materials.

1.4.3 Cohesionless and Cohesive Materials

Cohesionless materials include materials classified in ASTM D2487 as GW, GP, SW, and SP. Cohesive materials include materials classified as GC, SC, ML, CL, MH, and CH. Materials classified as GM and SM will be identified as cohesionless only when the fines are nonplastic. Perform testing, required for classifying materials, in accordance with ASTM D4318, ASTM C136/C136M and ASTM D1140.

1.4.4 Degree of Compaction

Degree of compaction required, except as noted in the second sentence, is expressed as a percentage of the maximum density obtained by the test procedure presented in ASTM D698 abbreviated as a percent of laboratory

maximum density. Since ASTM D1557 applies only to soils that have 30 percent or less by weight of their particles retained on the 3/4 inch sieve, express the degree of compaction for material having more than 30 percent by weight of their particles retained on the 3/4 inch sieve as a percentage of the maximum density in accordance with AASHTO T 180 and corrected with ASTM D4718/D4718M. To maintain the same percentage of coarse material, use the "remove and replace" procedure as described in NOTE 8 of Paragraph 7.2 in AASHTO T 180.

1.4.5 Topsoil

Material suitable for topsoils obtained from offsite areas, excavations, and areas indicated on the drawings is defined as: Natural, friable soil representative of productive, well-drained soils in the area, free of subsoil, stumps, rocks larger than one inch diameter, brush, weeds, toxic substances, and other material detrimental to plant growth. Amend topsoil pH range to obtain a pH of 5.5 to 7.

1.4.6 Hard/Unyielding Materials

Hard/Unyielding materials comprise weathered rock, dense consolidated deposits, or conglomerate materials which are not included in the definition of "rock" with stones greater than 3 inch in any dimension or as defined by the pipe manufacturer, whichever is smaller. These materials usually require the use of heavy excavation equipment, ripper teeth, or jack hammers for removal.

1.4.7 Rock

Solid homogeneous interlocking crystalline material with firmly cemented, laminated, or foliated masses or conglomerate deposits, neither of which can be removed without systematic drilling and blasting, drilling and the use of expansion jacks or feather wedges, or the use of backhoe-mounted pneumatic hole punchers or rock breakers; also large boulders, buried masonry, or concrete other than pavement exceeding 1/2 cubic yard in volume. Removal of hard material will not be considered rock excavation because of intermittent drilling and blasting that is performed merely to increase production.

1.4.8 Unstable Material

Unstable materials are too wet to properly support the utility pipe, conduit, or appurtenant structure.

1.4.9 Select Granular Material

1.4.9.1 General Requirements

Select granular material consist of materials classified as GW, GP, SW, or SP by ASTM D2487 where indicated. The liquid limit of such material must not exceed 35 percent when tested in accordance with ASTM D4318. The plasticity index must not be greater than 12 percent when tested in accordance with ASTM D4318, and not more than 35 percent by weight may be finer than No. 200 sieve when tested in accordance with ASTM D1140.

Granular material shall not be used as replacement material or backfill beneath building slabs or footings (except granular material shall be used to provide a 4-inch thick subgrade immediately beneath the slab on grade).

1.4.10 Initial Backfill Material

Initial backfill consists of select granular material or satisfactory materials free from rocks 3 inches or larger in any dimension or free from rocks of such size as recommended by the pipe manufacturer, whichever is smaller. When the pipe is coated or wrapped for corrosion protection, free the initial backfill material of stones larger than 3 inches in any dimension or as recommended by the pipe manufacturer, whichever is smaller.

1.4.11 Expansive Soils

Expansive soils are defined as soils that have a plasticity index equal to or greater than 10 when tested in accordance with ASTM D4318. Existing soil material on site is generally expansive and shall not be used as structural backfill unless explicitly permitted by the Contracting Officer.

1.4.12 Nonfrost Susceptible (NFS) Material

Nonfrost susceptible material are a uniformly graded washed sand with a maximum particle size of 1 inch and less than 5 percent passing the No. 200 size sieve, and with not more than 3 percent by weight finer than 0.02 mm grain size.

1.5 SYSTEM DESCRIPTION

Subsurface soil boring logs are appended to the SPECIAL CONTRACT REQUIREMENTS. The subsoil investigation report is also appended. These data represent the best subsurface information available; however, variations may exist in the subsurface between boring locations.

1.5.1 Classification of Excavation

No consideration will be given to the nature of the materials, and all excavation will be designated as unclassified excavation.

1.5.2 Dewatering Work Plan

Submit procedures for accomplishing dewatering work.

1.6 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Shoring

Dewatering Work Plan

SD-03 Product Data

Utilization of Excavated Materials

Opening of any Excavation or Borrow Pit

SD-06 Test Reports

Testing

Borrow Site Testing

SD-07 Certificates

Testing

PART 2 PRODUCTS

2.1 REQUIREMENTS FOR OFFSITE SOILS

Test offsite soils brought in for use as backfill for Total Petroleum Hydrocarbons (TPH), Benzene, Toluene, Ethyl Benzene, and Xylene (BTEX) and full Toxicity Characteristic Leaching Procedure (TCLP) including ignitability, corrosivity and reactivity. Provide backfill containing a maximum of 100 parts per million (ppm) of total petroleum hydrocarbons (TPH) and a maximum of 10 ppm of the sum of Benzene, Toluene, Ethyl Benzene, and Xylene (BTEX) and passing the TCPL test. Determine TPH concentrations by using EPA 600/4-79/020 Method 418.1. Determine BTEX concentrations by using EPA SW-846.3-3 Method 5030/8020. Perform TCLP in accordance with EPA SW-846.3-3 Method 1311. Provide Borrow Site Testing for TPH, BTEX and TCLP from a composite sample of material from the borrow site, with at least one test from each borrow site. Do not bring material onsite until tests have been approved by the Contracting Officer.

2.2 BURIED WARNING AND IDENTIFICATION TAPE

Provide polyethylene plastic and metallic core or metallic-faced, acid- and alkali-resistant, polyethylene plastic warning tape manufactured specifically for warning and identification of buried utility lines. Provide tape on rolls, 3 inches minimum width, color coded as specified below for the intended utility with warning and identification imprinted in bold black letters continuously over the entire tape length. Warning and identification to read, "CAUTION, BURIED (intended service) LINE BELOW" or similar wording. Provide permanent color and printing, unaffected by moisture or soil.

Warning Tape Color Codes	
Red	Electric
Yellow	Gas, Oil; Dangerous Materials
Orange	Telephone and Other Communications
Blue	Water Systems
Green	Sewer Systems
White	Steam Systems
Gray	Compressed Air

2.2.1 Warning Tape for Metallic Piping

Provide acid and alkali-resistant polyethylene plastic tape conforming to the width, color, and printing requirements specified above, with a minimum thickness of 0.003 inch and a minimum strength of 1500 psi lengthwise, and 1250 psi crosswise, with a maximum 350 percent elongation.

2.2.2 Detectable Warning Tape for Non-Metallic Piping

Provide polyethylene plastic tape conforming to the width, color, and printing requirements specified above, with a minimum thickness of 0.004 inch, and a minimum strength of 1500 psi lengthwise and 1250 psi crosswise. Manufacture tape with integral wires, foil backing, or other means of enabling detection by a metal detector when tape is buried up to 3 feet deep. Encase metallic element of the tape in a protective jacket or provide with other means of corrosion protection.

2.3 DETECTION WIRE FOR NON-METALLIC PIPING

Insulate a single strand, solid copper detection wire with a minimum of 12 AWG.

2.4 CAPILLARY WATER BARRIER

Provide capillary water barrier of clean, poorly graded crushed rock, crushed gravel, or uncrushed gravel placed beneath a building slab with a vapor barrier to cut off the capillary flow of pore water to the area immediately below. Conform to ASTM C33/C33M for fine aggregate grading with a maximum of 3 percent by weight passing ASTM D1140, No. 200 sieve.

PART 3 EXECUTION

3.1 STRIPPING OF TOPSOIL

Where indicated or directed, strip topsoil to a depth of 5 inches. Spread topsoil on areas already graded and prepared for topsoil, or transported and deposited in stockpiles convenient to areas that are to receive application of the topsoil later, or at locations indicated or specified. Keep topsoil separate from other excavated materials, brush, litter, objectionable weeds, roots, stones larger than 2 inches in diameter, and other materials that would interfere with planting and maintenance operations. Stockpile in locations indicated Remove from the site any surplus of topsoil from excavations and gradings.

3.2 GENERAL EXCAVATION

Perform excavation of every type of material encountered within the limits of the project to the lines, grades, and elevations indicated and as specified. Perform the grading in accordance with the typical sections shown and the tolerances specified in paragraph FINISHING. Transport satisfactory excavated materials and place in fill or embankment within the limits of the work. Excavate unsatisfactory materials encountered within the limits of the work below grade and replace with satisfactory materials as directed. Include such excavated material and the satisfactory material ordered as replacement in excavation. Dispose surplus satisfactory excavated material not required for fill and unsatisfactory excavated material as specified in paragraph DISPOSITION OF SURPLUS MATERIAL. During construction, perform excavation and fill in a manner and sequence that will provide proper drainage at all times.

Excavate material required for fill or embankment in excess of that produced by excavation within the grading limits from the borrow areas indicated or from other approved areas selected by the Contractor as specified.

3.2.1 Ditches, Gutters, and Channel Changes

Finish excavation of ditches, gutters, and channel changes by cutting accurately to the cross sections, grades, and elevations shown on Drawing Sheet No. C-301. Do not excavate ditches and gutters below grades shown. Backfill the excessive open ditch or gutter excavation with satisfactory, thoroughly compacted, material or with suitable stone or cobble to grades shown. Dispose excavated material as shown or as directed, except in no case allow material be deposited a maximum 4 feet from edge of a ditch. Maintain excavations free from detrimental quantities of leaves, brush, sticks, trash, and other debris until final acceptance of the work.

3.2.2 Drainage Structures

Make excavations to the lines, grades, and elevations shown, or as directed. Provide trenches and foundation pits of sufficient size to permit the placement and removal of forms for the full length and width of structure footings and foundations as shown. Clean rock or other hard foundation material of loose debris and cut to a firm, level, stepped, or serrated surface. Remove loose disintegrated rock and thin strata. Do not disturb the bottom of the excavation when concrete or masonry is to be placed in an excavated area. Do not excavate to the final grade level until just before the concrete or masonry is to be placed.

3.2.3 Drainage

Provide for the collection and disposal of surface and subsurface water encountered during construction. Completely drain construction site during periods of construction to keep soil materials sufficiently dry. Construct storm drainage features (ponds/basins) at the earliest stages of site development, and throughout construction grade the construction area to provide positive surface water runoff away from the construction activity and provide temporary ditches, swales, and other drainage features and equipment as required to maintain dry soils. When unsuitable working platforms for equipment operation and unsuitable soil support for subsequent construction features develop, remove unsuitable material and provide new soil material as specified herein. It is the responsibility of the Contractor to assess the soil and ground water conditions presented by the plans and specifications and to employ necessary measures to permit construction to proceed.

3.2.4 Dewatering

Control groundwater flowing toward or into excavations to prevent sloughing of excavation slopes and walls, boils, uplift and heave in the excavation and to eliminate interference with orderly progress of construction. Do not permit French drains, sumps, ditches or trenches within 3 feet of the foundation of any structure, except with specific written approval, and after specific contractual provisions for restoration of the foundation area have been made. Take control measures by the time the excavation reaches the water level in order to maintain the integrity of the in situ material.

3.2.5 Trench Excavation Requirements

Excavate the trench as recommended by the manufacturer of the pipe to be installed. Slope trench walls below the top of the pipe, or make vertical, and of such width as recommended in the manufacturer's printed installation manual. Provide vertical trench walls where no manufacturer's printed installation manual is available. Shore trench walls, cut back to a stable slope, or provide with equivalent means of protection for employees who may be exposed to moving ground or cave in, as determined by the Contractor’s Safety Engineer or other competent person; refer to USACE publication EM 385-1-1. Excavate trench walls which are cut back to at least the angle of repose of the soil. Give special attention to slopes which may be adversely affected by weather or moisture content. Do not exceed the trench width below the pipe top of 24 inches plus pipe outside diameter (O.D.) for pipes of less than 24 inches inside diameter, and do not exceed 36 inches plus pipe outside diameter for sizes larger than 24 inches inside diameter. Where recommended trench widths are exceeded, provide redesign, stronger pipe, or special installation procedures by the Contractor. The Contractor is responsible for the cost of redesign, stronger pipe, or special installation procedures without any additional cost to the Government.

3.2.5.1 Bottom Preparation

Grade the bottoms of trenches accurately to provide uniform bearing and support for the bottom quadrant of each section of the pipe. Excavate bell holes to the necessary size at each joint or coupling to eliminate point bearing. Remove stones of 3 inch or greater in any dimension, or as recommended by the pipe manufacturer, whichever is smaller, to avoid point bearing.

3.2.5.2 Removal of Unyielding Material

Where unyielding material is encountered in the bottom of the trench, remove such material 4 inch below the required grade and replaced with suitable materials as provided in paragraph BACKFILLING AND COMPACTION.

3.2.5.3 Removal of Unstable Material

Where unstable material is encountered in the bottom of the trench, remove such material to the depth directed and replace it to the proper grade with select granular material as provided in paragraph BACKFILLING AND COMPACTION. When removal of unstable material is required due to the Contractor's fault or neglect in performing the work, the Contractor is responsible for excavating the resulting material and replacing it without additional cost to the Government.

3.2.5.4 Excavation for Appurtenances

Provide excavation for manholes, catch-basins, inlets, or similar structures sufficient to leave at least 12 inches clear between the outer structure surfaces and the face of the excavation or support members. of sufficient size to permit the placement and removal of forms for the full length and width of structure footings and foundations as shown. Clean rock or loose debris and cut to a firm surface either level, stepped, or serrated, as shown or as directed. Remove loose disintegrated rock and thin strata. Specify removal of unstable material. When concrete or masonry is to be placed in an excavated area, take special care not to disturb the bottom of the excavation. Do not excavate to the final grade

level until just before the concrete or masonry is to be placed.

3.2.5.5 Jacking, Boring, and Tunneling

Unless otherwise indicated, provide excavation by open cut except that sections of a trench may be jacked, bored, or tunneled if, in the opinion of the Contracting Officer, the pipe, cable, or duct can be safely and properly installed and backfill can be properly compacted in such sections.

3.2.6 Underground Utilities

The Contractor is responsible for movement of construction machinery and equipment over pipes and utilities during construction. Perform work adjacent to non-Government utilities as indicated in accordance with procedures outlined by utility company. Excavation made with power-driven equipment is not permitted within 2 feet of known Government-owned utility or subsurface construction. For work immediately adjacent to or for excavations exposing a utility or other buried obstruction, excavate by hand. Start hand excavation on each side of the indicated obstruction and continue until the obstruction is uncovered or until clearance for the new grade is assured. Support uncovered lines or other existing work affected by the contract excavation until approval for backfill is granted by the Contracting Officer. Report damage to utility lines or subsurface construction immediately to the Contracting Officer.

3.2.7 Structural Excavation

Ensure that footing subgrades have been inspected and approved by the Contracting Officer prior to concrete placement.

3.3 SELECTION OF BORROW MATERIAL

Select borrow material to meet the requirements and conditions of the particular fill or embankment for which it is to be used. Obtain borrow material from the borrow areas. Unless otherwise provided in the contract, the Contractor is responsible for obtaining the right to procure material, pay royalties and other charges involved, and bear the expense of developing the sources, including rights-of-way for hauling from the owners. Borrow material from approved sources on Government-controlled land may be obtained without payment of royalties. Unless specifically provided, do not obtain borrow within the limits of the project site without prior written approval. Consider necessary clearing, grubbing, and satisfactory drainage of borrow pits and the disposal of debris thereon related operations to the borrow excavation.

3.4 OPENING AND DRAINAGE OF EXCAVATION AND BORROW PITS

Notify the Contracting Officer sufficiently in advance of the opening of any excavation or borrow pit or borrow areas to permit elevations and measurements of the undisturbed ground surface to be taken. Except as otherwise permitted, excavate borrow pits and other excavation areas providing adequate drainage. Transport overburden and other spoil material to designated spoil areas or otherwise dispose of as directed. Provide neatly trimmed and drained borrow pits after the excavation is completed. Ensure that excavation of any area, operation of borrow pits, or dumping of spoil material results in minimum detrimental effects on natural environmental conditions.

3.5 SHORING

3.5.1 General Requirements

Submit a Shoring and Sheeting plan for approval 15 days prior to starting work. Submit drawings and calculations, certified by a registered professional engineer, describing the methods for shoring and sheeting of excavations. Finish shoring, including sheet piling, and install as necessary to protect workmen, banks, adjacent paving, structures, and utilities. Remove shoring, bracing, and sheeting as excavations are backfilled, in a manner to prevent caving.

3.5.2 Geotechnical Engineer

Hire a Professional Geotechnical Engineer to provide inspection of excavations and soil/groundwater conditions throughout construction. The Geotechnical Engineer is responsible for performing pre-construction and periodic site visits throughout construction to assess site conditions. The Geotechnical Engineer is responsible for updating the excavation, sheeting and dewatering plans as construction progresses to reflect changing conditions and submit an updated plan if necessary. Submit a monthly written report, informing the Contractor and Contracting Officer of the status of the plan and an accounting of the Contractor's adherence to the plan addressing any present or potential problems. The Contracting Officer is responsible for arranging meetings with the Geotechnical Engineer at any time throughout the contract duration.

3.6 GRADING AREAS

Where indicated, divide work into grading areas within which satisfactory excavated material will be placed in embankments, fills, and required backfills. Do not haul satisfactory material excavated in one grading area to another grading area except when so directed in writing. Place and grade stockpiles of satisfactory and unsatisfactory and wasted materials as specified. Keep stockpiles in a neat and well drained condition, giving due consideration to drainage at all times. Clear, grub, and seal by rubber-tired equipment, the ground surface at stockpile locations; separately stockpile excavated satisfactory and unsatisfactory materials. Protect stockpiles of satisfactory materials from contamination which may destroy the quality and fitness of the stockpiled material. If the Contractor fails to protect the stockpiles, and any material becomes unsatisfactory, remove and replace such material with satisfactory material from approved sources.

3.7 FINAL GRADE OF SURFACES TO SUPPORT CONCRETE

Do not excavate to final grade until just before concrete is to be placed. Only use excavation methods that will leave the foundation rock in a solid and unshattered condition. Roughen the level surfaces, and cut the sloped surfaces, as indicated, into rough steps or benches to provide a satisfactory bond. Protect shales from slaking and all surfaces from erosion resulting from ponding or water flow.

3.8 GROUND SURFACE PREPARATION

3.8.1 General Requirements

Remove and replace unsatisfactory material with satisfactory materials, as directed by the Contracting Officer, in surfaces to receive fill or in

excavated areas. Scarify the surface to a depth of 6 inches before the fill is started. Plow, step, bench, or break up sloped surfaces steeper than 1 vertical to 4 horizontal so that the fill material will bond with the existing material. When subgrades are less than the specified density, break up the ground surface to a minimum depth of 6 inches, pulverizing, and compacting to the specified density. When the subgrade is part fill and part excavation or natural ground, scarify the excavated or natural ground portion to a depth of 12 inches and compact it as specified for the adjacent fill.

3.8.2 Frozen Material

Do not place material on surfaces that are muddy, frozen, or contain frost. Finish compaction by sheepsfoot rollers, pneumatic-tired rollers, steel-wheeled rollers, or other approved equipment well suited to the soil being compacted. Moisten material as necessary to plus or minus 3 percent of optimum moisture .

3.9 UTILIZATION OF EXCAVATED MATERIALS

Use satisfactory material removed from excavations, insofar as practicable, in the construction of fills, embankments, subgrades, shoulders, bedding (as backfill), and for similar purposes. Existing soil is not anticipated to be satisfactory and shall not be used as structural fill unless explicitly approved by the contracting officer. Dispose surplus satisfactory excavated material not required for fill and unsatisfactory excavated material as specified in paragraph DISPOSITION OF SURPLUS MATERIAL. Stockpile and use coarse rock from excavations for constructing slopes or embankments adjacent to streams, or sides and bottoms of channels and for protecting against erosion. Do not dispose excavated material to obstruct the flow of any stream, endanger a partly finished structure, impair the efficiency or appearance of any structure, or be detrimental to the completed work in any way.

3.10 BURIED TAPE AND DETECTION WIRE

3.10.1 Buried Warning and Identification Tape

Provide buried utility lines with utility identification tape. Bury tape 12 inches below finished grade; under pavements and slabs, bury tape 6 inches below top of subgrade.

3.10.2 Buried Detection Wire

Bury detection wire directly above non-metallic piping at a distance not to exceed 12 inches above the top of pipe. Extend the wire continuously and unbroken, from manhole to manhole. Terminate the ends of the wire inside the manholes at each end of the pipe, with a minimum of 3 feet of wire, coiled, remaining accessible in each manhole. Furnish insulated wire over its entire length. Install wires at manholes between the top of the corbel and the frame, and extend up through the chimney seal between the frame and the chimney seal. For force mains, terminate the wire in the valve pit at the pump station end of the pipe.

3.11 FILLING, BACKFILLING AND COMPACTION

Place fill and backfill beneath and adjacent to any and all type of structures, in successive horizontal layers of loose material not more than 8 inches in depth, or in loose layers not more than 4 inches in depth

when using hand-operated compaction equipment. Compact to at least 95 percent of laboratory maximum density per ASTM D698 except as otherwise specified. The upper 12 inches of fill shall be compacted to 98 percent per ASTM D698. Perform compaction in such a manner as to prevent wedging action or eccentric loading upon or against the structure. Moisture condition fill and backfill material to within range of +3 or -3 percent of optimum moisture content at the time of compaction.

Prepare ground surface on which backfill is to be placed and provide compaction requirements for backfill materials in conformance with the applicable portions of paragraphs GROUND SURFACE PREPARATION. Finish compaction by sheepsfoot rollers, pneumatic-tired rollers, steel-wheeled rollers, vibratory compactors, or other approved equipment.

3.11.1 Trench Backfill

Backfill trenches to the grade shown. Backfill the trench to 2 feet above the top of pipe prior to performing the required pressure tests. Leave the joints and couplings uncovered during the pressure test. Do not backfill the trench until all specified tests are performed.

3.11.1.1 Replacement of Unyielding Material

Replace unyielding material removed from the bottom of the trench with select granular material or initial backfill material.

3.11.1.2 Replacement of Unstable Material

Replace unstable material removed from the bottom of the trench or excavation with select granular material placed in layers not exceeding 6 inches loose thickness.

3.11.1.3 Bedding and Initial Backfill

Place initial backfill material and compact it with approved tampers to a height of at least one foot above the utility pipe or conduit. Bring up the backfill evenly on both sides of the pipe for the full length of the pipe. Take care to ensure thorough compaction of the fill under the haunches of the pipe. Except as specified otherwise in the individual piping section, provide bedding for buried piping in accordance with AWWA C600, Type 4, except as specified herein. Compact backfill to top of pipe to 95 percent of ASTM D698 maximum density. Provide plastic piping with bedding to spring line of pipe. Provide materials as follows:

3.11.1.3.1 Class I

Angular, 0.25 to 1.5 inch, graded stone, including a number of fill materials that have regional significance such as coral, slag, cinders, crushed stone, and crushed shells.

3.11.1.3.2 Class II

Coarse sands and gravels with maximum particle size of 1.5 inch, including various graded sands and gravels containing small percentages of fines, generally granular and noncohesive, either wet or dry. Soil Types GW, GP, SW, and SP are included in this class as specified in ASTM D2487.

3.11.1.3.3 Sand

Clean, coarse-grained sand in accordance with NCDOT Standard Specifications for bedding and backfill or as indicated.

3.11.1.3.4 Gravel and Crushed Stone

Clean, coarsely graded natural gravel, crushed stone or a combination thereof in accordance with NCDOT Standard Specifications for bedding and backfill or as indicated.

3.11.1.4 Final Backfill

Fill the remainder of the trench, except for special materials for roadways, railroads and airfields, with satisfactory material. Place backfill material and compact as follows:

3.11.1.4.1 Roadways, Railroads, and Airfields

Place backfill up to the required elevation as specified. Do not permit water flooding or jetting methods of compaction.

3.11.1.4.2 Sidewalks, Turfed or Seeded Areas and Miscellaneous Areas

Deposit backfill in layers of a maximum of 12 inches loose thickness, and compact it to 85 percent maximum density for cohesive soils and 90 percent maximum density for cohesionless soils. Allow water flooding or jetting methods of compaction for granular noncohesive backfill material. Do not allow water jetting to penetrate the initial backfill. Do not permit compaction by water flooding or jetting. Apply this requirement to all other areas not specifically designated above.

3.11.2 Backfill for Appurtenances

After the manhole, catch basin, inlet, or similar structure has been constructed, place backfill in such a manner that the structure is not be damaged by the shock of falling earth. Deposit the backfill material, compact it as specified for final backfill, and bring up the backfill evenly on all sides of the structure to prevent eccentric loading and excessive stress.

3.12 SPECIAL REQUIREMENTS

Special requirements for both excavation and backfill relating to the specific utilities are as follows:

3.12.1 Gas Distribution

Excavate trenches to a depth that will provide a minimum 18 inches of cover in rock excavation and a minimum 24 inch of cover in other excavation.

3.12.2 Water Lines

Excavate trenches to a depth that provides a minimum cover of 5 feet from the existing ground surface, or from the indicated finished grade, whichever is lower, to the top of the pipe.

3.12.3 Heat Distribution System

Free initial backfill material of stones larger than 1/4 inch in any dimension.

3.12.4 Electrical Distribution System

Provide a minimum cover of 24 inches from the finished grade to direct burial cable and conduit or duct line, unless otherwise indicated.

3.13 EMBANKMENTS

3.13.1 Earth Embankments

Construct earth embankments from satisfactory materials free of organic or frozen material and rocks with any dimension greater than 3 inches. Place the material in successive horizontal layers of loose material not more than 8 inches in depth. Spread each layer uniformly on a soil surface that has been moistened or aerated as necessary, and scarified or otherwise broken up so that the fill will bond with the surface on which it is placed. After spreading, plow, disk, or otherwise break up each layer; moisten or aerate as necessary; thoroughly mix; and compact to at least 90 percent laboratory maximum density for cohesive materials or 95 percent laboratory maximum density for cohesionless materials. Backfill and fill material must be to a moisture content that will readily facilitate obtaining the specified compaction.

Compaction requirements for the upper portion of earth embankments forming subgrade for pavements are identical with those requirements specified in paragraph SUBGRADE PREPARATION. Finish compaction by sheepsfoot rollers, pneumatic-tired rollers, steel-wheeled rollers, vibratory compactors, or other approved equipment.

3.14 SUBGRADE PREPARATION

3.14.1 Proof Rolling

Finish proof rolling on an exposed subgrade free of surface water (wet conditions resulting from rainfall) which would promote degradation of an otherwise acceptable subgrade. After stripping, proof roll each area of the existing subgrade with four passes (two in each orthogonal direction) of a 25 ton pneumatic-tire roller. Operate the roller in a systematic manner to ensure the number of passes over all areas, and at speeds of 3 mph. Notify the Contracting Officer a minimum of 3 days prior to proof rolling. Perform proof rolling in the presence of the Contracting Officer. Undercut rutting or pumping of material as directed by the Contracting Officer.

3.14.2 Construction

Shape subgrade to line, grade, and cross section, and compact as specified. Include plowing, disking, and any moistening or aerating required to obtain specified compaction for this operation. Remove soft or otherwise unsatisfactory material and replace with satisfactory excavated material or other approved material as directed. Excavate rock encountered in the cut section to a depth of 6 inches below finished grade for the subgrade. Bring up low areas resulting from removal of unsatisfactory material or excavation of rock to required grade with satisfactory materials, and shape the entire subgrade to line, grade, and

cross section and compact as specified. After rolling, do not show deviations for the surface of the subgrade for roadways greater than 1/2 inch when tested with a 12-foot straightedge applied both parallel and at right angles to the centerline of the area. Do not vary the elevation of the finish subgrade more than 0.05 foot from the established grade and cross section.

3.14.3 Compaction

Finish compaction by sheepsfoot rollers, pneumatic-tired rollers, steel-wheeled rollers, vibratory compactors, or other approved equipment. Except for paved areas and railroads, compact each layer of the embankment to at least 98 percent of laboratory maximum density per ASTM D698.

3.14.3.1 Subgrade for Pavements

Compact subgrade for pavements to at least 95 percentage laboratory maximum density for the depth below the surface of the pavement shown. When more than one soil classification is present in the subgrade, thoroughly blend, reshape, and compact the top 6 inch of subgrade.

3.15 FINISHING

Finish the surface of excavations, embankments, and subgrades to a smooth and compact surface in accordance with the lines, grades, and cross sections or elevations shown. Provide the degree of finish for graded areas within 0.1 foot of the grades and elevations indicated except that the degree of finish for subgrades specified in paragraph SUBGRADE PREPARATION. Finish gutters and ditches in a manner that will result in effective drainage. Finish the surface of areas to be turfed to a smoothness suitable for the application of turfing materials. Repair graded, topsoiled, or backfilled areas prior to acceptance of the work, and re-established grades to the required elevations and slopes.

3.15.1 Subgrade and Embankments

During construction, keep embankments and excavations shaped and drained. Maintain ditches and drains along subgrade to drain effectively at all times. Do not disturb the finished subgrade by traffic or other operation. Protect and maintain the finished subgrade in a satisfactory condition until ballast, subbase, base, or pavement is placed. Do not permit the storage or stockpiling of materials on the finished subgrade. Do not lay subbase, base course, ballast, or pavement until the subgrade has been checked and approved, and in no case place subbase, base, surfacing, pavement, or ballast on a muddy, spongy, or frozen subgrade.

3.15.2 Capillary Water Barrier

Place a capillary water barrier under concrete floor and area-way slabs grade directly on the subgrade and compact with a minimum of two passes of a hand-operated plate-type vibratory compactor.

3.15.3 Grading Around Structures

Construct areas within 5 feet outside of each building and structure line true-to-grade, shape to drain, and maintain free of trash and debris until final inspection has been completed and the work has been accepted.

3.16 PLACING TOPSOIL

On areas to receive topsoil, prepare the compacted subgrade soil to a 2 inches depth for bonding of topsoil with subsoil. Spread topsoil evenly to a thickness of 4 inch and grade to the elevations and slopes shown. Do not spread topsoil when frozen or excessively wet or dry. Obtain material required for topsoil in excess of that produced by excavation within the grading limits from areas indicated.

3.17 TESTING

Prior to concrete placement, all footing excavations shall be evaluated by a Geotechnical Engineer. Bearing soils shall be verified with a dynamic cone penetrometer. A hand auger shall be used to advance a borehole for this evaluation to a depth equal to at least the foundation width or 3 feet, whichever is greater.

Perform testing by a Corps validated commercial testing laboratory or the Contractor's validated testing facility. Submit qualifications of the Corps validated commercial testing laboratory or the Contractor's validated testing facilities. If the Contractor elects to establish testing facilities, do not permit work requiring testing until the Contractor's facilities have been inspected, Corps validated and approved by the Contracting Officer.

a. Determine field in-place density in accordance with ASTM D1556/D1556M, ASTM D2167, or ASTM D6938 as applicable.

b. When test results indicate, as determined by the Contracting Officer, that compaction is not as specified, remove the material, replace and recompact to meet specification requirements.

c. Perform tests on recompacted areas to determine conformance with specification requirements. Appoint a registered professional civil engineer to certify inspections and test results. TState that the tests and observations were performed by or under the direct supervision of the engineer and that the results are representative of the materials or conditions being certified by the tests. The following number of tests, if performed at the appropriate time, will be the minimum acceptable for each type operation.

3.17.1 Fill and Backfill Material Gradation

One test per 100 cubic yards stockpiled or in-place source material. Determine gradation of fill and backfill material in accordance with ASTM C136/C136M or ASTM D1140.

3.17.2 In-Place Densities

a. One test per 2500 square feet, or fraction thereof, of each lift of fill or backfill areas compacted by other than hand-operated machines.

b. One test per 2500 square feet, or fraction thereof, of each lift of fill or backfill areas compacted by hand-operated machines.

c. One test per 75 linear feet, or fraction thereof, of each lift of embankment or backfill for roads or trenches.

3.17.3 Check Tests on In-Place Densities

If ASTM D6938 is used, check in-place densities by ASTM D1556/D1556M as follows:

a. One check test per lift for each 2500 square feet, or fraction thereof, of each lift of fill or backfill compacted by other than hand-operated machines.

b. One check test per lift for each 2500 square feet, of fill or backfill areas compacted by hand-operated machines.

c. One check test per lift for each 75 linear feet, or fraction thereof, of embankment or backfill for roads or trenches.

3.17.4 Moisture Contents

In the stockpile, excavation, or borrow areas, perform a minimum of two tests per day per type of material or source of material being placed during stable weather conditions. During unstable weather, perform tests as dictated by local conditions and approved by the Contracting Officer.

3.17.5 Optimum Moisture and Laboratory Maximum Density

Perform tests for each type material or source of material including borrow material to determine the optimum moisture and laboratory maximum density values. One representative test per 100 cubic yards of fill and backfill, or when any change in material occurs which may affect the optimum moisture content or laboratory maximum density.

3.17.6 Tolerance Tests for Subgrades

Perform continuous checks on the degree of finish specified in paragraph SUBGRADE PREPARATION during construction of the subgrades.

3.17.7 Displacement of Sewers

After other required tests have been performed and the trench backfill compacted to the finished grade surface, inspect the pipe to determine whether significant displacement has occurred. Conduct this inspection in the presence of the Contracting Officer. Inspect pipe sizes larger than 36 inches, while inspecting smaller diameter pipe by shining a light or laser between manholes or manhole locations, or by the use of television cameras passed through the pipe. If, in the judgment of the Contracting Officer, the interior of the pipe shows poor alignment or any other defects that would cause improper functioning of the system, replace or repair the defects as directed at no additional cost to the Government.

3.18 DISPOSITION OF SURPLUS MATERIAL

Remove surplus material and excavated unsatisfactory material not required or suitable for filling or backfilling, and brush, refuse, stumps, roots, and timber from Government property and properly disposed of in accordance with all applicable laws and regulations.

-- End of Section --

Intertek - PSI
5021-A W. WT Harris Blvd.
Charlotte, North Carolina 28269
Phone: (704) 598-2234
Fax: (704) 598-2236

March 16, 2023

AECOM
9400 Amberglen Boulevard
Austin, Texas 78729

Attn: Mr. Mike Russell
email: mike.russell@aecom.com

Re: **Report of Geotechnical Engineering Services**
Proposed Construct Security Forces Facility
North Carolina Air National Guard
Charlotte Douglass International Airport
Charlotte, North Carolina
PSI Report No.: 05111037

Dear Mr. Russell:

Professional Service Industries (PSI), an Intertek Company, is pleased to transmit our Geotechnical Engineering Services Report for the proposed Construct Security Forces Facility to be located at the North Carolina Air National Guard (NCANG) base at Charlotte Douglass International Airport in Charlotte, North Carolina. This report includes the results of field and laboratory testing, and recommendations for foundation and pavement design, as well as general site development.

PSI appreciates the opportunity to perform this Geotechnical Study and look forward to continued participation during the design and construction phases of this project. If you have any questions pertaining to this report, or if PSI may be of further service, please contact our office at 704-598-2234.

PSI also has great interest in providing materials testing and inspection services during the construction of this project. If you will advise us of the appropriate time to discuss these engineering services, we will be pleased to meet with you at your convenience.

Very truly yours,
PROFESSIONAL SERVICE INDUSTRIES, INC.

Andrew O. Steege, P.G.
Senior Geologist

THIS ITEM HAS BEEN DIGITALLY SIGNED AND SEALED BY:

Lloyd T Lasher
Digitally signed by Lloyd T Lasher
Date: 2023.03.16 07:34:12 -06'00'

NORTH CAROLINA PROFESSIONAL SEAL 53158 ENGINEER LLOYD T LASHER JR

Lloyd T. Lasher, Jr., P.E.
Senior Geotechnical Engineer
North Carolina License #53158

ON THE DATE ADJACENT TO THE SEAL PRINTED COPIES OF THIS DOCUMENT ARE NOT CONSIDERED SIGNED AND SEALED. THE SIGNATURE MUST BE VERIFIED ON ANY ELECTRONIC COPIES

TABLE OF CONTENTS

1 PROJECT INFORMATION 1
1.1 PROPOSAL AND PROJECT AUTHORIZATION 1
1.2 PROJECT DESCRIPTION 1
1.3 PURPOSE AND SCOPE OF WORK 2
2 EXPLORATION PROCEDURES 3
2.1 FIELD SERVICES 3
2.2 LABORATORY TESTING 4
3 SITE AND SUBSURFACE CONDITIONS 4
3.1 SITE DESCRIPTION 4
3.2 SITE GEOLOGY 5
3.3 SUBSURFACE CONDITIONS 5
4 GEOTECHNICAL EVALUATION AND RECOMMENDATIONS 8
4.1 GEOTECHNICAL ASSESSMENT 8
4.2 SITE PREPARATION AND EARTHWORK 9
4.3 SEISMIC CONSIDERATIONS 11
4.4 FOUNDATION RECOMMENDATIONS 11
4.5 FLOOR SLAB RECOMMENDATIONS 13
4.6 PAVEMENT DESIGN GUIDELINES AND PARAMETERS 15
4.7 SLOPE STABILITY ANALYSIS RESULTS 17
5 CONSTRUCTION CONSIDERATIONS 18
5.1 GROUNDWATER 18
5.2 EXCAVATION AND SAFETY 18
6 REPORT LIMITATIONS 19

APPENDIX
Site Vicinity Map
Boring Location Plan
General Notes and Soil Classification Chart
Boring Logs
Boring Summary
Laboratory Test Results
Slope Stability Package

1 PROJECT INFORMATION

1.1 PROPOSAL AND PROJECT AUTHORIZATION

This report presents the findings and recommendations of a geotechnical exploration and assessment performed by Professional Service Industries (PSI) for the proposed Construct Security Forces Facility to be located at the North Carolina Air National Guard (NCANG) base at Charlotte Douglass International Airport in Charlotte, North Carolina. These services were performed in general accordance with a Continuing Services Agreement between AECOM Technical Services, Inc. (AECOM) and PSI dated November 10, 2022 which references PSI Proposal No. 0511-317012 2nd Revision dated December 16, 2021.

1.2 PROJECT DESCRIPTION

Project information was initially provided through an emailed request for proposal (RFP) from Ashleigh Hernandez of AECOM on July 20, 2020. Additional project information has been provided by Mike Russell of AECOM through subsequent email correspondence. Provided information includes the following documents:

- "Project Documentation Package", dated April 2020
- "Request for Proposal (RFP) 20RFP26137AU14, Geotechnical Services", dated July 20, 2020
- Revised "Geotechnical Service Scope", dated August 5, 2020
- "Standard Conditions for Soil Engineer for Soil Investigation and Engineering Services, undated
- "Existing Utility Plan" dated 12-13-2021
- "Boring Plan" (Sheet B01) prepared by AECOM, undated

The "Boring Plan", provided to PSI on January 26, 2023, presents the proposed building footprint, five requested boring locations, and existing site features including topographic contour lines. Site plans providing information about additional proposed construction such as pavement areas, the pedestrian bridge and communications tower were not provided to PSI at the time of this report.

Based on the provided information, we understand the project consists of the construction of a new Construct Security Forces Building for the 145th Airlift Wing of the North Carolina Air National Guard at their base in Charlotte, North Carolina. Proposed construction will include a two-story building with a footprint of about 5,500 square feet (approximately 100 feet by 55 feet). The building will likely be steel framing or masonry with a concrete slab-on-grade (no basement or below grade walls). Provided structural loading information indicates maximum column loads will be on the order of 185 kips (95 kips dead load and 90 kips live load). We also understand a pedestrian entry bridge will be constructed to provide access to the second level from the street along the north side of the building.

We understand paved areas providing access to existing roads, parking lots for government and privately-owned vehicles, and sidewalks are also proposed. However, as noted above, additional details for the proposed pavement such as location and traffic loading information were not provided. Based on the provided topographic information and our site reconnaissance, the ground surface across the site has a downward slope from north to south. Relief within the building footprint is about 4 feet and relief across the entire site is on the order of 21 feet. Specific proposed grading information was not provided. However, we understand the building will have a finished floor elevation on the

order of 712.5 feet. As such, maximum cut and fill depths within the proposed building footprint will be about ½ and 3 feet, respectively.

Most of the site relief, about 15 feet or more, occurs between the roadway and parking spaces to the north and the north side of the proposed building footprint area. As noted previously, we understand a pedestrian bridge will be constructed to provide access to the second level of the building from the street to the north side of the building. AECOM has indicated the bridge will be about 55 to 60 feet long and the north abutment will be comprised of two columns about 10 feet apart and each supporting a maximum structural load of 40 kips. Details regarding the size and depth of the columns were not provided. According to information provided by AECOM, no additional grading or retaining wall installation is planned in the area of the north slope and abutment.

Based on information provided by AECOM on March 7, 2023, PSI understands that a 30-foot communications tower will be constructed at the top of the hill near the northern bridge abutment. We understand the tower will impact a maximum load of about 4 kips. Per the designers' specifications, the tower is planned to be supported by a 6-foot 9-inch mat foundation; but the exact location or thickness of the mat was not provided.

The information presented in this section was used in the evaluation. Estimated loads and corresponding foundation sizes have a direct effect on the recommendations, including the type of foundation, the allowable soil bearing capacity, and the estimated potential settlement. In addition, estimated subgrade elevations and cut/fill quantities can have a direct effect on the provided recommendations. If any of the noted information is incorrect or has changed, please inform PSI so that we may amend the recommendations presented in this report, if appropriate. If PSI is not retained to perform this function, PSI cannot be responsible for the impact of the changes on the performance of the project.

1.3 PURPOSE AND SCOPE OF WORK

The purpose of this study was to obtain information regarding the general subsurface conditions within the proposed construction area, to assess the engineering characteristics of the subsurface materials, and to provide general design recommendations regarding the geotechnical aspects of the proposed construction. To accomplish this, PSI performed a site reconnaissance, drilled five soil test borings within the areas of proposed site improvements, obtained two undisturbed (Shelby tube) samples, conducted laboratory classification testing and prepared this report summarizing the findings, as well as our conclusions and recommendations.

The scope of our geotechnical services did not include an environmental assessment for determining the presence or absence of wetlands, or hazardous or toxic materials in the soil, bedrock, groundwater, or air, on or below or around this site. Any statement in this report or on the boring logs regarding odors, colors, unusual or suspicious items, or conditions are strictly for the information of our client.

PSI did not provide nor was it requested to provide any service to investigate or detect the presence of moisture, mold or other biological contaminants in or around any structure, or any service that was designed or intended to prevent or lower the risk of the occurrence of the amplification of the same. Client acknowledges that mold is ubiquitous to the environment with mold amplification occurring when building materials are impacted by moisture. Client further acknowledges that site conditions are outside of PSI's control, and that mold amplification will likely occur, or continue to occur, in the presence of moisture. As such, PSI cannot and shall not be held responsible for the occurrence or recurrence of mold amplification.

2 EXPLORATION PROCEDURES

2.1 FIELD SERVICES

PSI advanced five soil test borings (Borings B-1 through B-5) within the proposed site at the approximate locations requested by AECOM. Some of the borings were offset due to buried utilities identified during private utility location services. Borings B-1 through B-4 were drilled within the proposed two-story building footprint area, and boring B-5 was drilled within the reported area of the proposed north pedestrian bridge abutment. The approximate boring locations are shown on the "Boring Location Plan" (Figure 2) included in the Appendix. Horizontal and vertical survey control was not performed for the test boring locations prior to our field exploration program. The borings were located based upon estimated distances and relationships to obvious landmarks, and the site plan provided by the client. The boring locations are considered accurate to the degree implied by these methods.

Soil test borings were advanced at this site by HPC, a subcontractor hired by PSI, utilizing a CME 550 ATV-mounted drilling rig using hollow-stem, continuous-flight augers. All boring and sampling operations were conducted in general compliance with ASTM D 1586. At regular intervals, soil samples were obtained with a standard 2-inch O.D. split-barrel sampler.

An automatic trip drop hammer was used for the standard penetration testing, which generally has a higher efficiency than a manual cathead-and-rope hammer. Typically, the automatic hammer yields lower standard penetration test resistances (N-values) than a manual cathead-and-rope hammer. This reduction has been taken into account in our evaluation. However, the N-values reported on the logs, and the consistency descriptions on the boring logs are based on the field-recorded values and were not corrected for hammer efficiency.

The recovered soil samples were classified visually in the field by the drill crew and a PSI geologist, then transported to our laboratory for additional visual classification and laboratory testing. A "Boring Log" was prepared for each boring and the "Logs" are included in the Appendix of the report. The logs were prepared using the observations made in the field, as well as the classifications in the laboratory and the laboratory test results. Strata descriptions, presented on the logs, were based on visual-manual evaluations by our geologist and include the classifications in general accordance with the Unified Soil Classification System (USCS). The "Soil Classification Chart", included in the Appendix, illustrates the USCS legend depicted on the logs. The ground surface elevations presented on the boring logs were interpolated from the provided site topographic information and should be considered approximate.

Groundwater levels were measured in the boreholes at the time of boring and upon completion. In addition, delayed groundwater level readings were conducted on selected borings prior to site departure. The results of the readings are presented in Section 3.3.4 and included on the soil test boring logs when encountered. The borings were backfilled upon completion or after the delayed reading using the soil cuttings for safety considerations.

2.2 LABORATORY TESTING

A geologist visually-manually classified the soil samples in the laboratory in general accordance with the Unified Soil Classification System (USCS) (ASTM D2487 and D2488). Percent finer than the No. 200 sieve (ASTM D1140), Atterberg limits tests (ASTM D4318), natural water content determinations (ASTM D2216), consolidation (ASTM D2435) and unconfined compressive strength (ASTM D2166) tests were also conducted on representative samples recovered from the test boring locations. The laboratory test results are presented in Section 3.3.5 and/or are shown on the individual boring logs.

3 SITE AND SUBSURFACE CONDITIONS

3.1 SITE DESCRIPTION

The site encompasses an area of about ¼ acre and is located north of and adjacent to Payne Boulevard, approximately 300 feet east of its intersection with 1st Union Road, in Charlotte, North Carolina. The site also lies within the North Carolina Air National Guard (NCANG) base at Charlotte Douglass International Airport. The site location is depicted on the “Site Vicinity Map” (Figure 1) included in the Appendix.

At the time of our site reconnaissance (February 2023), most of the site, including the proposed building footprint area; generally consisted of a grass-covered area and the western edge of an asphalt-paved parking lot with a gradual downward slope to the south. However, the north portion of the site contains a steep grass-covered slope to the south with an approximately 5-foot-high concrete retaining wall at the bottom. A thin, level grass-covered area was observed at the top of the slope, followed by asphalt-paved parking spaces and a roadway further to the north. The slope also contained a concrete stairway. Based on the provided topographic information and our site reconnaissance, relief within the building footprint is about 4 feet and relief across the entire site is on the order of 21 feet. Most of the site relief, about 15 feet or more, occurs in the vicinity of the steep slope in the north site area. Numerous buried utility lines are contained within the proposed site area.

PSI performed a review of historical aerial photographs of the site available on Google Earth. Based on this, the site was developed as the current facility prior to 1993. However, former buildings occupied the north and southwest site area that were removed between 2004 and 2007.

3.2 SITE GEOLOGY

The project site is located within Mecklenburg County, North Carolina, and lies within the Charlotte Belt of the Piedmont Physiographic Province of the eastern United States. This province is characterized by broad, gently rolling ridges formed on the stronger bedrock of the area. Between these ridges, lowlands and drainage areas are formed on the less resistant bedrock. The Piedmont is a complex assemblage of igneous (volcanic and plutonic) and sedimentary rocks that were generally formed during the Late Proterozoic Era and the Early Cambrian Period (approximately 550 to 900 million years ago). During and subsequent to formation, these rocks were subjected to several major tectonic events, including plate collisions, folding, faulting, and igneous intrusions, that resulted in the uplift and metamorphism of the preexisting rocks. The tectonic activity generally stopped about 200 to 250 million years ago and erosional forces have formed the current ground surface. Review of the Geologic Map of the Charlotte 1° by 2° Quadrangle, North Carolina and South Carolina (USGS, by Goldsmith, Milton and Horton, 1988) indicates the site is underlain by meta quartz diorite of late Proterozoic to early Cambrian age.

Residual soils are the result of in-place physical and chemical weathering of the parent bedrock. In this area residual soils generally consist of an upper layer of fine-grained SILT or CLAY underlain by Sandy SILT or Silty SAND. The sand content generally increases with depth. Separating the residual soil from the underlying parent bedrock is typically a transition zone of high consistency material referred to as partially weathered rock. Partially weathered rock is defined as residual material with standard penetration resistance (ASTM D1586) in excess of 50 blows per 6-inches penetration.

The weathering processes that produced the residual soils and partially weathered rock were extremely variable, due to such factors as rock type and mineralogy, past groundwater conditions, and the tectonic history of the specific area (resulting in localized fractures, joints and faults within the bedrock). Differential weathering of the parent bedrock has resulted in highly variable subsurface conditions and can include abrupt changes in soil type and consistency over relatively short horizontal and vertical distances. Furthermore, depths to rock can also be highly variable; and suspended boulders, discontinuous rock layers/lenses, or rock pinnacles can be present within the residual soils and transitional zones of soft weathered rock.

Although only about 1 foot of apparent fill material was encountered in one of the borings, fill materials are often encountered on previously graded/developed sites such as this and is often difficult to discern in the absence of deleterious materials as development often relocates native soil during site grading activities. The suitability of existing fill can vary significantly across the site. It is not uncommon to encounter buried debris and unsuitable materials on previously developed sites.

3.3 SUBSURFACE CONDITIONS

General subsurface conditions encountered during the subsurface exploration are described below. For more detailed soil descriptions and stratifications at the boring locations, the “Boring Logs” should be reviewed. The “Boring Logs” represent our interpretation of the subsurface conditions based on a review of the field logs and an engineering examination of the samples. The horizontal stratification lines designating the interface between various strata represent approximate boundaries. Transition between different strata in the field may be gradual in both

the horizontal and vertical directions. Groundwater, or lack thereof, encountered in the borings and noted on the "Boring Logs" represents conditions only at the time of the exploration.

3.3.1 SURFACE

Initially, four of the borings encountered a layer of topsoil approximately 3 to 5 inches thick. The term topsoil, as used in this report, is a general designation given to the surface horizon of soil which appears to have an elevated organic content. No laboratory testing was performed on the topsoil to determine its suitability for supporting plant life, or ability to satisfy a particular specification. At boring B-4 gravel was noted mixed into the topsoil layer.

Boring B-2 initially encountered an asphalt layer approximately 2 inches thick. The asphalt was underlain by approximately 6 inches of gravel.

3.3.2 FILL

A thin layer of apparent fill soils, extending to a depth of about 1-foot, was noted beneath the topsoil layer at B-4. The apparent fill soils consisted of Elastic SILT (MH) with gravel. The apparent fill material encountered at B-4 was not of sufficient thickness for recording a Standard Penetration Test Resistance (N-value).

3.3.3 RESIDUUM

Residual soils were encountered beneath the apparent fill soils at B-4, and underlying the topsoil or pavement layer at the remaining borings. At all of the borings except B-3, the residuum initially consisted of soft the very stiff Elastic SILT (MH). These MH soils extended to depths ranging from about 3 to 17 feet beneath the existing ground surface. N-values recorded within the Elastic SILT (MH) soils ranged from 4 blows per foot (bpf) to 30 bpf.

Other residual soils sampled at the site generally consisted of soft to very stiff Sandy SILT (ML), and very loose to medium dense Silty SAND (SM). N-values recorded within these residual soils ranged from 2 to 25 bpf but were typically in the 5 to 10 bpf range. All of the borings were terminated in the residual soils at depths ranging from about 30 to 35 feet beneath the existing ground surface.

3.3.4 GROUNDWATER INFORMATION

Groundwater levels were measured in the boreholes at the time of boring and upon completion. Most of the borings were backfilled upon completion using the soil cuttings for safety considerations. Therefore, long term delayed groundwater levels were not available. However, a delayed groundwater level reading was conducted on boring B-3 after a period of about 5 hours. Groundwater was noted in two of the borings at the approximate depths indicated in the following table.

Groundwater Depths

Boring	Approximate Depth to Groundwater at Time of Drilling (feet)	Approximate Depth to Groundwater at the Completion of Drilling (feet)	Approximate Depth to Groundwater After a Period of about 5 hours (feet)
B-1	32	Dry, Caved at 15	BF
B-2	21	15 ½	BF
B-3	17	18	14 ½
B-4	19	12 ½	BF

BF = Backfilled

The groundwater information presented in this report is the information that was collected at the time of our field activities. We recommend that the Contractor determine the actual groundwater level at the site at the time of the construction activities.

Subsurface water levels within this region tend to fluctuate with seasonal and climatic changes, as well as with some types of construction operations. Generally, the highest groundwater levels occur in late winter and early spring; and the lowest levels in late summer and early fall. Therefore, water may be encountered during construction at depths not indicated during this study.

Additionally, perched groundwater conditions can develop over low permeability soil or weathered rock following periods of heavy or prolonged precipitation. Groundwater may be encountered during construction at depths not indicated during this exploration.

3.3.5 LABORATORY TEST RESULTS

The results of the laboratory testing program are summarized in the following table.

Sample Location	Sample Depth (ft)	Moisture Content (%)	Percent Fines (%)	ATTERBERG LIMITS			USCS Soil Classification
				LL	PL	PI	
B-1	1 - 2 ½	41.3	97.1	63	44	19	MH*
B-1	8 – 10	32.7	62.7	53	43	10	MH*
B-3	1 – 2 ½	19.7	69.1	45	28	17	ML
B-5	1 – 2 ½	31.1	--	--	--	--	--
B-5	3 ½ - 5	29.7	--	--	--	--	--
B-5	6 – 7 ½	28.1	74.4	54	39	15	MH*

*Typically not recommended for direct support of foundations, slabs or pavements.

Additional laboratory testing including unconfined compressive strength (ASTM D2166) and consolidation (ASTM D2435) was performed on an undisturbed sample (Shelby tube) collected from boring B-1 at a depth of approximately 8 to 10 feet beneath the existing grade. The results of that testing is presented in the Appendix of this report.

4 GEOTECHNICAL EVALUATION AND RECOMMENDATIONS

4.1 GEOTECHNICAL ASSESSMENT

The following geotechnical design recommendations have been developed on the basis of the previously described project characteristics and subsurface conditions encountered. If there are any changes in these project criteria, including building location on the site, a review should be made by PSI to determine if modifications to the recommendations are warranted.

Once final design plans and specifications are available, a general review by PSI is recommended as a means to check that the evaluations made in preparation of this report are correct and that earthwork and foundation recommendations are properly interpreted and implemented.

Based on the results of the fieldwork, laboratory evaluation and engineering analyses, we have identified the following potential constraints to the development of this site; the presence of high plasticity soils (MH).

Elastic SILT (MH) comprised the near-surface soils in four of the five borings. These MH soils generally extended to depths ranging from about 3 to 17 feet beneath the existing ground surface. These soils generally exhibit moderately high to high plastic properties and are typically susceptible to changes in volume with even slight changes in moisture content (i.e. shrink/swell behavior). As a result, MH soils are not recommended for direct support of foundations, slabs or pavements. We typically recommend a minimum 2-foot thick buffer of low-plasticity structural fill material between these soils and slabs or foundations, and a minimum 1-foot buffer between these soils and pavements. As an alternative, foundations may be deepened to bear below the MH soils or bear in these materials provided the bottom of the foundations are at least 4 feet below final finished grade.

The extent of MH soils encountered during the proposed construction will be dependent upon proposed grading plans. Based on the borings and a proposed FFE of 712.5 feet, it appears that MH soils should be anticipated to be encountered at foundation or slab bearing elevations across much of the proposed building footprint area as well as that of the north bridge abutment and communications tower, as illustrated on the Boring Summary included in the Appendix. When MH soils are encountered at or within 2 feet of the foundation or slab bearing elevation, or within 1 foot of pavement bearing elevations, they should be removed and replaced with low-plasticity structural fill as described above. In the case of the bridge abutment and tower foundations, the undercut should extend to the slope face to prevent water from being trapped below shallow foundation elements. Therefore, the project budget should include a contingency for the removal and replacement of residual MH soils to provide the buffers described above. The high plasticity MH soils should be replaced with properly compacted fill, flowable fill, or lean concrete. In addition, MH soils are typically not recommended for reuse as structural fill.

High plasticity MH soils are moisture sensitive and will likely become unstable due to the presence of excess moisture and normal construction equipment traffic operating over them. Accordingly, construction traffic should be kept to a minimum on the exposed soils to reduce the potential for creating an unstable subgrade. Elevated moisture contents were noted in some of the recovered soil samples. Some drying and reworking of the on-site soils should be anticipated.

4.2 SITE PREPARATION AND EARTHWORK

Site clearing, stripping and grubbing operations should only be performed in dry weather conditions.

Initially, wet soils, topsoil, organics, debris, pavements, utilities, and other unsuitable materials, should be stripped from an area extending at least 10 feet beyond the outline of the proposed construction. Any existing below-grade construction encountered during site grading or construction should be examined by the Geotechnical Engineer to determine if these materials will require removal. Depressions or low areas resulting from stripping and grubbing or removal of other subsurface appurtenances should be backfilled with compacted structural fill in accordance with the recommendations presented in this report.

After stripping, removal of unsuitable surface soils, and rough excavation grading, we recommend that areas to provide support for the floor slabs, pavements, and/or structural fill be evaluated for the presence of soft, surficial soils and/or plastic soils by proofrolling and inspection by the Geotechnical Engineer. The proofroll should be performed using a loaded tandem axle dump truck, or similar rubber-tired equipment, weighing between 15 and 25 tons. The vehicle should make at least four passes over each location, with the last two passes perpendicular to the first two. Areas that wave, rut, or deflect significantly and continue to do so after several passes of the proofroller should be undercut to firmer soils as recommended by the geotechnical engineer. Based on the borings, some over-excavation of marginal bearing soil should be expected. Undercut areas should be backfilled in thin lifts with approved, compacted fill materials. Proofroll operations should be monitored carefully by PSI's Project Geotechnical Engineer.

We caution that the subgrade soils exposed after stripping contain sufficient silt and clay to render them both moisture sensitive and frost susceptible. Due to their moisture sensitivity, proper site drainage should be maintained during earthwork operations to reduce accumulation of moisture and wet weather delays. These soils may become unstable due to the presence of excess moisture and normal construction equipment traffic operating over them. Accordingly, construction traffic should be kept to a minimum on the exposed soils to reduce the potential for creating an unstable subgrade. If the surface soils become softened/unstable during wet weather or frozen, these soils should be removed before additional fill is placed.

Drying soils for re-use as structural fill is often considered a routine aspect of typical grading operations and is not considered a pay item. If unit prices for earthwork operations are established, they should be examined closely before the contract is executed. If undercutting is a pay item, then undercut volumes should be determined by field measurement. Methods such as counting trucks should not be used for determination of undercut volume, as they are less accurate.

Recommended criteria for soil fill characteristics (both on-site and imported materials) and compaction procedures are listed below. The project design documents should include the following recommendations to address proper placement and compaction of project fill materials. Earthwork operations should not begin until representative samples are collected and tested. The maximum dry density and optimum moisture content should be determined.

EARTH FILL MATERIALS

- Imported or on-site fill material satisfactory for structural fill should include clean soil material with USCS classifications of (SP, SW, SM, and some SC, CL or ML). The fill material should have a Standard Proctor (ASTM D698) Maximum Dry Density of at least 100 pcf, a maximum Liquid Limit of 45 and a Plasticity Index of 20 or less. Fat CLAY (CH) and Elastic SILT (MH) soils should not be used as structural fill.

- Organic content or other foreign matter (debris) should be no greater than 3 percent by weight, and no large roots (greater than ¼ inch in diameter) should be allowed. Organic materials should not be intentionally mixed into structural fill.

- Material utilized as fill should not contain rocks greater that 3 inches in diameter or greater than 30 percent retained on the ¾-inch sieve.

COMPACTION RECOMMENDATIONS

- Maximum loose lift thickness – 8 inches, mass fill. Loose lifts of 4 to 6 inches in trenches and other confined spaces where hand operated equipment is used.

- Compaction requirements – 95 percent of the maximum dry density and 98 percent within the upper 12 inches as determined by the standard Proctor (ASTM D698) compaction test.

- Soil moisture content at time of compaction – within ±3 percent of the optimum moisture content.

TEST CRITERIA TO EVALUATE FILL AND COMPACTION

- One standard Proctor compaction test and one Atterberg limits test for each soil type used as project fill. Gradation tests may be necessary and should be performed at the Geotechnical Engineer's discretion.

- One density test every 2,500 square feet for each lift or two tests per lift, whichever is greater (for preliminary planning only; the test frequency should be determined by our engineering staff).

- Trench fill areas – one density test every 75 linear feet at vertical intervals of 2 feet or less.

It will be important to maintain positive site drainage throughout construction. Storm water runoff should be diverted around the building and pavement areas. The site should be graded at all times such that water is not allowed to pond. The surface should be sealed with a smooth drum roller to enhance drainage if precipitation is expected. Subgrades damaged by construction equipment should be repaired immediately to avoid further degradation in adjacent areas and to help prevent water ponding.

Should there be a significant time lag or period of inclement weather between site grading and the fine grading of the slab prior to the placement of stone or concrete, the Geotechnical Engineer of Record or qualified representative should assess the condition of the prepared subgrade. The subgrade may

require scarification and re-compaction or other remedial measures to provide a firm and unyielding subgrade prior to final slab construction.

4.3 SEISMIC CONSIDERATIONS

The project site is located within a municipality that employs the 2018 North Carolina Building Code, a fully integrated code based on the 2015 International Building Code® (IBC). As part of this Code, the design of structures must consider dynamic forces resulting from seismic events. These forces are dependent upon the magnitude of the earthquake event, as well as the properties of the soils that underlie the site. As part of the procedure to evaluate seismic forces, the Code requires the evaluation of the Seismic Site Class, which categorizes the site based upon the characteristics of the subsurface profile within the upper 100 feet of the ground surface.

To define the Site Class for this project, we first interpreted the results of soil test borings drilled within the project site and estimated appropriate soil properties below the base of the borings to a depth of 100 feet, as permitted by the Code. The estimated soil properties were based upon our experience with subsurface conditions in the general site area.

Based upon the SPT N-values recorded during the field exploration, the subsurface conditions within the site are consistent with the characteristics of a ***Site Class "D"*** as defined in Table 1613.5.2 of the Code.

The associated IBC (2015) probabilistic ground acceleration values and site coefficients for the general site area were obtained from the USGS U.S. Seismic Design Maps Web Application (http://geohazards.usgs.gov/designmaps/us/application.php) and are presented in the table below:

Ground Motion Values for Site Class "D"*

Period (sec)	Mapped MCE Spectral Response Acceleration** (g)		Site Coefficients		Adjusted MCE Spectral Response Acceleration (g)		Design Spectral Response Acceleration (g)	
0.2	S_s	0.24	F_a	1.6	SM_s	0.384	SD_s	0.256
1.0	S_1	0.103	F_v	2.388	SM_1	0.246	SD_1	0.164

**2% Probability of Exceedance in 50 years for Latitude 35.21417 and Longitude -80.92993*
MCE = Maximum Considered Earthquake

The Site Coefficients, F_a and F_v presented in the above table were obtained also from the noted USGS webpage, as a function of the site classification and mapped spectral response acceleration at the short (S_s) and 1-second (S_1) periods, but can also be interpolated from IBC Tables 1613.5.3(1) and 1613.5.3(2).

4.4 FOUNDATION RECOMMENDATIONS

Based on the subsurface exploration performed at the site and the recommended site preparation, the following recommendations are provided to support the proposed structure at the site.

SHALLOW FOUNDATIONS

Based on the results of the geotechnical exploration, the proposed structure may be supported on conventional shallow spread footings. We recommend that footings be designed for a maximum net allowable soil bearing capacity of 2,000 psf. This recommendation assumes that the building foundations will bear in low plasticity natural soil or new structural fill placed and compacted in accordance with the recommendations of this report. We recommend continuous wall and isolated column footings with minimum widths of at least 18 inches and 24 inches, respectively, regardless of the actual resulting bearing pressure.

All foundation excavations should be evaluated for the presence of organic-laden or high plasticity soils. Due to the presence of potentially expansive, high plasticity soils (MH), inspection of all foundation excavations will be required to determine if these materials are present at or within 2 feet of the bearing elevation. If high plasticity soils are found within 2 feet of the bearing level for foundations, the plastic soils should be removed and replaced with a low-plasticity fill to a depth of 2 feet below the footing bottom or the footing extended to bear at least 4 feet below the adjacent finished grade. The replacement material should be silty sand, low plasticity silt, lean clay, non-excavatable flowable fill, or lean concrete. If compacted structural fill is used as backfill, the undercut excavations to remove unsuitable materials should be centered beneath the footing and widened ½ foot in each direction for each foot of undercut depth, measured from the outside edge of the new foundation. If lean concrete or non-excavatable flowable fill is used as backfill, the foundation excavation need not be widened. Open graded stone, such as No. 57 stone, should not be used as backfill beneath foundations because of the tendency of water to accumulate in open-graded aggregate. In the case of the bridge abutment and communications tower foundations, it would be beneficial to extend the undercut of high plasticity soils to the slope face to prevent water from being trapped below the foundations.

All foundations should bear at a minimum depth of 18 inches below the lowest adjacent final ground surface for frost penetration, and protective embedment. PSI recommends that the foundations be designed in accordance with the 2015 International Building Code.

We estimate that footings with width no larger than 9 feet, designed and constructed in accordance with the recommendations herein will experience post-construction total settlements generally less than 1-inch with differential settlement along a 25-foot long portion of a continuous footing, or similarly spaced column footings generally less than ½-inch. Total and differential settlements of these magnitudes are usually considered tolerable for the anticipated construction. However, the tolerance of the proposed structure to the predicted total and differential settlements should be confirmed by the structural engineer.

The base adhesion/frictional resistance and the passive soil resistance will resist the horizontal loads on shallow foundations. For a footing cast against natural soil or properly compacted fill, the adhesion/frictional resistance and the passive soil resistance values for both transient and sustained loading conditions are given herein. For sustained and transient loading conditions, a frictional coefficient of 0.35 and an allowable passive resistance of 225 psf per foot depth is recommended. Passive resistance from the upper two feet of soil should be neglected unless the area adjacent to the footing is paved. Also, the passive resistance of any un-compacted fill material should be neglected.

The uplift resistance of a shallow foundation formed in an open excavation will be limited to the weight of the foundation concrete and the soil above it. For design purposes, the ultimate uplift resistance should be based on effective unit weights of 110 and 150 pcf for soil and concrete, respectively. This value should then be reduced by an appropriate factor of safety to arrive at the allowable uplift load. If there is a chance of submergence, the buoyant unit weights should be used.

Foundation concrete should be placed as soon as possible after excavation. If foundation excavations must be left open overnight, or exposed to inclement weather, the base of the excavation should be protected with a "mud mat" consisting of a couple of inches of lean concrete. Footing excavations should be protected from surface water run-off and freezing. If water is allowed to accumulate within a footing excavation and soften the bearing soils, or if the bearing soils are allowed to freeze, the deficient soils should be removed from the excavation prior to concrete placement.

Footing excavations should be evaluated by the Geotechnical Engineer or Record, or his representative to determine that soils capable of supporting the recommended design bearing pressures are present at and immediately below the bearing level after excavation and prior to placement of reinforcing steel in the footing excavations. We recommend that the bearing soils at the bottom of and below the footing excavations be verified with a dynamic cone penetrometer to assess the suitability of the soils. A hand auger should be used to advance a borehole for this evaluation to a depth equal to at least the foundation width or 3 feet, whichever is greater. Footing evaluations should be performed prior to reinforcement and concrete placement.

If unsuitable bearing soils are encountered, these materials should be removed. The foundations can then be established at the new, lower bearing elevation, or the unsuitable material can be replaced with properly compacted fill, flowable fill, or lean concrete. If compacted structural fill is used as backfill, the undercut excavations to remove unsuitable materials should be centered beneath the footing and widened ½ foot, in each direction, for each foot of undercut depth, measured from the outside edge of the new foundation. If lean concrete or flowable fill is used as backfill, the foundation excavation need not be widened. Open graded stone, such as No. 57 stone, should not be used to backfill foundation excavations.

4.5 FLOOR SLAB RECOMMENDATIONS

Floor slabs may be supported on subgrades prepared in accordance with the SITE PREPARATION AND EARTHWORK section (paragraph 4.2) of this report. Depending upon proposed grading, we anticipate that potentially expansive Elastic SILT (MH) soils may have to be removed and replaced with low plasticity structural fill to a depth of 2 feet below the slab subgrade in isolated areas of the site.

Where concrete slabs are designed as beams on an elastic foundation, the soils that will comprise the subgrade soils should be assumed to have a modulus of subgrade reaction (k) of 100 pounds per cubic inch (pci). This value is estimated based on the expected results of a plate load test using a nominal 12-inch square plate and should be adjusted for the size and geometry of the proposed slab.

In order to provide uniform support beneath any proposed floor slab-on-grade, we recommend that floor slabs be underlain by a minimum of 4 inches of compacted aggregate base course material. The estimated modulus of subgrade reaction after the addition of 4 inches of aggregate subbase material is 120 pci.

The aggregate base course material should be compacted to at least 98 percent of its standard Proctor maximum dry density. Open-graded crushed stone, such as No. 57 stone, may also be used; however, it is our experience that open graded crushed stone can collect water during periods of rain and cause saturation and softening of the subgrade soils prior to placement of the floor slab concrete. Therefore, construction sequencing/timing, and the season in which the stone is placed, should be taken into consideration.

The crushed rock base course is intended to provide a capillary break to limit migration of moisture through the slab. If additional protection against moisture vapor is desired or moisture sensitive floor coverings are proposed, a vapor retarding membrane may also be incorporated into the design; however, there are no specific conditions that mandate its use. Factors such as cost, special considerations for construction, and the floor coverings suggest that decisions on the use of vapor retarding membranes be made by the architect and owner. Based on the subsurface materials and the intended use of the structure, we recommend the use of a vapor retarding membrane. Vapor retarders, if used, should be installed in accordance with ACI 302.1, Chapter 3.

The precautions listed below should be closely followed for construction of slabs-on-grade. These details will not prevent the amount of slab movement but are intended to reduce potential damage should some settlement of the supporting subgrade take place.

- Cracking of slabs-on-grade is normal and should be expected. Cracking can occur not only as a result of heaving or compression of the supporting soil, but also as a result of concrete curing stresses. The occurrence of concrete shrinkage cracks, and problems associated with concrete curing may be reduced and/or controlled by limiting the water to cement ratio of the concrete, proper concrete placement, finishing, and curing, and by the placement of crack control joints at frequent intervals, particularly, where re-entrant slab corners occur. The American Concrete Institute (ACI) recommends a maximum panel size (in feet) equal to approximately three times the thickness of the slab (in inches) in both directions. For example, joints are recommended at a maximum spacing of 12 feet assuming a four-inch thick slab. We also recommend that control joints be scored three feet in from and parallel to all foundation walls. Using fiber reinforcement in the concrete can also control shrinkage cracking.

- Some increase in moisture content is inevitable as a result of development and associated landscaping; however, extreme moisture content increases can be largely controlled by proper and responsible site drainage, building maintenance and irrigation practices.

- All backfill in areas supporting slabs should be moisture conditioned and compacted as described earlier in this report. Backfill in all interior and exterior utility line trenches should be carefully compacted.

- Exterior slabs should be isolated from the building. These slabs should be reinforced to function as independent units. Movement of these slabs should not be transmitted to the building foundation or superstructure.

4.6 PAVEMENT DESIGN GUIDELINES AND PARAMETERS

4.7.1 PAVEMENT SUBGRADE PREPARATION

Following the stripping of deleterious materials, we recommend the proposed pavement subgrade be prepared and compacted in accordance with the recommendations provided in Section 4.2 "SITE PREPARATION AND EARTHWORK" of this report. Based on the borings and depending on proposed grading, high plasticity Elastic SILT (MH) is anticipated within portions of the site. The final amount of removal and replacement of the Elastic SILT (MH) will be determined during construction; however, because of the poor subgrade characteristics, a minimum buffer of at least 1 foot of non-expansive low plasticity compacted fill should be placed prior to pavement construction in areas in which Elastic SILT (MH) is determined to be present. Based on the borings and assumed grading plans, the owner should anticipate removal of MH soils to provide a minimum buffer of at least 1 foot of non-expansive, low plasticity compacted fill across some proposed pavement construction areas.

We recommend proof-rolling and re-compacting (to 98 percent of the materials maximum dry density as determined by the standard Proctor (ASTM D698) compaction test) the upper six inches of subgrade immediately prior to placement of the aggregate base course (ABC). The exposed pavement subgrade should also be evaluated by a representative of PSI immediately prior to placing ABC. If low consistency soils are encountered which cannot be adequately compacted in place, such soils should be removed and replaced with well-compacted soil fill or crushed stone materials.

Based upon the findings of our borings, proposed grading plans, and the recommendations presented herein, we anticipate residual ML or SM soils, or newly placed structural fill soils will be present at the subgrade elevation. Further, some borings indicate that weak surface soils are present in the areas to be paved and scarifying and recompaction as well as some removal and replacement of subgrade soils should be expected. A conservative California Bearing Ratio (CBR) value of about 5 can be reasonably assumed for these soils at compaction levels of about 98 percent of the standard Proctor maximum dry density within about 2 percent of optimum moisture.

Site grading is generally accomplished early in the construction phase. Subsequently as construction proceeds, the subgrade may be disturbed due to utility excavations, construction traffic, desiccation, and rainfall. As a result, the pavement subgrade may not be suitable for pavement construction and corrective action will be required. The subgrade should be carefully evaluated at the time of pavement construction by PSI and subgrade areas should be reworked, moisture conditioned, and property compacted to the recommendations in this report immediately prior to paving.

Prevention of infiltration of water into the subgrade is essential for the successful long-term performance of any pavement. Both the subgrade and the pavement surface should be sloped to promote surface drainage away from the pavement structure.

4.6.2 FLEXIBLE PAVEMENT RECOMMENDATIONS

Traffic loading information was not provided at the time of this report. Therefore, specific detailed pavement sections cannot be provided. However, we anticipate that traffic loads will be produced primarily by automobile traffic, occasional delivery and trash removal trucks, and fully loaded semi-tractor trailers. A conservative California Bearing Ratio (CBR) value of 5 was assumed for a mixture of the on-site SILTS or SANDS, or newly placed structural fill, at compaction levels of about 98 percent of the standard Proctor maximum dry density within about 3 percent of optimum moisture.

Based on our experience with similar facilities and subgrade conditions which are typical for this region, we recommend the following preliminary pavement sections. Once detailed traffic information is available, actual pavement section calculations should be performed to develop the design sections.

PAVEMENT SECTION	MATERIAL THICKNESS (in.)			TOTAL PAVEMENT SECTION (in.)
	Graded Aggregate Base	Asphalt Course INTERMEDIATE (I-19.0B)	Asphalt Course SURFACE (S-9.5B)	
Light Duty Areas	6	--	3	9
Heavy Duty Areas	8	2 ½	1 ½	12

Notes: 1) Light Duty Areas calculated based on traffic loading of 25,000 ESALS or less. Parking stalls only with no through traffic.

2) Heavy Duty Areas calculated based on traffic loading of 75,000 ESALS or less.

Actual pavement section thickness should be provided by the design civil engineer based upon anticipated traffic loads, volume, and the owner's design life requirements. The above sections represent minimum thickness representative of typical, local construction practices, and as such periodic maintenance should be anticipated.

4.6.3 RIGID PAVEMENT RECOMMENDATIONS

The use of concrete for paving has become more prevalent in recent years due to the long-term maintenance cost benefits of concrete compared to asphaltic pavements. Proper finishing of concrete pavements requires the use of appropriate construction joints to reduce the potential for cracking. Construction joints should be designed in accordance with current Portland Cement Association guidelines. Joints should be sealed to reduce the potential for water infiltration into pavement joints and subsequent infiltration into the supporting soils. The concrete should have a minimum compressive strength of 4,000 psi at 28 days. The concrete should also be designed with 5 $\pm$ 1 percent entrained air to improve workability and durability. All pavement materials and construction procedures should conform to NCDOT or appropriate city, county requirements.

Large front-loading trash dump trucks frequently impose concentrated front-wheel loads on pavements during loading. This type of loading typically results in rutting of the pavement and ultimately, pavement failures. Therefore, we recommend that the pavement in trash pickup areas consist of a minimum 6-inch graded aggregate base overlain by a minimum 7-inch thick, rigid pavement.

RIGID (CONCRETE) PAVEMENT	LIGHT-DUTY*	HEAVY-DUTY
Portland Cement Concrete (4,000 psi)	5 inches	6 inches
Graded Aggregate Base (ABC)	4 inches	6 inches

Notes: *Parking stalls only

4.7 SLOPE STABILITY ANALYSIS RESULTS

North of the proposed building is an approximately 15-foot high, 2:1 slope on which is an existing paved parking area. A pedestrian bridge is proposed to span from the parking area on top of the slope to the second floor of the proposed building. The information provided regarding the bridge did not indicate where the bridge abutment would be in relation to the slope but did state that the bridge will be supported on two columns spaced 10 feet apart and each will carry 20 kips Dead load and 20 kips Live load. The size, depth or foundation support of the columns was not provided. In addition to the bridge, a 30-foot-high communications tower will be erected. The exact location was not provided but the weight of the tower was estimated to be between 3 and 4 kips and will be supported on a 6'-9" diameter mat foundation.

Since the locations of the bridge and communication tower were not provided, and the bridge abutment type and bearing elevation were not specified, it was decided that the loading from the bridge abutment would be the critical condition. As such, the bridge abutment was modelled as a line load of 8,000 pounds per foot placed 10 feet from the crest of the slope. This loading condition should be more severe than an embedded footing or deep foundation system and more severe than the loading of the mat foundation of the communication tower. However, we still strongly recommend details regarding the bridge abutment and tower foundations be provided to confirm the slope stability analysis. The loading from the proposed building perimeter wall footing and slab-on-grade were also modelled. There is an existing retaining wall along the bottom of the slope that was modelled as being 5 feet high and embedded 2 feet below grade. The wall height, foundation dimensions and embedment depth should also be confirmed.

Short-term (undrained) and long-term (drained) conditions were analyzed. Both conditions showed a Factor of Safety greater than 1.5 which indicates the assumed loading conditions from the proposed bridge should not make the slope unstable. The slope stability Factor of Safety accounts for not only the soil conditions and slope geometry, but also the magnitude of the loading on the slope, the position of the loading, and any resisting elements such as the retaining wall embedment depth and proposed building position in relation to the slope. When the final position of the bridge abutment and communication tower are finalized, and the retaining wall embedment depth is verified, the stability of slope should be re-evaluated.

The results of and data utilized for the slope stability analysis are included in Appendix.

5 CONSTRUCTION CONSIDERATIONS

5.1 GROUNDWATER

Based on the results of the boring explorations, it appears that groundwater will not significantly impact the proposed construction. However, groundwater levels within this region tend to fluctuate with seasonal and climatic changes, and confined pockets of perched water often occur above impermeable or low permeability soils. Generally, the highest groundwater levels occur in late winter and early spring; and the lowest levels in late summer and early fall. Therefore, water may be encountered during construction at depths not indicated during this study.

If groundwater is encountered, we recommend that the groundwater table be lowered and maintained at a depth of at least 2 feet below bearing levels and excavation bottoms during construction. Adequate control of groundwater could likely be accomplished by means of pumping from gravel-lined, cased sumps. However, the contractor should be responsible for selecting the most optimal dewatering method. If a sheet pile wall is installed to cut-off the groundwater seepage into the excavation, sump and pump technique can be employed to dewater the excavation pit. Furthermore, we recommend that the Contractor determine the actual groundwater levels at the time of construction to determine the groundwater impact on the construction procedures. The contractor should be prepared to promptly remove surface water from the general construction area by similar methods. If groundwater is encountered during trenching or foundation installation, PSI should be notified so that we might determine whether there is a need for underslab drainage, perimeter drains, or other recommendations for temporary or permanent dewatering.

5.2 EXCAVATION AND SAFETY

Based on the subsurface information obtained, the anticipated excavations during site grading and construction should be able to be removed by conventional earthmoving equipment such as pans, scrapers, and backhoes.

In evaluating grading considerations, please keep in mind that subsurface conditions, particularly the level and location of bedrock (boulder or massive form) vary erratically in the Piedmont Geologic Province of which Mecklenburg County and this site are parts. If large boulders or massive rock is encountered during the grading operations between boring locations, blasting may be necessary to facilitate removal. In addition, confined excavations such as utility trenches are more likely to require rock excavation techniques than large open cuts. All excavations should be sloped or shored in accordance with applicable OSHA regulations.

In Federal Register, Volume 54, No. 209 (October 1989), the United States Department of Labor, Occupational Safety and Health Administration (OSHA) amended its “Construction Standards for Excavations, 29 CFR, Part 1926, Subpart P”. This document was issued to better allow for the safety of workers entering trenches or excavations. It is mandated by this federal regulation that excavations, whether they be utility trenches, basement excavations or footing excavations, be constructed in accordance with the new OSHA guidelines. It is our understanding that these regulations are being strictly enforced and if they are not closely followed, the owner and the Contractor could be liable for substantial penalties.

The Contractor is solely responsible for designing and constructing stable, temporary excavations and should shore, slope, or bench the sides of the excavations as required to maintain stability of both the excavation sides and bottom. The Contractor's “responsible person”, as defined in 29 CFR Part 1926, should evaluate the soil exposed in the excavations as part of the Contractor’s safety procedures. In no case should slope height, slope inclination, or excavation depth, including utility trench excavation depth, exceed those specified in all local, state, and federal safety regulations.

We are providing this information solely as a service to our client. PSI does not assume responsibility for construction site safety or the Contractor’s or other parties' compliance with local, state, and federal safety or other regulations. Groundwater control is critical to excavation safety.

6 REPORT LIMITATIONS

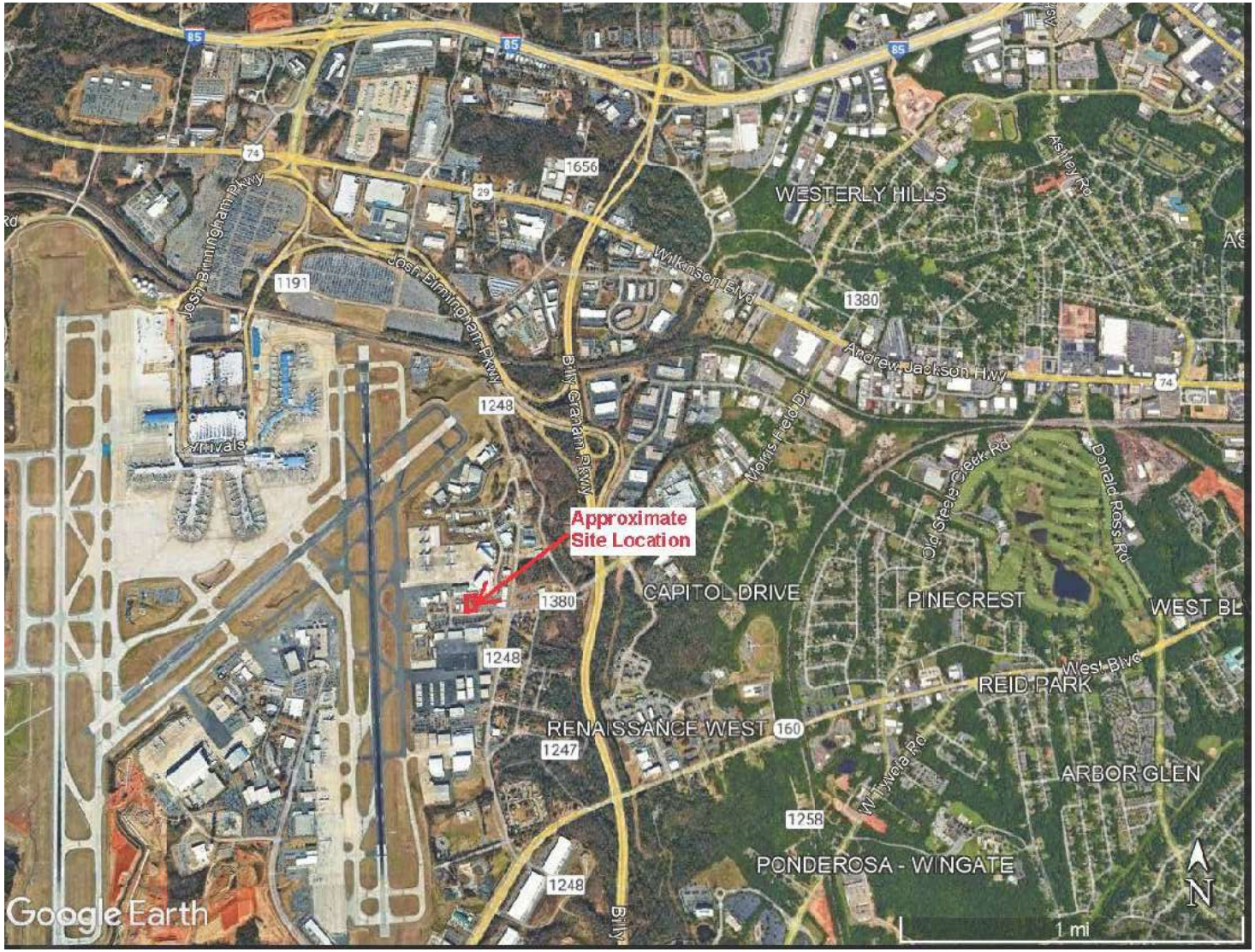
The recommendations submitted are based on the available subsurface information obtained by PSI and design details furnished by **AECOM** for the proposed project. If there are any revisions to the plans for this project or if deviations from the subsurface conditions noted in this report are encountered during construction, PSI should be notified immediately to determine if changes in the foundation recommendations are required. If PSI is not retained to perform these functions, we will not be responsible for the impact of those conditions on the geotechnical recommendations for the project.

PSI warrants that the findings, recommendations, specifications, or professional advice contained herein have been made in accordance with generally accepted professional geotechnical engineering practices in the local area at the date of this report. No other warranties are implied or expressed.

After the plans and specifications are more complete, PSI should be retained and provided the opportunity to review the final design plans and specifications to check that our engineering recommendations have been properly incorporated into the design documents. At that time, it may be necessary to submit supplementary recommendations. This report has been prepared for the exclusive use of **AECOM** and their consultants for the specific application to the **Proposed Construct Security Forces Facility to be located at the North Carolina Air National Guard (NCANG) base at Charlotte Douglass International Airport in Charlotte, North Carolina**.

APPENDICES

SITE VICINITY MAP



Project Name:

Proposed New Security Forces Building
North Carolina ANG
Charlotte, North Carolina

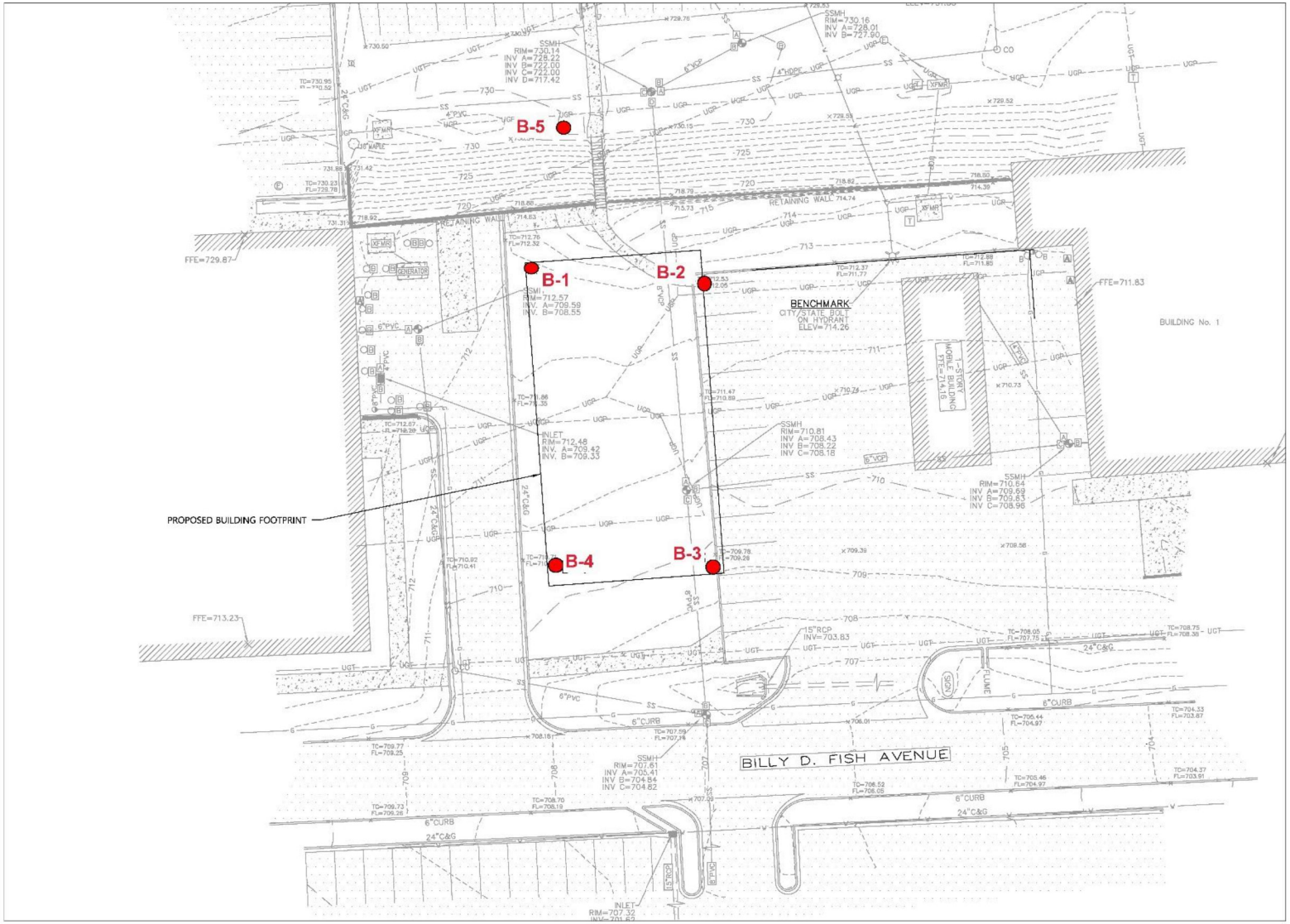
2021 Base Aerial Obtained From Google Earth

Project No.:	**Date:**
05111037	**February 2023**

Figure 1
Site Vicinity Map

intertek psi

BORING LOCATION PLAN



NORTH

Legend

● Approximate Boring Location

Project Name: **Proposed New Security Forces Building** **North Carolina ANG** **Charlotte, North Carolina**		**Base Drawing (Sheet B01)** **Prepared by AECOM, undated**	**Approximate Scale** **0 — 52 feet**
Project No.: **05111037**	**Date:** **February 2023**	**Figure 2** **Boring Location Plan**	intertek psi

GENERAL NOTES AND SOIL CLASSIFICATION CHART

GENERAL NOTES

SAMPLE IDENTIFICATION

The Unified Soil Classification System (USCS), AASHTO 1988 and ASTM designations D2487 and D-2488 are used to identify the encountered materials unless otherwise noted. Coarse-grained soils are defined as having more than 50% of their dry weight retained on a #200 sieve (0.075mm); they are described as: boulders, cobbles, gravel or sand. Fine-grained soils have less than 50% of their dry weight retained on a #200 sieve; they are defined as silts or clay depending on their Atterberg Limit attributes. Major constituents may be added as modifiers and minor constituents may be added according to the relative proportions based on grain size.

DRILLING AND SAMPLING SYMBOLS

SFA: Solid Flight Auger - typically 4" diameter flights, except where noted.
HSA: Hollow Stem Auger - typically 3¼" or 4¼ I.D. openings, except where noted.
M.R.: Mud Rotary - Uses a rotary head with Bentonite or Polymer Slurry
R.C.: Diamond Bit Core Sampler
H.A.: Hand Auger
P.A.: Power Auger - Handheld motorized auger

SS: Split-Spoon - 1 3/8" I.D., 2" O.D., except where noted.
ST: Shelby Tube - 3" O.D., except where noted.
RC: Rock Core
TC: Texas Cone
BS: Bulk Sample
PM: Pressuremeter
CPT-U: Cone Penetrometer Testing with Pore-Pressure Readings

SOIL PROPERTY SYMBOLS

N: Standard "N" penetration: Blows per foot of a 140 pound hammer falling 30 inches on a 2-inch O.D. Split-Spoon.
N_{60}: A "N" penetration value corrected to an equivalent 60% hammer energy transfer efficiency (ETR)
Q_u: Unconfined compressive strength, TSF
Q_p: Pocket penetrometer value, unconfined compressive strength, TSF
w%: Moisture/water content, %
LL: Liquid Limit, %
PL: Plastic Limit, %
PI: Plasticity Index = (LL-PL),%
DD: Dry unit weight, pcf
▼,▽,▼ Apparent groundwater level at time noted

RELATIVE DENSITY OF COARSE-GRAINED SOILS

Relative Density	N - Blows/foot
Very Loose	0 - 4
Loose	4 - 10
Medium Dense	10 - 30
Dense	30 - 50
Very Dense	50 - 80
Extremely Dense	80+

ANGULARITY OF COARSE-GRAINED PARTICLES

Description	Criteria
Angular:	Particles have sharp edges and relatively plane sides with unpolished surfaces
Subangular:	Particles are similar to angular description, but have rounded edges
Subrounded:	Particles have nearly plane sides, but have well-rounded corners and edges
Rounded:	Particles have smoothly curved sides and no edges

GRAIN-SIZE TERMINOLOGY

Component	Size Range
Boulders:	Over 300 mm (>12 in.)
Cobbles:	75 mm to 300 mm (3 in. to 12 in.)
Coarse-Grained Gravel:	19 mm to 75 mm (¾ in. to 3 in.)
Fine-Grained Gravel:	4.75 mm to 19 mm (No.4 to ¾ in.)
Coarse-Grained Sand:	2 mm to 4.75 mm (No.10 to No.4)
Medium-Grained Sand:	0.42 mm to 2 mm (No.40 to No.10)
Fine-Grained Sand:	0.075 mm to 0.42 mm (No. 200 to No.40)
Silt:	0.005 mm to 0.075 mm
Clay:	<0.005 mm

PARTICLE SHAPE

Description	Criteria
Flat:	Particles with width/thickness ratio > 3
Elongated:	Particles with length/width ratio > 3
Flat & Elongated:	Particles meet criteria for both flat and elongated

RELATIVE PROPORTIONS OF FINES

Descriptive Term	% Dry Weight
Trace:	< 5%
With:	5% to 12%
Modifier:	>12%

GENERAL NOTES

(Continued)

CONSISTENCY OF FINE-GRAINED SOILS

Q_U - TSF	N - Blows/foot	Consistency
0 - 0.25	0 - 2	Very Soft
0.25 - 0.50	2 - 4	Soft
0.50 - 1.00	4 - 8	Firm (Medium Stiff)
1.00 - 2.00	8 - 15	Stiff
2.00 - 4.00	15 - 30	Very Stiff
4.00 - 8.00	30 - 50	Hard
8.00+	50+	Very Hard

MOISTURE CONDITION DESCRIPTION

Description	Criteria
Dry:	Absence of moisture, dusty, dry to the touch
Moist:	Damp but no visible water
Wet:	Visible free water, usually soil is below water table

RELATIVE PROPORTIONS OF SAND AND GRAVEL

Descriptive Term	% Dry Weight
Trace:	< 15%
With:	15% to 30%
Modifier:	>30%

STRUCTURE DESCRIPTION

Description	Criteria
Stratified:	Alternating layers of varying material or color with layers at least ¼-inch (6 mm) thick
Laminated:	Alternating layers of varying material or color with layers less than ¼-inch (6 mm) thick
Fissured:	Breaks along definite planes of fracture with little resistance to fracturing
Slickensided:	Fracture planes appear polished or glossy, sometimes striated
Blocky:	Cohesive soil that can be broken down into small angular lumps which resist further breakdown
Lensed:	Inclusion of small pockets of different soils
Layer:	Inclusion greater than 3 inches thick (75 mm)
Seam:	Inclusion 1/8-inch to 3 inches (3 to 75 mm) thick extending through the sample
Parting:	Inclusion less than 1/8-inch (3 mm) thick

SCALE OF RELATIVE ROCK HARDNESS

Q_U - TSF	Consistency
2.5 - 10	Extremely Soft
10 - 50	Very Soft
50 - 250	Soft
250 - 525	Medium Hard
525 - 1,050	Moderately Hard
1,050 - 2,600	Hard
>2,600	Very Hard

ROCK BEDDING THICKNESSES

Description	Criteria
Very Thick Bedded	Greater than 3-foot (>1.0 m)
Thick Bedded	1-foot to 3-foot (0.3 m to 1.0 m)
Medium Bedded	4-inch to 1-foot (0.1 m to 0.3 m)
Thin Bedded	1¼-inch to 4-inch (30 mm to 100 mm)
Very Thin Bedded	½-inch to 1¼-inch (10 mm to 30 mm)
Thickly Laminated	1/8-inch to ½-inch (3 mm to 10 mm)
Thinly Laminated	1/8-inch or less "paper thin" (<3 mm)

ROCK VOIDS

Voids	Void Diameter
Pit	<6 mm (<0.25 in)
Vug	6 mm to 50 mm (0.25 in to 2 in)
Cavity	50 mm to 600 mm (2 in to 24 in)
Cave	>600 mm (>24 in)

GRAIN-SIZED TERMINOLOGY

(Typically Sedimentary Rock)

Component	Size Range
Very Coarse Grained	>4.76 mm
Coarse Grained	2.0 mm - 4.76 mm
Medium Grained	0.42 mm - 2.0 mm
Fine Grained	0.075 mm - 0.42 mm
Very Fine Grained	<0.075 mm

ROCK QUALITY DESCRIPTION

Rock Mass Description	RQD Value
Excellent	90 -100
Good	75 - 90
Fair	50 - 75
Poor	25 -50
Very Poor	Less than 25

DEGREE OF WEATHERING

Slightly Weathered:	Rock generally fresh, joints stained and discoloration extends into rock up to 25 mm (1 in), open joints may contain clay, core rings under hammer impact.
Weathered:	Rock mass is decomposed 50% or less, significant portions of the rock show discoloration and weathering effects, cores cannot be broken by hand or scraped by knife.
Highly Weathered:	Rock mass is more than 50% decomposed, complete discoloration of rock fabric, core may be extremely broken and gives clunk sound when struck by hammer, may be shaved with a knife.

SOIL CLASSIFICATION CHART

NOTE: DUAL SYMBOLS ARE USED TO INDICATE BORDERLINE SOIL CLASSIFICATIONS

MAJOR DIVISIONS			SYMBOLS		TYPICAL DESCRIPTIONS
			GRAPH	LETTER	
COARSE GRAINED SOILS MORE THAN 50% OF MATERIAL IS LARGER THAN NO. 200 SIEVE SIZE	GRAVEL AND GRAVELLY SOILS MORE THAN 50% OF COARSE FRACTION RETAINED ON NO. 4 SIEVE	CLEAN GRAVELS		GW	WELL-GRADED GRAVELS, GRAVEL - SAND MIXTURES, LITTLE OR NO FINES
		(LITTLE OR NO FINES)		GP	POORLY-GRADED GRAVELS, GRAVEL - SAND MIXTURES, LITTLE OR NO FINES
		GRAVELS WITH FINES		GM	SILTY GRAVELS, GRAVEL - SAND - SILT MIXTURES
		(APPRECIABLE AMOUNT OF FINES)		GC	CLAYEY GRAVELS, GRAVEL - SAND - CLAY MIXTURES
	SAND AND SANDY SOILS MORE THAN 50% OF COARSE FRACTION PASSING ON NO. 4 SIEVE	CLEAN SANDS		SW	WELL-GRADED SANDS, GRAVELLY SANDS, LITTLE OR NO FINES
		(LITTLE OR NO FINES)		SP	POORLY-GRADED SANDS, GRAVELLY SAND, LITTLE OR NO FINES
		SANDS WITH FINES		SM	SILTY SANDS, SAND - SILT MIXTURES
		(APPRECIABLE AMOUNT OF FINES)		SC	CLAYEY SANDS, SAND - CLAY MIXTURES
FINE GRAINED SOILS MORE THAN 50% OF MATERIAL IS SMALLER THAN NO. 200 SIEVE SIZE	SILTS AND CLAYS	LIQUID LIMIT LESS THAN 50		ML	INORGANIC SILTS AND VERY FINE SANDS, ROCK FLOUR, SILTY OR CLAYEY FINE SANDS OR CLAYEY SILTS WITH SLIGHT PLASTICITY
				CL	INORGANIC CLAYS OF LOW TO MEDIUM PLASTICITY, GRAVELLY CLAYS, SANDY CLAYS, SILTY CLAYS, LEAN CLAYS
				OL	ORGANIC SILTS AND ORGANIC SILTY CLAYS OF LOW PLASTICITY
	SILTS AND CLAYS	LIQUID LIMIT GREATER THAN 50		MH	INORGANIC SILTS, MICACEOUS OR DIATOMACEOUS FINE SAND OR SILTY SOILS
				CH	INORGANIC CLAYS OF HIGH PLASTICITY
				OH	ORGANIC CLAYS OF MEDIUM TO HIGH PLASTICITY, ORGANIC SILTS
HIGHLY ORGANIC SOILS				PT	PEAT, HUMUS, SWAMP SOILS WITH HIGH ORGANIC CONTENTS

psi

BORING LOGS

BORING B-1

DATE STARTED:	2/23/23	**DRILL COMPANY:**	HPC
DATE COMPLETED:	2/23/23	**DRILLER:** Price	**LOGGED BY:** Steege
COMPLETION DEPTH	35.0 ft	**DRILL RIG:**	CME 550
BENCHMARK:	N/A	**DRILLING METHOD:**	Hollow Stem Auger
ELEVATION:	713 ft	**SAMPLING METHOD:**	2-in SS, Standard
LATITUDE:		**HAMMER TYPE:**	Automatic
LONGITUDE:		**EFFICIENCY**	N/A
STATION: N/A	**OFFSET:** N/A	**REVIEWED BY:**	AOS

Water

While Drilling	32	feet
Upon Completion Dry, CID=15		feet
Delay	N/A	

BORING LOCATION:
See Boring Location Plan

REMARKS: Borehole backfilled with the auger cuttings upon completion. CID = Cave-In Depth

Elevation (feet)	Depth, (feet)	Sample No.	Recovery (inches)	MATERIAL DESCRIPTION	USCS Classification	SPT Blows per 6-inch (SS)	Moisture, %	Additional Remarks
	0			**TOPSOIL** (4 inches)				
710		1	16	**RESIDUUM** - Firm, Red/Brown, Elastic SILT - Moist	MH	3-2-3 N=5	41	LL = 63 PL = 44 Fines = 97.1%
	5	2	18			3-3-4 N=7		
705		3	18	Firm, Brown/Red, Sandy Elastic SILT with Mica - Moist	MH	3-3-5 N=8	33	LL = 53 PL = 43 Fines = 62.7
	10	4	16			2-2-3 N=5		
700		5	18	Soft, Brown/Gray, Fine Sandy SILT with Mica - Moist to Wet	ML	1-2-2 N=4		
695	15	6	18			1-2-2 N=4		
690	20	7	18			0-2-2 N=4		
685	25	8	18			2-2-2 N=4		
680	30	9	16	Medium Dense, Brown/Gray, Silty SAND with Mica - Wet	SM	6-6-4 N=10		
	35			Boring terminated at 35 feet.				

STANDARD PENETRATION TEST DATA
N in blows/ft ◎
× Moisture ◪ PL ✚ LL
0 25 50
STRENGTH, tsf
▲ Qu ✳ Qp
0 2.0 4.0

intertek psi
Professional Service Industries, Inc.
5021-A West W.T. Harris Boulevard
Charlotte, NC 28269
Telephone: (704) 598-2234

PROJECT NO.: 05111037
PROJECT: Construct Security Forces Facility
LOCATION: NCANG
Charlotte Douglas International Airport
Charlotte, North Carolina

The stratification lines represent approximate boundaries. The transition may be gradual.

BORING B-2

DATE STARTED:	2/23/23	**DRILL COMPANY:**	HPC
DATE COMPLETED:	2/23/23	**DRILLER:** Price	**LOGGED BY:** Steege
COMPLETION DEPTH	35.0 ft	**DRILL RIG:**	CME 550
BENCHMARK:	N/A	**DRILLING METHOD:**	Hollow Stem Auger
ELEVATION:	712 ft	**SAMPLING METHOD:**	2-in SS, Standard
LATITUDE:		**HAMMER TYPE:**	Automatic
LONGITUDE:		**EFFICIENCY**	N/A
STATION: N/A	**OFFSET:** N/A	**REVIEWED BY:**	AOS

Water

While Drilling	21	feet
Upon Completion	15.5	feet
Delay	N/A	

BORING LOCATION:
See Boring Location Plan

REMARKS: Borehole backfilled with the auger cuttings upon completion.

Elevation (feet)	Depth, (feet)	Sample No.	Recovery (inches)	MATERIAL DESCRIPTION	USCS Classification	SPT Blows per 6-inch (SS)	Moisture, %	Additional Remarks
	0			**ASPHALT** (2 inches)				
				GRAVEL (6 inches)				
710		1	16	**RESIDUUM** - Stiff, Red/Brown, Elastic SILT - Moist	MH	3-4-7 N=11		
				Firm, Red/Tan, Sandy SILT with Clay - Moist				
	5	2	14		ML	3-3-5 N=8		
705		3	15			2-2-3 N=5		
				Soft to Firm, Brown/Gray, Fine Sandy SILT - Moist				
	10	4	16			2-2-2 N=4		
700								
		5	18		ML	2-2-3 N=5		
	15							
695								
		6	18			2-3-4 N=7		
	20							
690				Firm to Stiff, Brown/Gray, Sandy SILT - Wet				
		7	18			2-2-3 N=5		
	25							
685					ML			
		8	18			2-2-4 N=6		
	30							
680								
		9	18			5-4-5 N=9		
	35			Boring terminated at 35 feet.				

STANDARD PENETRATION TEST DATA
N in blows/ft ◎
× Moisture ◪ PL ✚ LL
0 25 50
STRENGTH, tsf
▲ Qu ✳ Qp
0 2.0 4.0

intertek psi
Professional Service Industries, Inc.
5021-A West W.T. Harris Boulevard
Charlotte, NC 28269
Telephone: (704) 598-2234

PROJECT NO.: 05111037
PROJECT: Construct Security Forces Facility
LOCATION: NCANG
Charlotte Douglas International Airport
Charlotte, North Carolina

The stratification lines represent approximate boundaries. The transition may be gradual.

BORING B-3

DATE STARTED:	2/23/23	**DRILL COMPANY:**	HPC
DATE COMPLETED:	2/23/23	**DRILLER:** Price	**LOGGED BY:** Steege
COMPLETION DEPTH	30.0 ft	**DRILL RIG:**	CME 550
BENCHMARK:	N/A	**DRILLING METHOD:**	Hollow Stem Auger
ELEVATION:	709 ft	**SAMPLING METHOD:**	2-in SS, Standard
LATITUDE:		**HAMMER TYPE:**	Automatic
LONGITUDE:		**EFFICIENCY**	N/A
STATION: N/A	**OFFSET:** N/A	**REVIEWED BY:**	AOS

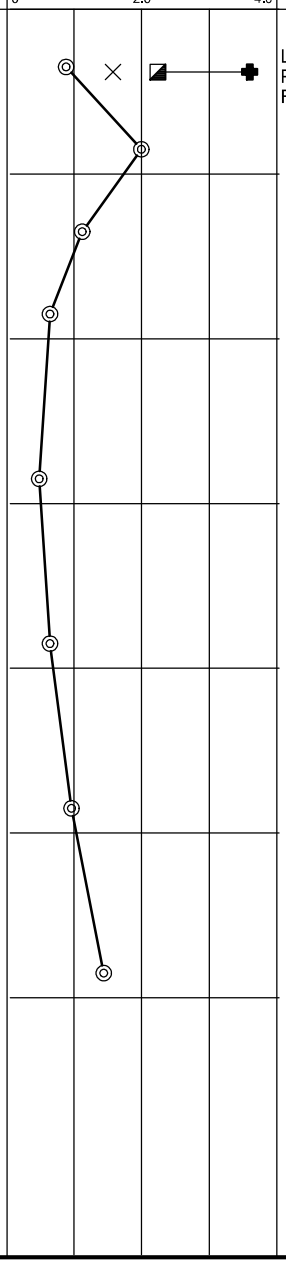
Water

While Drilling	17	feet
Upon Completion	18	feet
5 Hr Delay	14.5	feet

BORING LOCATION:
See Boring Location Plan

REMARKS: Borehole backfilled with the auger cuttings prior to site departure.

Elevation (feet)	Depth, (feet)	Sample No.	Recovery (inches)	MATERIAL DESCRIPTION	USCS Classification	SPT Blows per 6-inch (SS)	Moisture, %	Additional Remarks
	0			**TOPSOIL** (5 inches)				
		1	16	**RESIDUUM** - Stiff to Very Stiff, Red/Brown/Tan, Sandy SILT with Clay - Moist	ML	3-5-6 N=11	20	LL = 45 PL = 28 Fines = 69.1%
705	5	2	18			7-11-14 N=25		
		3	18	Stiff to Firm, Tan/Brown, Sandy SILT with Clay - Moist	ML	6-7-7 N=14		
700	10	4	18			3-3-5 N=8		
				Firm, Brown/Tan, Fine Sandy SILT with Mica - Moist	ML			
695	15	5	18			2-3-3 N=6		
				Firm to Stiff, Brown, Sandy SILT - Wet	ML			
690	20	6	18			2-4-4 N=8		
685	25	7	18			2-5-7 N=12		
				Very Stiff, Brown, Sandy SILT - Moist to Wet	ML			
680	30	8	18			4-8-10 N=18		
				Boring terminated at 30 feet.				



intertek psi

Professional Service Industries, Inc.
5021-A West W.T. Harris Boulevard
Charlotte, NC 28269
Telephone: (704) 598-2234

PROJECT NO.: 05111037
PROJECT: Construct Security Forces Facility
LOCATION: NCANG
Charlotte Douglas International Airport
Charlotte, North Carolina

The stratification lines represent approximate boundaries. The transition may be gradual.

BORING B-4

DATE STARTED:	2/23/23	**DRILL COMPANY:**	HPC
DATE COMPLETED:	2/23/23	**DRILLER:** Price	**LOGGED BY:** Steege
COMPLETION DEPTH	30.0 ft	**DRILL RIG:**	CME 550
BENCHMARK:	N/A	**DRILLING METHOD:**	Hollow Stem Auger
ELEVATION:	710 ft	**SAMPLING METHOD:**	2-in SS, Standard
LATITUDE:		**HAMMER TYPE:**	Automatic
LONGITUDE:		**EFFICIENCY**	N/A
STATION: N/A	**OFFSET:** N/A	**REVIEWED BY:**	AOS

Water

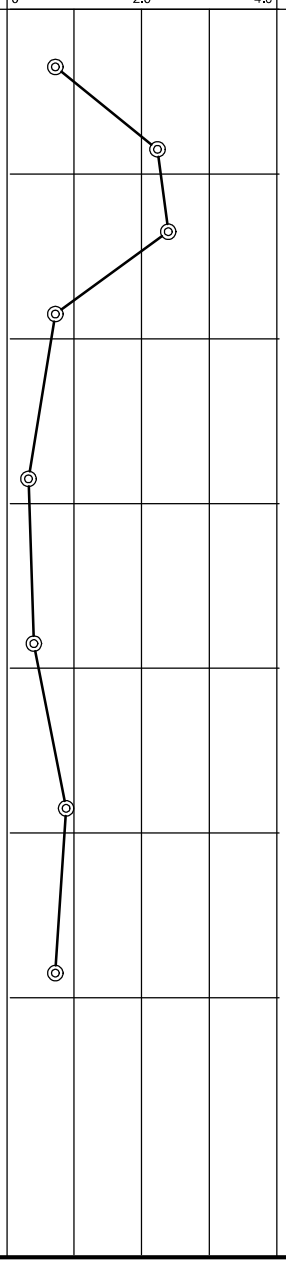
While Drilling	19	feet
Upon Completion	12.5	feet
Delay	N/A	

BORING LOCATION:
See Boring Location Plan

REMARKS: Borehole backfilled with the auger cuttings upon completion.

Elevation (feet)	Depth, (feet)	Sample No.	Recovery (inches)	MATERIAL DESCRIPTION	USCS Classification	SPT Blows per 6-inch (SS)	Moisture, %	Additional Remarks
	0			**TOPSOIL WITH GRAVEL** (3 inches)	MH			
		1	12	**FILL** - Red/Brown, Elastic SILT with some gravel - Moist **RESIDUUM** - Stiff to Very Stiff, Red/Brown, Elastic SILT - Moist		4-4-5 N=9		
705	5	2	16		MH	7-12-16 N=28		
		3	18			13-14-16 N=30		
700	10	4	18	Stiff, Brown/Tan, Sandy SILT with Clay - Moist	ML	4-4-5 N=9		
695	15	5	16	Very Loose, Brown/Gray, Silty SAND - Moist to Wet	SM	2-2-2 N=4		
690	20	6	18	Loose and Medium Dense, Brown/Gray, Silty SAND - Wet		2-2-3 N=5		
685	25	7	18		SM	2-4-7 N=11		
680	30	8	18			2-4-5 N=9		
				Boring terminated at 30 feet.				

STANDARD PENETRATION TEST DATA
N in blows/ft ◎
× Moisture ◪ PL ✚ LL
0 25 50
STRENGTH, tsf
▲ Qu ✳ Qp
0 2.0 4.0



intertek psi

Professional Service Industries, Inc.
5021-A West W.T. Harris Boulevard
Charlotte, NC 28269
Telephone: (704) 598-2234

PROJECT NO.: 05111037
PROJECT: Construct Security Forces Facility
LOCATION: NCANG
Charlotte Douglas International Airport
Charlotte, North Carolina

The stratification lines represent approximate boundaries. The transition may be gradual.

BORING B-5

DATE STARTED:	2/23/23	**DRILL COMPANY:**	HPC
DATE COMPLETED:	2/23/23	**DRILLER:** Price	**LOGGED BY:** Steege
COMPLETION DEPTH	30.0 ft	**DRILL RIG:**	CME 550
BENCHMARK:	N/A	**DRILLING METHOD:**	Hollow Stem Auger
ELEVATION:	730 ft	**SAMPLING METHOD:**	2-in SS, Standard
LATITUDE:		**HAMMER TYPE:**	Automatic
LONGITUDE:		**EFFICIENCY**	N/A
STATION: N/A	**OFFSET:** N/A	**REVIEWED BY:**	AOS

Water

While Drilling	None
Upon Completion	Dry
Delay	N/A

BORING LOCATION:
See Boring Location Plan

REMARKS: Borehole backfilled with the auger cuttings upon completion.

Elevation (feet)	Depth, (feet)	Sample No.	Recovery (inches)	MATERIAL DESCRIPTION	USCS Classification	SPT Blows per 6-inch (SS)	Moisture, %	Additional Remarks
	0			**TOPSOIL** (4 1/2 inches)				
		1	8	**RESIDUUM** - Soft to Firm, Red/Brown, Elastic SILT - Moist	MH	2-2-2 N=4	31	
725	5	2	12			2-3-3 N=6	30	
		3	15	Stiff and Firm, Red/Brown, Elastic SILT - Moist	MH	3-5-5 N=10	28	LL = 54 PL = 39 Fines = 74.4%
720	10	4	14			2-3-3 N=6		
715	15	5	16			3-4-7 N=11		
				Firm, Brown, Sandy SILT with Mica - Moist	ML			
710	20	6	18			2-4-4 N=8		
705	25	7	15			2-3-3 N=6		
700	30	8	18			2-2-3 N=5		
				Boring terminated at 30 feet.				

STANDARD PENETRATION TEST DATA
N in blows/ft ◎
× Moisture ◪ PL ✚ LL
0 25 50

STRENGTH, tsf
▲ Qu ✳ Qp
0 2.0 4.0

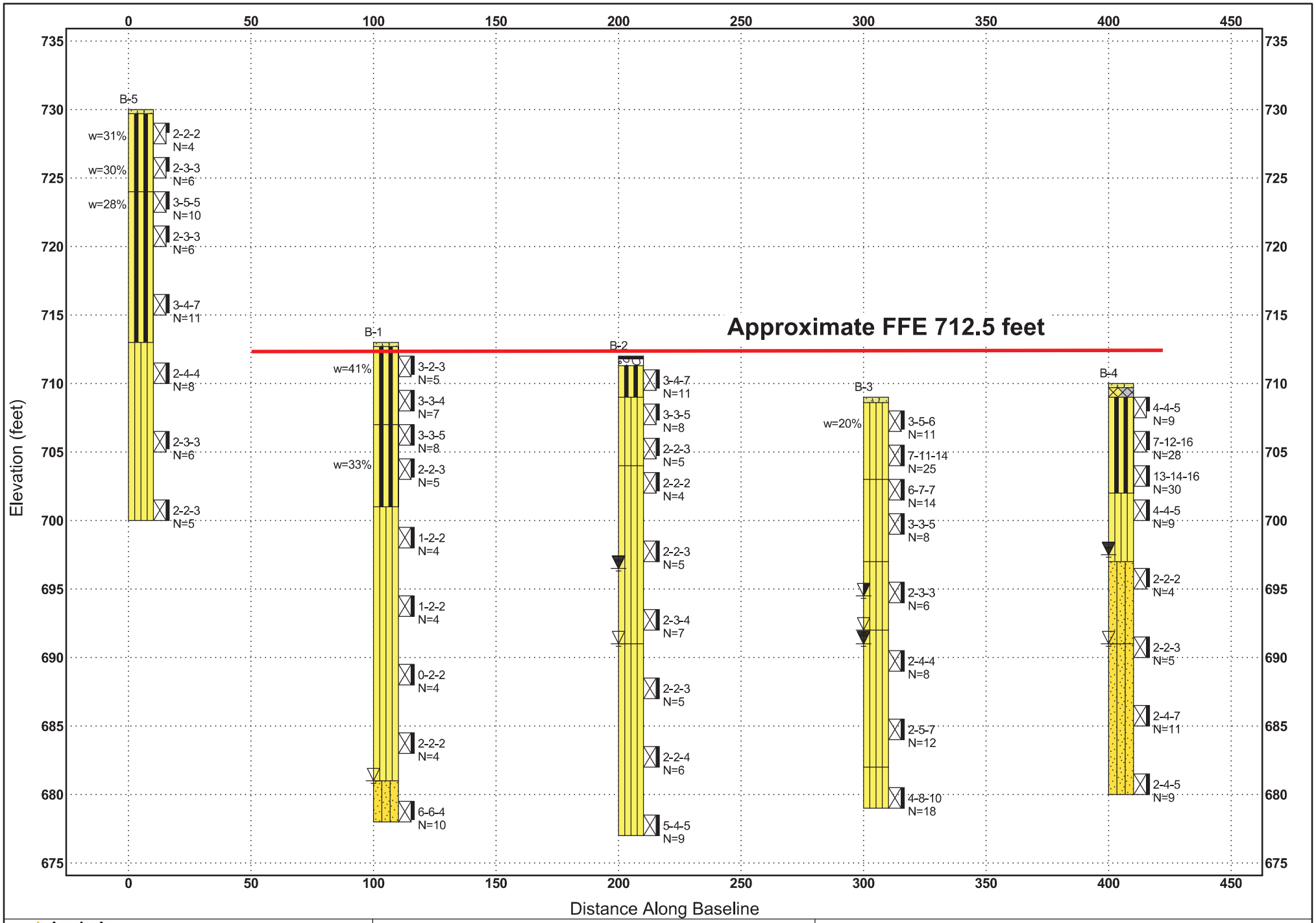
intertek psi

Professional Service Industries, Inc.
5021-A West W.T. Harris Boulevard
Charlotte, NC 28269
Telephone: (704) 598-2234

PROJECT NO.: 05111037
PROJECT: Construct Security Forces Facility
LOCATION: NCANG
Charlotte Douglas International Airport
Charlotte, North Carolina

The stratification lines represent approximate boundaries. The transition may be gradual.

BORING SUMMARY



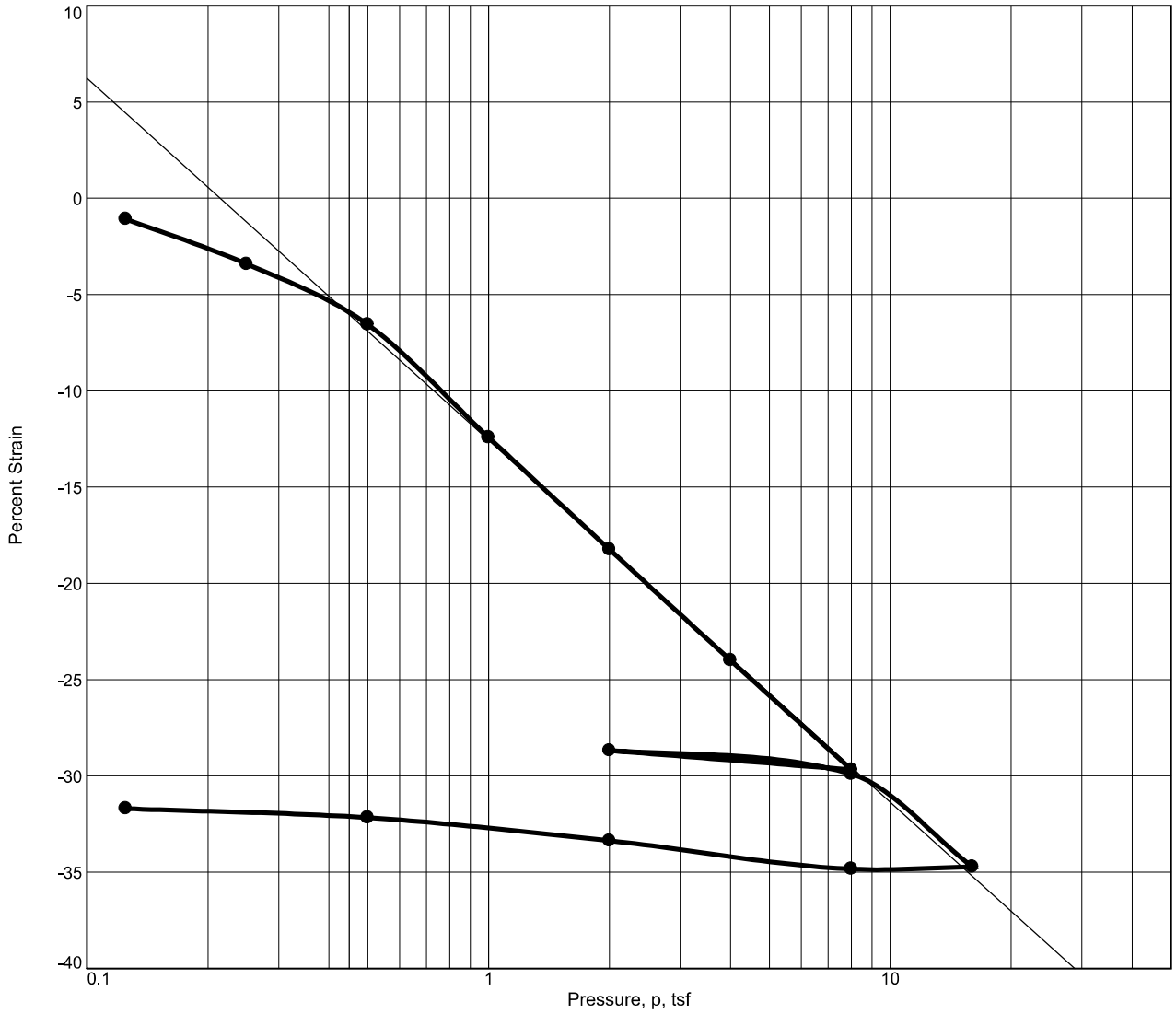
intertek psi
Professional Service Industries, Inc.
5021-A West W.T. Harris Boulevard
Charlotte, NC 28269
Telephone: (704) 598-2234

Boring Summary

Construct Security Forces Facility
PSI Project Number: 05111037

LABORATORY TEST RESULTS

CONSOLIDATION TEST REPORT



SUMMARY OF TEST RESULTS

	DRY DENSITY (pcf)	MOISTURE CONTENT, (%)	SATURATION (%)	VOID RATIO	SPECIFIC GRAVITY	OVERBURDEN (pcf)	P_C (pcf)	C_C	SWELL PRESS. (pcf)
INITIAL	72.4	32.7	66.5	1.335	2.710	.365	0.44	0.44	
FINAL		23.4	20.6	0.595					

Source of Sample: B-1 **Depth:** 8.0'-10.0' **Sample Number:** UD-1
Material Description: Moist Stiff Sandy Elastic SILT w/ Clay **USCS:** MH **AASHTO:** A-5(7)
Remarks: 62.7% Fines / LL 53 / PL 43 / PI 10

Professional Service Industries, Inc.
5021 W. W.T. Harris Blvd.
Charlotte, NC

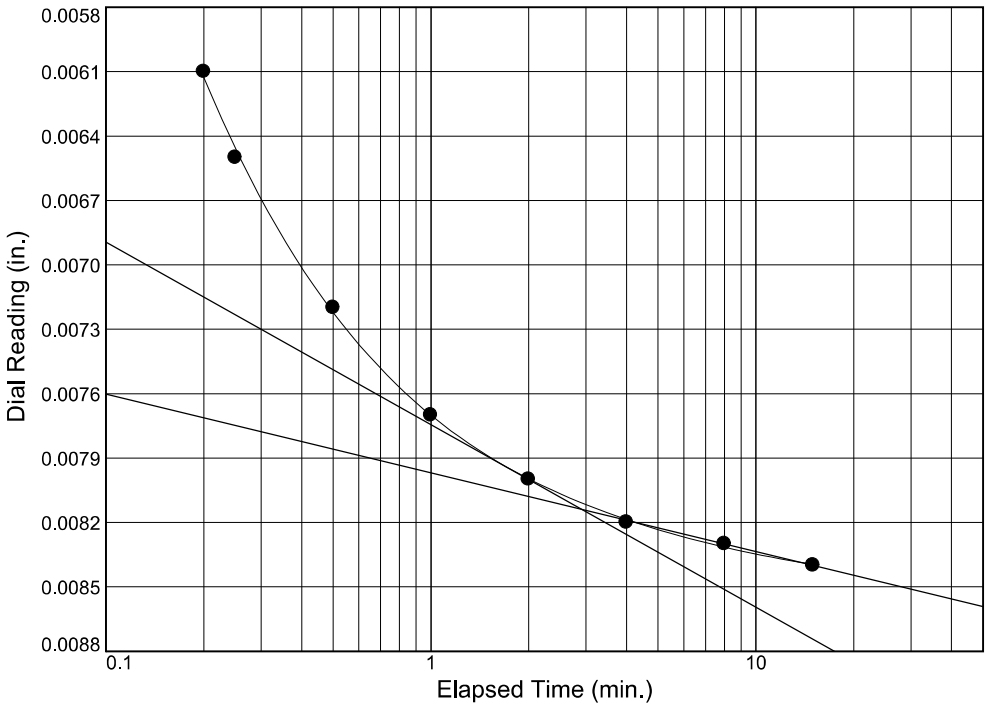
Client: Intertek-PSI
Project: NCANG
Project No.: 05111037 **Figure** 1

Checked By: AS

Dial Reading vs. Time

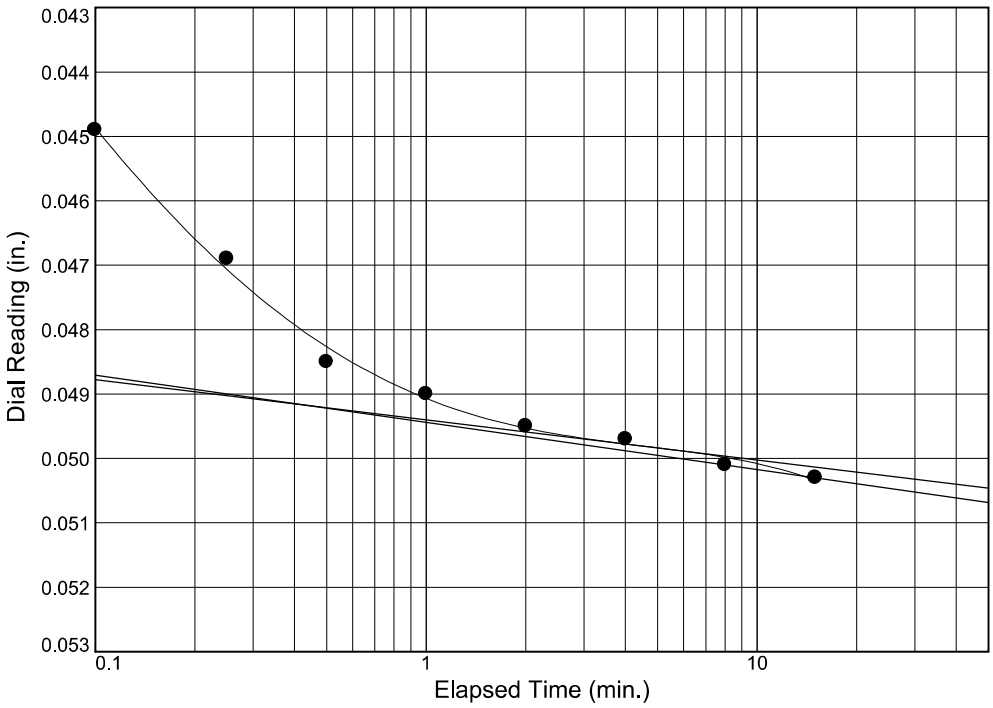
Project No.: 05111037
Project: NCANG

Source of Sample: B-1 Depth: 8.0'-10.0' Sample Number: UD-1



Load No.= 1
Load= 0.13 tsf
D_0 = 0.0000
D_{50} = 0.0041
D_{100} = 0.0081
T_{50} =

C_α = 0.001



Load No.= 3
Load= 0.50 tsf
D_0 = 0.0260
D_{50} = 0.0376
D_{100} = 0.0492
T_{50} =

C_α = 0.002

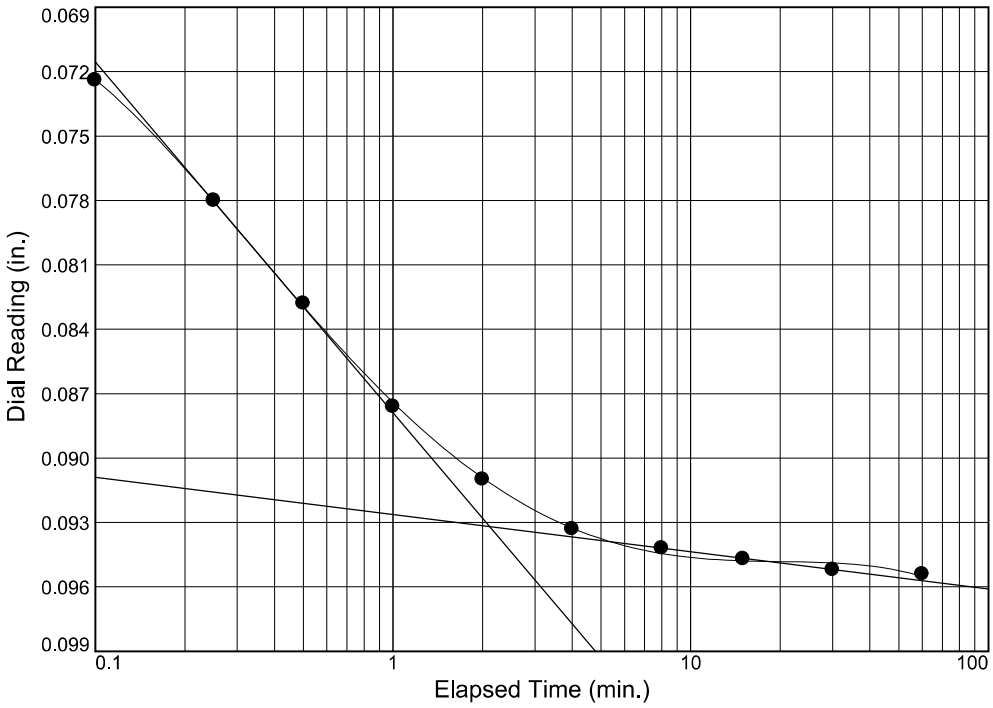
Figure 2

Professional Service Industries, Inc.

Dial Reading vs. Time

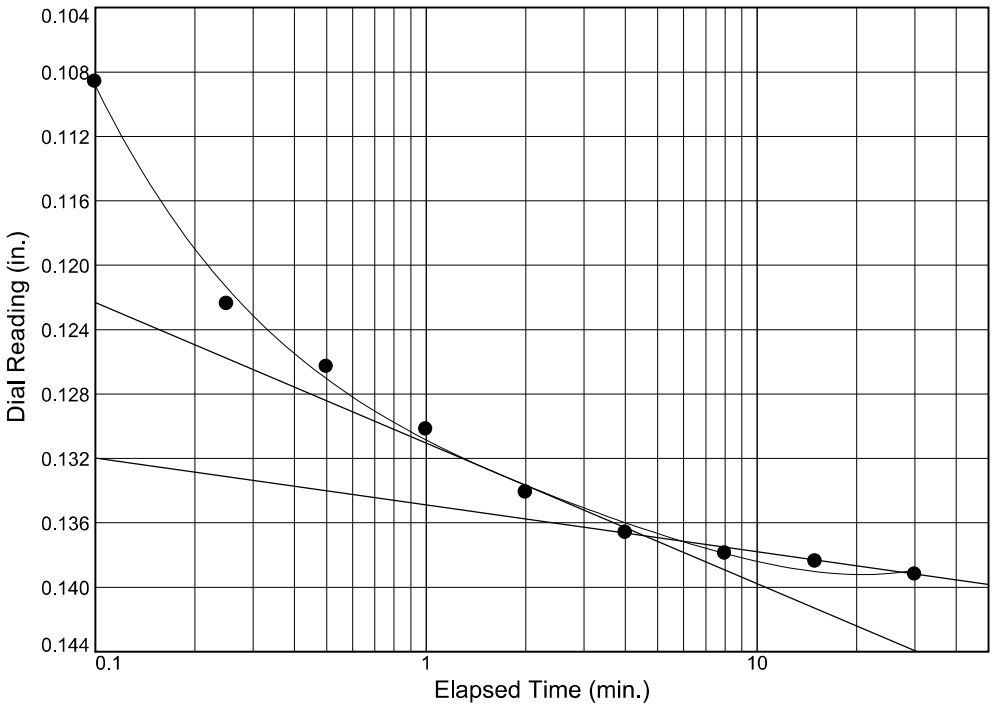
Project No.: 05111037
Project: NCANG

Source of Sample: B-1 Depth: 8.0'-10.0' Sample Number: UD-1



Load No.= 4
Load= 1.00 tsf
D_0 = 0.0503
D_{50} = 0.0718
D_{100} = 0.0932
T_{50} =

C_α = 0.005



Load No.= 5
Load= 2.00 tsf
D_0 = 0.0954
D_{50} = 0.1161
D_{100} = 0.1368
T_{50} = 0.16 min.

C_v @ T_{50}
4.982 ft.^{2}/day

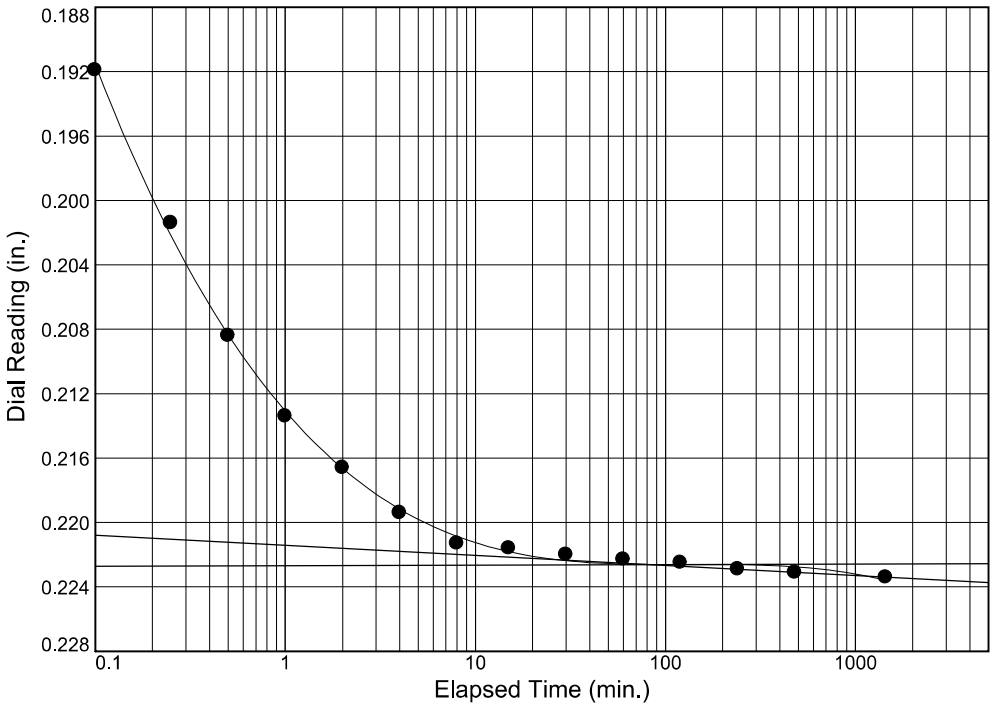
C_α = 0.009

Figure 3

Dial Reading vs. Time

Project No.: 05111037
Project: NCANG

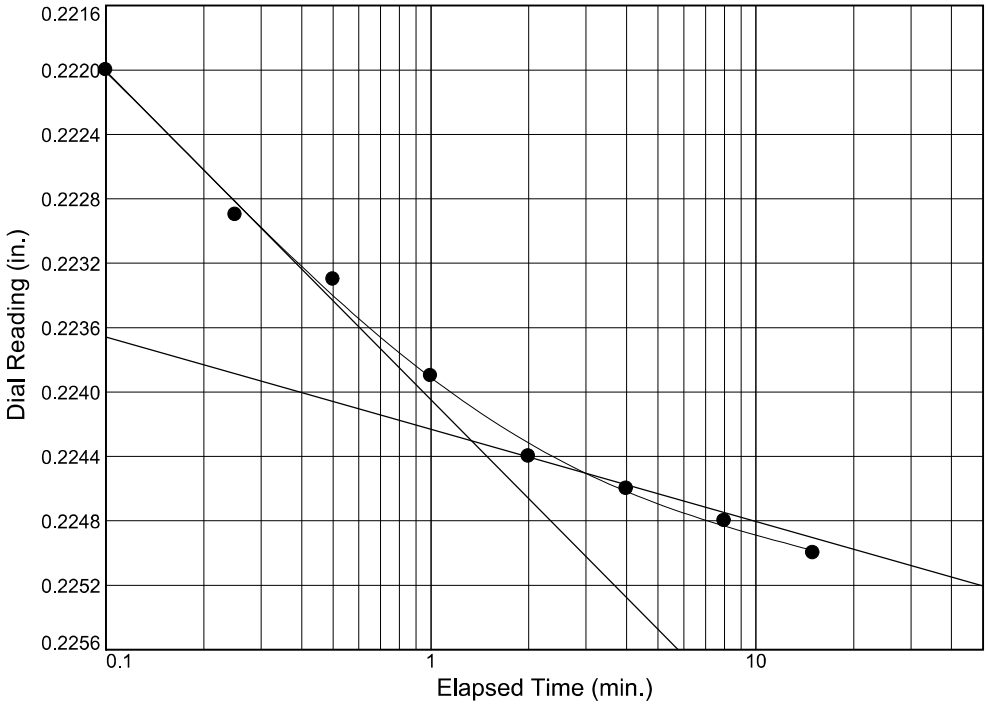
Source of Sample: B-1 Depth: 8.0'-10.0' Sample Number: UD-1



Load No.= 7
Load= 8.00 tsf
D_0 = 0.1814
D_{50} = 0.2020
D_{100} = 0.2226
T_{50} = 0.25 min.

C_v @ T_{50}
2.403 ft.^{2}/day

C_α = 0.002



Load No.= 9
Load= 8.00 tsf
D_0 = 0.2141
D_{50} = 0.2192
D_{100} = 0.2243
T_{50} =

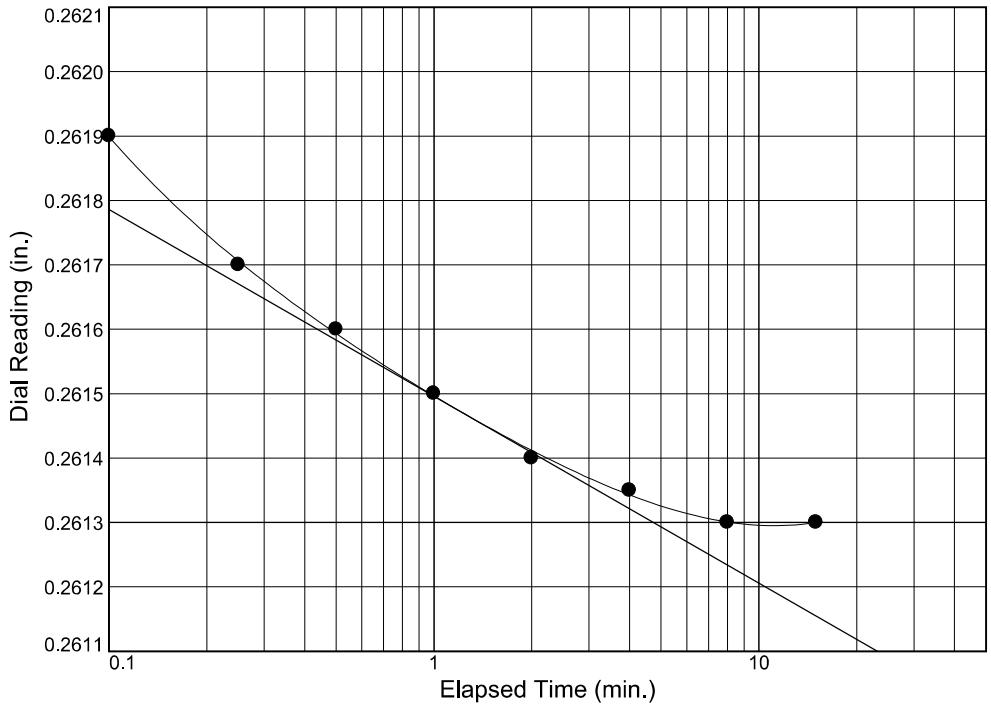
C_α = 0.002

Figure 4

Dial Reading vs. Time

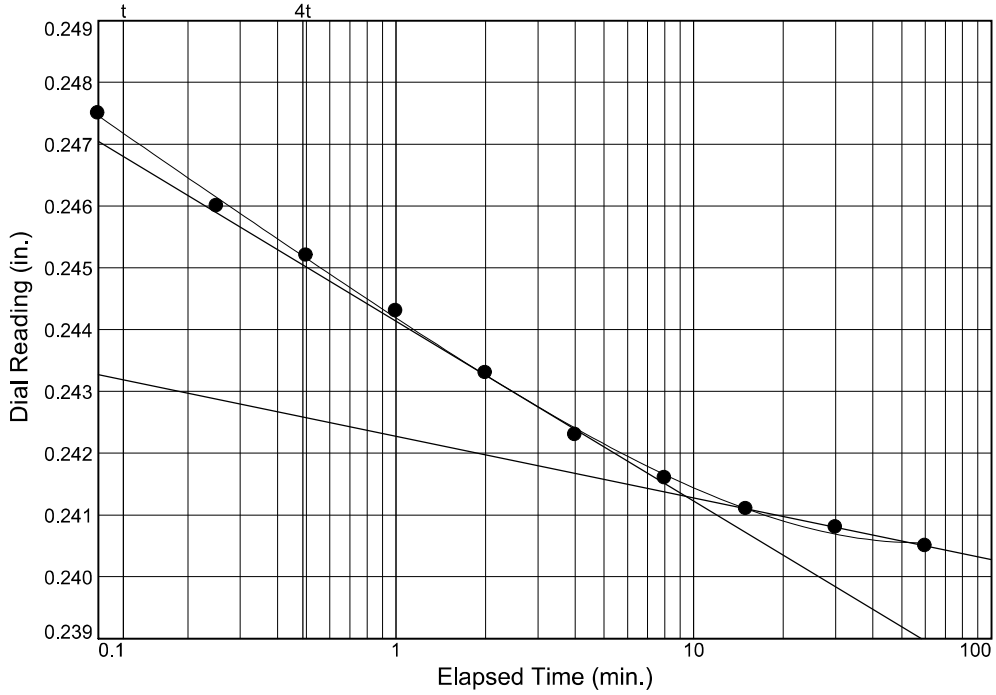
Project No.: 05111037
Project: NCANG

Source of Sample: B-1 Depth: 8.0'-10.0' Sample Number: UD-1



Load No.= 11
Load= 8.00 tsf
D_0 = 0.2639
D_{50} = 0.2626
D_{100} = 0.2613
T_{50} =

C_α = 0.000



Load No.= 13
Load= 0.50 tsf
D_0 = 0.2492
D_{50} = 0.2452
D_{100} = 0.2413
T_{50} = 0.47 min.

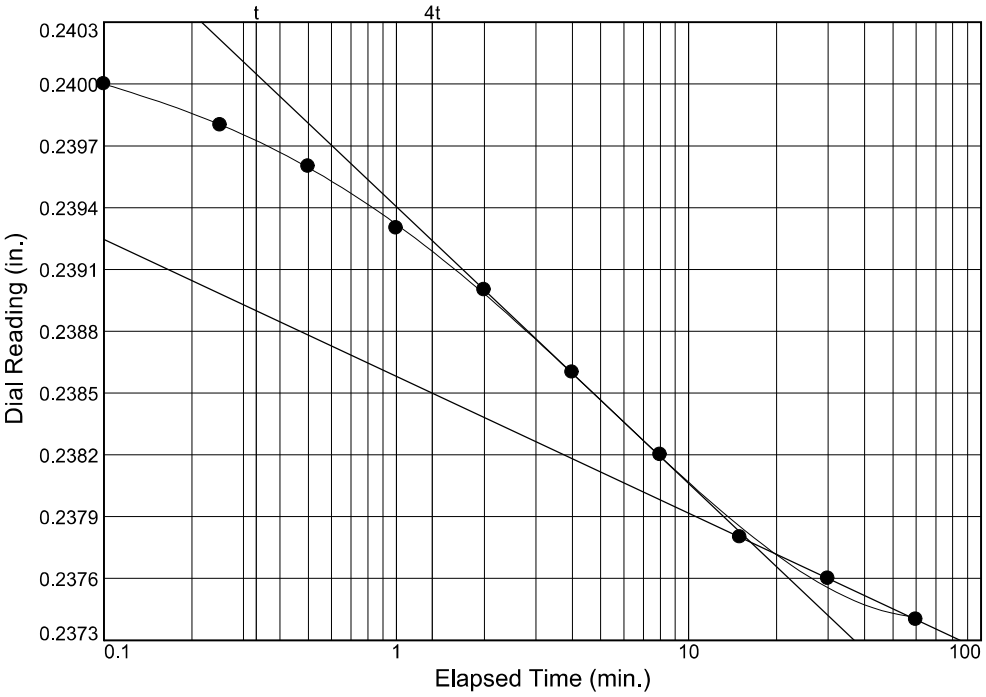
C_v @ T_{50}
1.060 ft.^{2}/day

Figure 5

Dial Reading vs. Time

Project No.: 05111037
Project: NCANG

Source of Sample: B-1 Depth: 8.0'-10.0' Sample Number: UD-1



Load No.= 14

Load= 0.13 tsf

D_0 = 0.2403

D_{50} = 0.2390

D_{100} = 0.2378

T_{50} = 1.86 min.

C_v @ T_{50}
0.277 ft.^{2}/day

Figure 6

CONSOLIDATION TEST DATA

3/6/2023

Client: Intertek-PSI
Project: NCANG
Project Number: 05111037
Location: B-1
Depth: 8.0'-10.0' **Sample Number:** UD-1
Material Description: Moist Stiff Sandy Elastic SILT w/ Clay
USCS: MH **Figure No.:** 1
Tested by: SMP **Checked by:** AS

Test Specimen Data

NATURAL MOISTURE			VOID RATIO			AFTER TEST		
Wet w+t	=	76.46 g.	Spec. Gr.	=	2.710	Wet w+t	=	100.61 g.
Dry w+t	=	60.66 g.	Est. Ht. Solids	=	0.321 in.	Dry w+t	=	84.17 g.
Tare Wt.	=	12.41 g.	Init. V.R.	=	1.335	Tare Wt.	=	13.79 g.
Moisture	=	32.7 %	Init. Sat.	=	66.5 %	Moisture	=	23.4 %

UNIT WEIGHT			TEST START					
Height	=	0.750 in.	Height	=	0.750 in.	Dry Wt.	=	70.38 g.
Diameter	=	2.500 in.	Diameter	=	2.500 in.			
Weight	=	92.93 g.						
Dry Dens.	=	72.4 pcf						

End-Of-Load Summary

Pressure (tsf)	Final Dial (in.)	Deformation (in.)	C_v (ft.^{2}/day)	C_α	Void Ratio	% Strain
start	0.00000	0.00000			1.335	
0.13	0.00840	0.00840*		0.001	1.310	1.1 Comprs.
0.25	0.02600	0.02600*		0.002	1.256	3.4 Comprs.
0.50	0.05030	0.05030*		0.002	1.182	6.6 Comprs.
1.00	0.09540	0.09540*		0.005	1.045	12.4 Comprs.
2.00	0.13920	0.13920*	4.982	0.009	0.909	18.2 Comprs.
4.00	0.18140	0.18140*		0.003	0.775	24.0 Comprs.
8.00	0.22340	0.22340*	2.403	0.002	0.642	29.7 Comprs.
2.00	0.21410	0.21410*			0.666	28.7 Comprs.
8.00	0.22500	0.22500*		0.002	0.637	29.9 Comprs.
16.00	0.26390	0.26390*		0.006	0.524	34.7 Comprs.
8.00	0.26130	0.26130*		0.000	0.522	34.8 Comprs.
2.00	0.24940	0.24940*			0.556	33.4 Comprs.
0.50	0.24050	0.24050*	1.060		0.584	32.2 Comprs.
0.13	0.23740	0.23740*	0.277		0.595	31.7 Comprs.

***CALCULATED USING D_{100} INSTEAD OF FINAL READING**

Compression index (C_c), tsf = 0.44 **Preconsolidation pressure (P_p), tsf =** 0.44 **Void ratio at P_p (e_m) =** 1.201

Overburden (σ_{vo}), tsf = .365 **Void ratio at σ_{vo} (e_o) =** 1.222

Pressure: 0.13 tsf	TEST READINGS	Load No. 1

No.	Elapsed Time	Dial Reading
1	0	0.00000
2	.2	0.00610
3	.25	0.00650
4	.5	0.00720
5	1	0.00770
6	2	0.00800
7	4	0.00820
8	8	0.00830
9	15	0.00840

Void Ratio = 1.310 **Compression =** 1.1%

Pressure: 0.25 tsf	TEST READINGS	Load No. 2

No.	Elapsed Time	Dial Reading
1	0	0.00840
2	.1	0.01740
3	.25	0.02240
4	.5	0.02400
5	1	0.02460
6	2	0.02500
7	4	0.02540
8	8	0.02560
9	15	0.02580
10	30	0.02600

Void Ratio = 1.256 **Compression =** 3.4%

Pressure: 0.50 tsf	TEST READINGS	Load No. 3

No.	Elapsed Time	Dial Reading
1	0	0.02600
2	.1	0.04490
3	.25	0.04690
4	.5	0.04850
5	1	0.04900
6	2	0.04950
7	4	0.04970
8	8	0.05010
9	15	0.05030

Void Ratio = 1.182 **Compression =** 6.6%

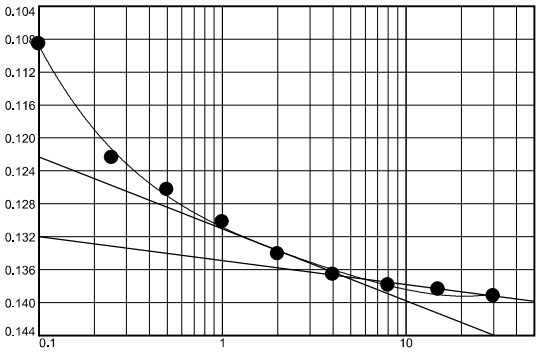
Pressure: 1.00 tsf — **TEST READINGS** — **Load No. 4**

No.	Elapsed Time	Dial Reading	No.	Elapsed Time	Dial Reading
1	0	0.05030	11	60	0.09540
2	.1	0.07240			
3	.25	0.07800			
4	.5	0.08280			
5	1	0.08760			
6	2	0.09100			
7	4	0.09330			
8	8	0.09420			
9	15	0.09470			
10	30	0.09520			

Void Ratio = 1.045 **Compression =** 12.4%

Pressure: 2.00 tsf — **TEST READINGS** — **Load No. 5**

No.	Elapsed Time	Dial Reading
1	0	0.09540
2	.1	0.10860
3	.25	0.12240
4	.5	0.12630
5	1	0.13020
6	2	0.13410
7	4	0.13660
8	8	0.13790
9	15	0.13840
10	30	0.13920



Void Ratio = 0.909 **Compression =** 18.2% >>> CALCULATED USING D_{100}

D_0 = 0.0954 **D_{50} =** 0.1161 **D_{100} =** 0.1368 **C_v at 0.16 min. =** 4.982 ft.^{2}/day **C_α =** 0.009

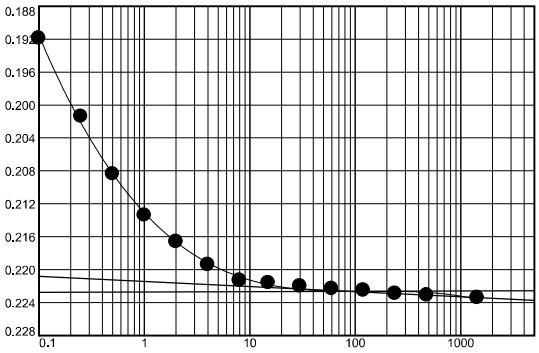
Pressure: 4.00 tsf — **TEST READINGS** — **Load No. 6**

No.	Elapsed Time	Dial Reading	No.	Elapsed Time	Dial Reading
1	0	0.13920	11	60	0.18140
2	.1	0.16000			
3	.25	0.16410			
4	.5	0.16780			
5	1	0.17240			
6	2	0.17610			
7	4	0.17860			
8	8	0.17990			
9	15	0.18060			
10	30	0.18110			

Void Ratio = 0.775 **Compression =** 24.0%

Pressure: 8.00 tsf — **TEST READINGS** — **Load No. 7**

No.	Elapsed Time	Dial Reading	No.	Elapsed Time	Dial Reading
1	0	0.18140	11	60	0.22230
2	.1	0.19190	12	120	0.22250
3	.25	0.20140	13	240	0.22290
4	.5	0.20840	14	480	0.22310
5	1	0.21340	15	1440	0.22340
6	2	0.21660			
7	4	0.21940			
8	8	0.22130			
9	15	0.22160			
10	30	0.22200			



Void Ratio = 0.642 **Compression =** 29.7% >>> CALCULATED USING D_{100}

D_0 = 0.1814 **D_{50} =** 0.2020 **D_{100} =** 0.2226 **C_v at 0.25 min. =** 2.403 ft.^{2}/day **C_α =** 0.002

Pressure: 2.00 tsf | **TEST READINGS** | **Load No. 8**

No.	Elapsed Time	Dial Reading
1	0	0.22340
2	.1	0.21690
3	.25	0.21640
4	.5	0.21590
5	1	0.21540
6	2	0.21480
7	4	0.21450
8	8	0.21430
9	15	0.21420
10	30	0.21410

Void Ratio = 0.666 **Compression =** 28.7%

Pressure: 8.00 tsf | **TEST READINGS** | **Load No. 9**

No.	Elapsed Time	Dial Reading
1	0	0.21410
2	.1	0.22200
3	.25	0.22290
4	.5	0.22330
5	1	0.22390
6	2	0.22440
7	4	0.22460
8	8	0.22480
9	15	0.22500

Void Ratio = 0.637 **Compression =** 29.9%

Pressure: 16.00 tsf | **TEST READINGS** | **Load No. 10**

No.	Elapsed Time	Dial Reading	No.	Elapsed Time	Dial Reading
1	0	0.22500	11	60	0.26240
2	.1	0.24330	12	120	0.26280
3	.25	0.24610	13	240	0.26320
4	.5	0.24940	14	480	0.26360
5	1	0.25320	15	1440	0.26390
6	2	0.25690			
7	4	0.25910			
8	8	0.26070			
9	15	0.26140			
10	30	0.26180			

Void Ratio = 0.524 **Compression =** 34.7%

Pressure: 8.00 tsf — **TEST READINGS** — **Load No. 11**

No.	Elapsed Time	Dial Reading
1	0	0.26390
2	.1	0.26190
3	.25	0.26170
4	.5	0.26160
5	1	0.26150
6	2	0.26140
7	4	0.26135
8	8	0.26130
9	15	0.26130

Void Ratio = 0.522 **Compression =** 34.8%

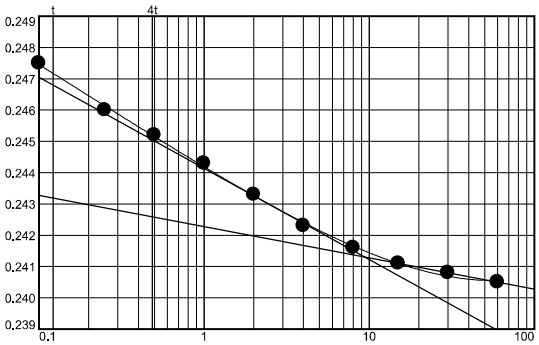
Pressure: 2.00 tsf — **TEST READINGS** — **Load No. 12**

No.	Elapsed Time	Dial Reading
1	0	0.26130
2	.1	0.25430
3	.25	0.25340
4	.5	0.25240
5	1	0.25150
6	2	0.25060
7	4	0.25000
8	8	0.24970
9	15	0.24940

Void Ratio = 0.556 **Compression =** 33.4%

Pressure: 0.50 tsf — **TEST READINGS** — **Load No. 13**

No.	Elapsed Time	Dial Reading	No.	Elapsed Time	Dial Reading
1	0	0.24940	11	60	0.24050
2	.1	0.24750			
3	.25	0.24600			
4	.5	0.24520			
5	1	0.24430			
6	2	0.24330			
7	4	0.24230			
8	8	0.24160			
9	15	0.24110			
10	30	0.24080			

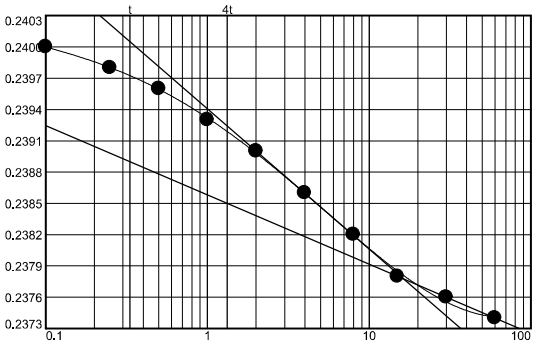


Void Ratio = 0.584 **Compression =** 32.2% >>> CALCULATED USING D_{100}

D_0 = 0.2492 **D_{50} =** 0.2452 **D_{100} =** 0.2413 **C_v at 0.47 min. =** 1.060 ft.^{2}/day

Pressure: 0.13 tsf | **TEST READINGS** | **Load No. 14**

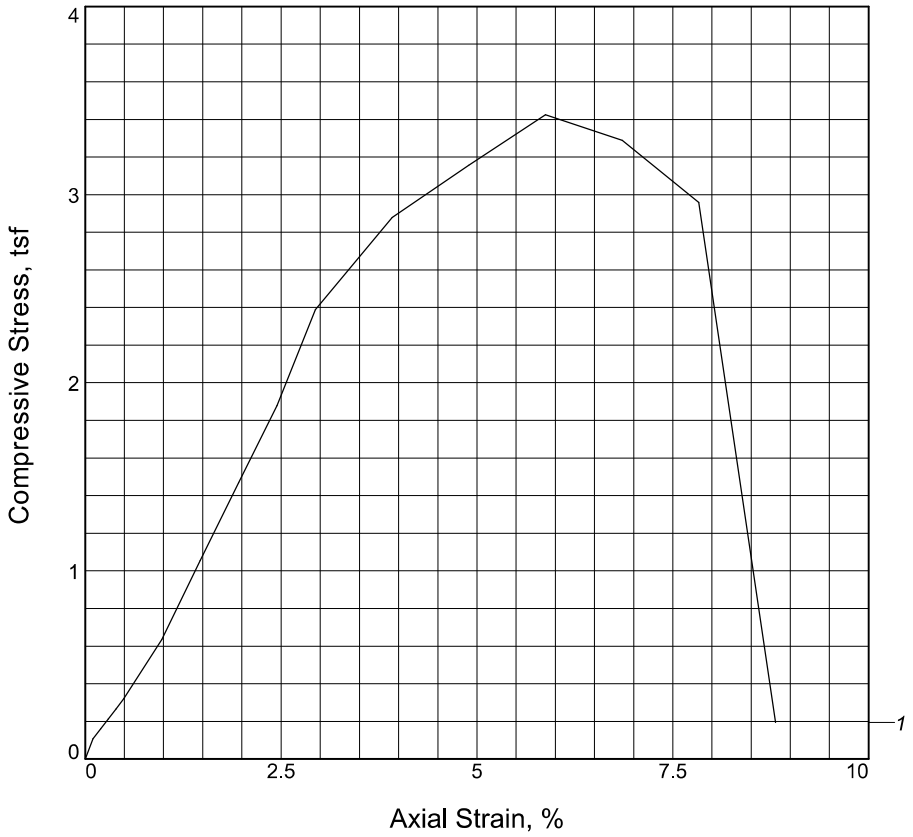
No.	Elapsed Time	Dial Reading	No.	Elapsed Time	Dial Reading
1	0	0.24050	11	60	0.23740
2	.1	0.24000			
3	.25	0.23980			
4	.5	0.23960			
5	1	0.23930			
6	2	0.23900			
7	4	0.23860			
8	8	0.23820			
9	15	0.23780			
10	30	0.23760			



Void Ratio = 0.595 **Compression =** 31.7% >>> CALCULATED USING D_{100}

D_0 = 0.2403 D_{50} = 0.2390 D_{100} = 0.2378 C_v **at 1.86 min. =** 0.277 ft.^{2}/day

UNCONFINED COMPRESSION TEST



Sample No.	1			
Unconfined strength, tsf	3.425			
Undrained shear strength, tsf	1.712			
Failure strain, %	5.9			
Strain rate, in./min.	0.050			
Water content, %	35.8			
Wet density, pcf	109.3			
Dry density, pcf	80.5			
Saturation, %	88.0			
Void ratio	1.1017			
Specimen diameter, in.	2.84			
Specimen height, in.	4.08			
Height/diameter ratio	1.44			

Description: Moist Stiff Red Sandy Elastic SILT w/ Clay and Mica

LL = 53	**PL =** 43	**PI =** 10	**GS=** 2.71	**Type:** Shelby Tube

Project No.: 05111037
Date Sampled:
Remarks:

Figure 01

Client:

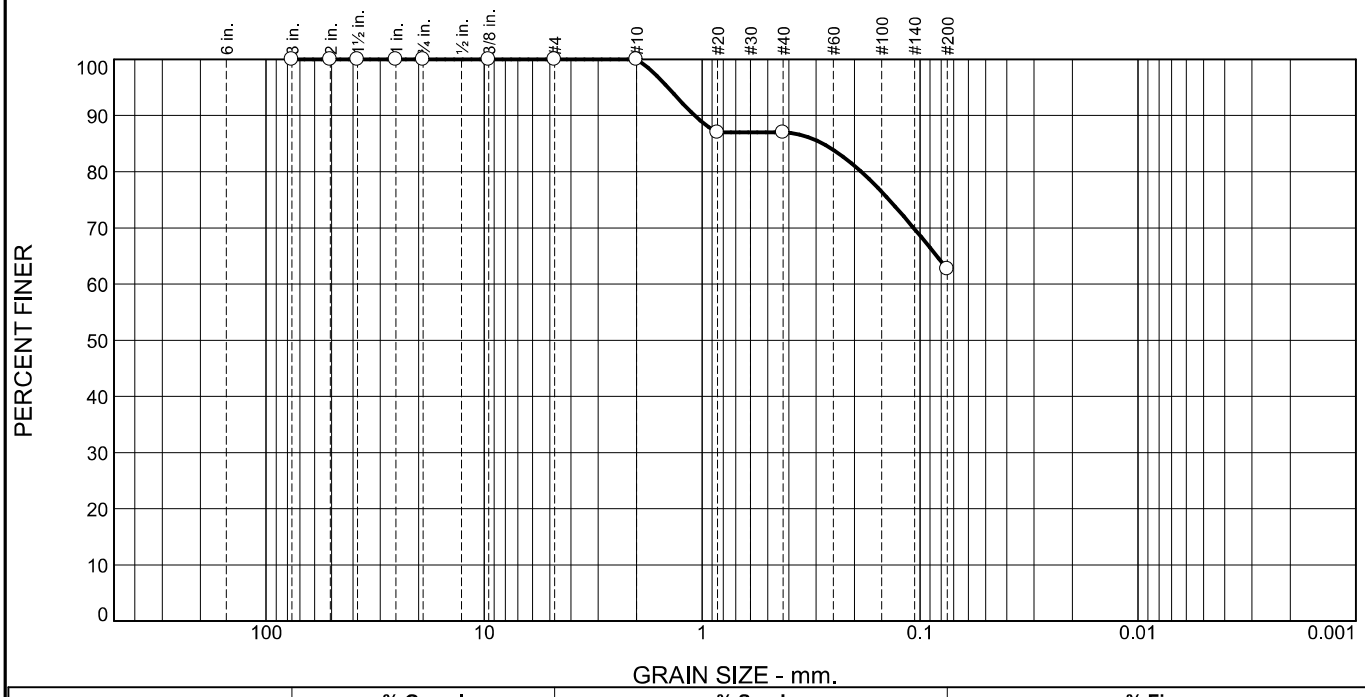
Project: NCANG

Source of Sample: B-1 **Depth:** 8.0'-10.0'
Sample Number: UD-1

UNCONFINED COMPRESSION TEST
Professional Service Industries, Inc.
5021 W. W.T. Harris Blvd.

Tested By: SP **Checked By:** AS

Particle Size Distribution Report



% +3"	% Gravel		% Sand			% Fines	
	Coarse	Fine	Coarse	Medium	Fine	Silt	Clay
0.0	0.0	0.0	0.0	13.0	24.3	62.7	

Test Results (ASTM D 422 & ASTM D 1140)

Opening Size	Percent Finer	Spec.* (Percent)	Pass? (X=Fail)
3	100.0		
2	100.0		
1.5	100.0		
1	100.0		
.75	100.0		
.375	100.0		
#4	100.0		
#10	100.0		
#20	87.0		
#40	87.0		
#200	62.7		

* (no specification provided)

Material Description

Moist Stiff Red Sandy Elastic SILT w/ Clay and Mica

Atterberg Limits (ASTM D 4318)

PL= 43 **LL=** 53 **PI=** 10

Classification

USCS (D 2487)= MH **AASHTO (M 145)=** A-5(7)

Coefficients

D_{90}= 1.0815 D_{85}= 0.2800 D_{60}=
D_{50}= D_{30}= D_{15}=
D_{10}= C_u= C_c=

Remarks

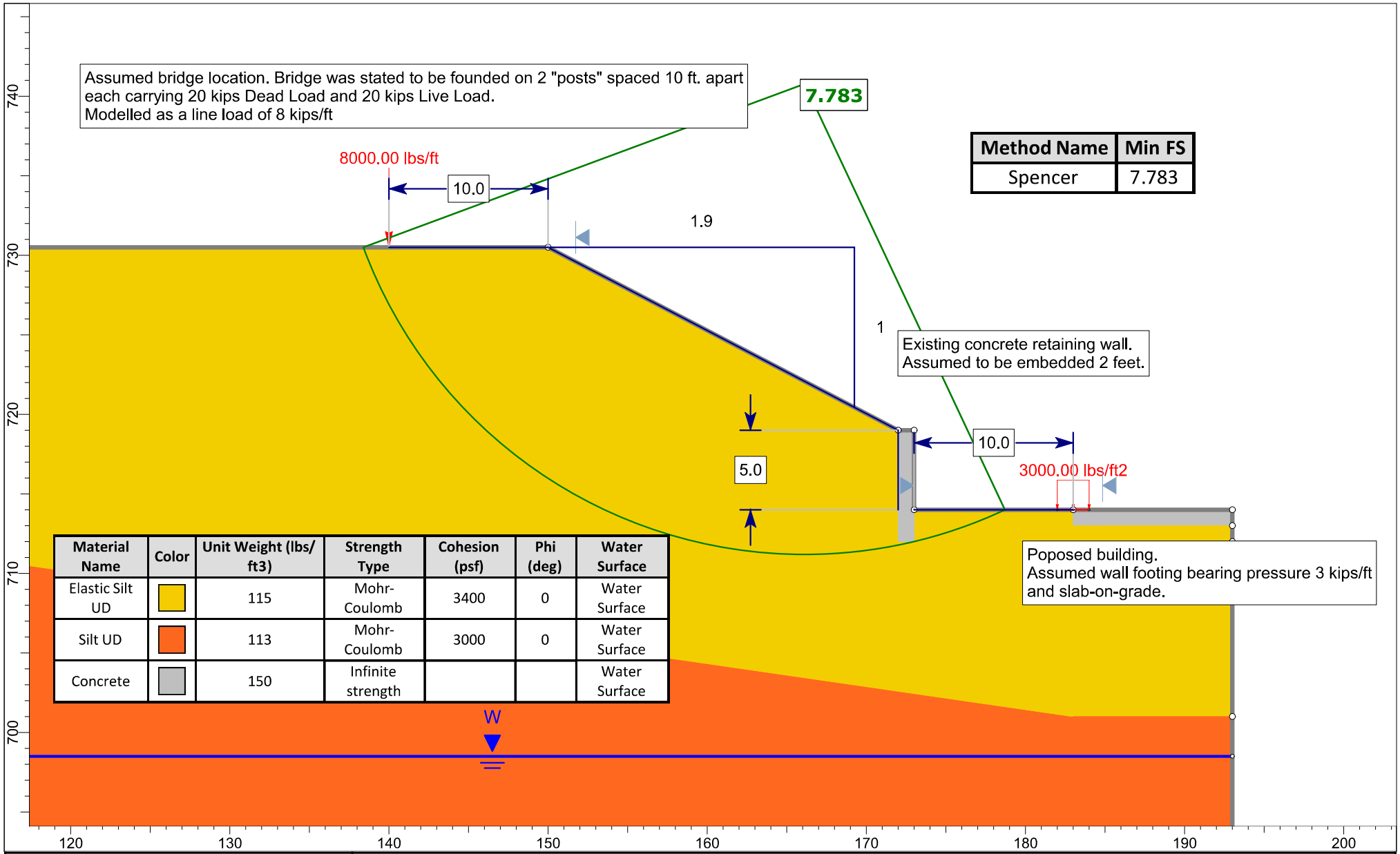
Date Received: 3/3/23 **Date Tested:** 3/5/23
Tested By: SMP
Checked By: AS
Title: Project Manager

Source of Sample: B-1 **Depth:** 8.0'-10.0' **Date Sampled:**
Sample Number: UD-1

Professional Service Industries, Inc.
5021 W. W.T. Harris Blvd.
Charlotte, NC

Client:
Project: NCANG
Project No: 05111037 **Figure**

SLOPE STABILITY PACKAGE



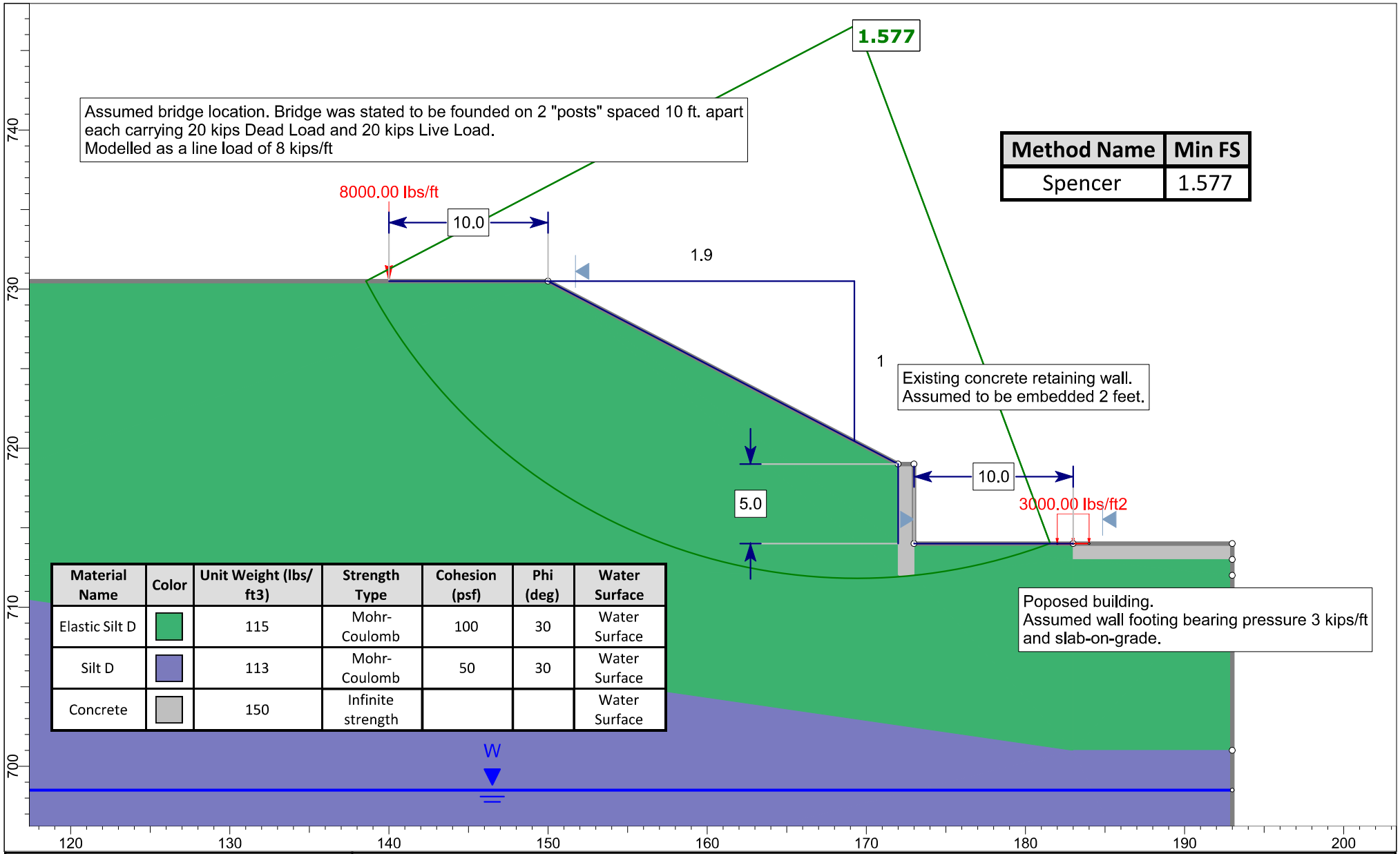
Method Name	Min FS
Spencer	7.783

Material Name	Color	Unit Weight (lbs/ft3)	Strength Type	Cohesion (psf)	Phi (deg)	Water Surface
Elastic Silt UD		115	Mohr-Coulomb	3400	0	Water Surface
Silt UD		113	Mohr-Coulomb	3000	0	Water Surface
Concrete		150	Infinite strength			Water Surface

intertek psi

SLIDEINTERPRET 9.009

Project	North Carolina Air National Guard Facility, Charlotte, NC (Charlotte Douglass International Airport)
Analysis Description	Undrained Stress Conditions; Circular Failure; with groundwater.
Drawn By	RLJ
Company	INTERTEK/PSI
Date	3/15/2023
Scale	1:100
File Name	Slope - Bridge.slmd



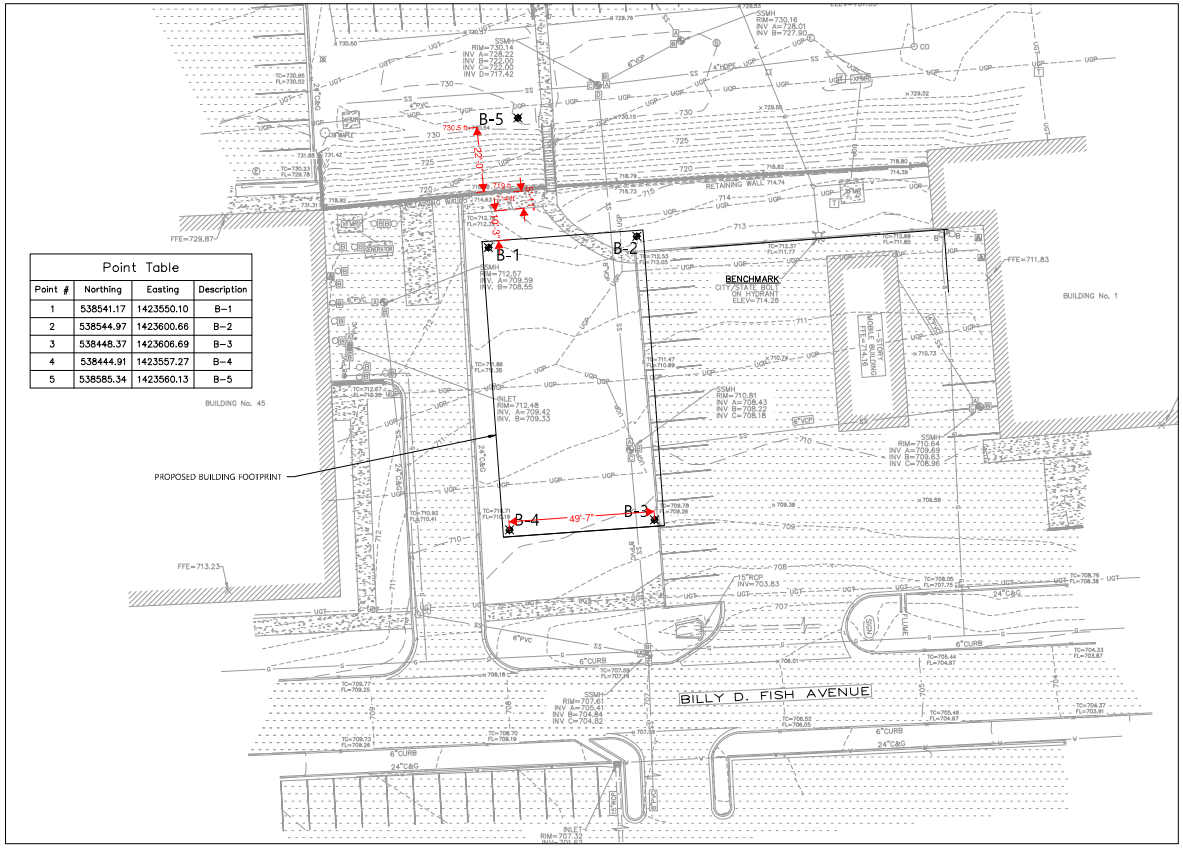
Method Name	Min FS
Spencer	1.577

Material Name	Color	Unit Weight (lbs/ft3)	Strength Type	Cohesion (psf)	Phi (deg)	Water Surface
Elastic Silt D		115	Mohr-Coulomb	100	30	Water Surface
Silt D		113	Mohr-Coulomb	50	30	Water Surface
Concrete		150	Infinite strength			Water Surface

intertek psi

SLIDEINTERPRET 9.009

Project	North Carolina Air National Guard Facility, Charlotte, NC (Charlotte Douglass International Airport)
Analysis Description	Drained Stress Conditions; Circular Failure; with groundwater.
Drawn By	RLJ
Company	INTERTEK/PSI
Date	3/15/2023
Scale	1:100
File Name	Slope - Bridge.slmd



Point Table			
Point #	Northing	Easting	Description
1	538541.17	1423550.10	B-1
2	538544.97	1423600.66	B-2
3	538448.37	1423606.69	B-3
4	538444.91	1423557.27	B-4
5	538585.34	1423560.13	B-5

1 **BORING PLAN**

AECOM

PROJECT

NORTH CAROLINA ANG

NEW SECURITY FORCES BUILDING

CLIENT

NORTH CAROLINA ANG

145th AIRLIFT WING
4930 MINUTEMAN WAY
CHARLOTTE, NORTH CAROLINA 28208

CONSULTANT

AECOM

277 W NATIONWIDE BLVD
COLUMBUS, OH 43215
614.464.4500

CONSULTANTS

REGISTRATION

ISSUE/REVISION

I/R	DATE	DESCRIPTION

PROJECT NUMBER

60637899

SHEET TITLE

BORING PLAN

SHEET NUMBER

B01

©2016 AECOM Corporation

A01-OPTION 1 Approver(ARCH E1 30" x 42" Approval Checker Checkout Designer Designer Project Management Initials
Last Plotted: 3/26/2021 10:43:24 AM
File name: P:\60637899-ANG\11-CAD\03SITE\SPECIAL\ANG145\60637899_B-NC-ANG_A_R01.rvt
Printed on ___% Post-Consumer Recycled Content Paper

BORING B-1

DATE STARTED:	2/23/23	**DRILL COMPANY:**	HPC
DATE COMPLETED:	2/23/23	**DRILLER:** Price	**LOGGED BY:** Steege
COMPLETION DEPTH	35.0 ft	**DRILL RIG:**	CME 550
BENCHMARK:	N/A	**DRILLING METHOD:**	Hollow Stem Auger
ELEVATION:	713 ft	**SAMPLING METHOD:**	2-in SS, Standard
LATITUDE:		**HAMMER TYPE:**	Automatic
LONGITUDE:		**EFFICIENCY**	N/A
STATION: N/A	**OFFSET:** N/A	**REVIEWED BY:**	AOS

Water

While Drilling	32	feet
Upon Completion Dry, CID=15		feet
Delay	N/A	

BORING LOCATION:
See Boring Location Plan

REMARKS: Borehole backfilled with the auger cuttings upon completion. CID = Cave-In Depth

Elevation (feet)	Depth, (feet)	Sample No.	Recovery (inches)	MATERIAL DESCRIPTION	USCS Classification	SPT Blows per 6-inch (SS)	Moisture, %	Additional Remarks
	0			**TOPSOIL** (4 inches)				
710		1	16	**RESIDUUM** - Firm, Red/Brown, Elastic SILT - Moist	MH	3-2-3 N=5	41	LL = 63 PL = 44 Fines = 97.1%
	5	2	18			3-3-4 N=7		
705		3	18	Firm, Brown/Red, Sandy Elastic SILT with Mica - Moist	MH	3-3-5 N=8	33	LL = 53 PL = 43 Fines = 62.7
	10	4	16			2-2-3 N=5		
700		5	18	Soft, Brown/Gray, Fine Sandy SILT with Mica - Moist to Wet	ML	1-2-2 N=4		
695	15	6	18			1-2-2 N=4		
690	20	7	18			0-2-2 N=4		
685	25	8	18			2-2-2 N=4		
680	30	9	16	Medium Dense, Brown/Gray, Silty SAND with Mica - Wet	SM	6-6-4 N=10		
	35			Boring terminated at 35 feet.				

STANDARD PENETRATION TEST DATA
N in blows/ft ◎
× Moisture ◪ PL ✚ LL
0 25 50
STRENGTH, tsf
▲ Qu ✳ Qp
0 2.0 4.0

intertek psi
Professional Service Industries, Inc.
5021-A West W.T. Harris Boulevard
Charlotte, NC 28269
Telephone: (704) 598-2234

PROJECT NO.: 05111037
PROJECT: Construct Security Forces Facility
LOCATION: NCANG
Charlotte Douglas International Airport
Charlotte, North Carolina

The stratification lines represent approximate boundaries. The transition may be gradual.

BORING B-5

DATE STARTED:	2/23/23	**DRILL COMPANY:**	HPC
DATE COMPLETED:	2/23/23	**DRILLER:** Price	**LOGGED BY:** Steege
COMPLETION DEPTH	30.0 ft	**DRILL RIG:**	CME 550
BENCHMARK:	N/A	**DRILLING METHOD:**	Hollow Stem Auger
ELEVATION:	730 ft	**SAMPLING METHOD:**	2-in SS, Standard
LATITUDE:		**HAMMER TYPE:**	Automatic
LONGITUDE:		**EFFICIENCY**	N/A
STATION: N/A	**OFFSET:** N/A	**REVIEWED BY:**	AOS

Water

While Drilling	None
Upon Completion	Dry
Delay	N/A

BORING LOCATION:
See Boring Location Plan

REMARKS: Borehole backfilled with the auger cuttings upon completion.

Elevation (feet)	Depth, (feet)	Sample No.	Recovery (inches)	MATERIAL DESCRIPTION	USCS Classification	SPT Blows per 6-inch (SS)	Moisture, %	Additional Remarks
	0			**TOPSOIL** (4 1/2 inches)				
		1	8	**RESIDUUM** - Soft to Firm, Red/Brown, Elastic SILT - Moist	MH	2-2-2 N=4	31	
725	5	2	12			2-3-3 N=6	30	
		3	15	Stiff and Firm, Red/Brown, Elastic SILT - Moist	MH	3-5-5 N=10	28	LL = 54 PL = 39 Fines = 74.4%
720	10	4	14			2-3-3 N=6		
715	15	5	16			3-4-7 N=11		
				Firm, Brown, Sandy SILT with Mica - Moist	ML			
710	20	6	18			2-4-4 N=8		
705	25	7	15			2-3-3 N=6		
700	30	8	18			2-2-3 N=5		
				Boring terminated at 30 feet.				

STANDARD PENETRATION TEST DATA
N in blows/ft ◎
× Moisture ◪ PL ✚ LL
0 25 50

STRENGTH, tsf
▲ Qu ✳ Qp
0 2.0 4.0

intertek psi

Professional Service Industries, Inc.
5021-A West W.T. Harris Boulevard
Charlotte, NC 28269
Telephone: (704) 598-2234

PROJECT NO.: 05111037
PROJECT: Construct Security Forces Facility
LOCATION: NCANG
Charlotte Douglas International Airport
Charlotte, North Carolina

The stratification lines represent approximate boundaries. The transition may be gradual.

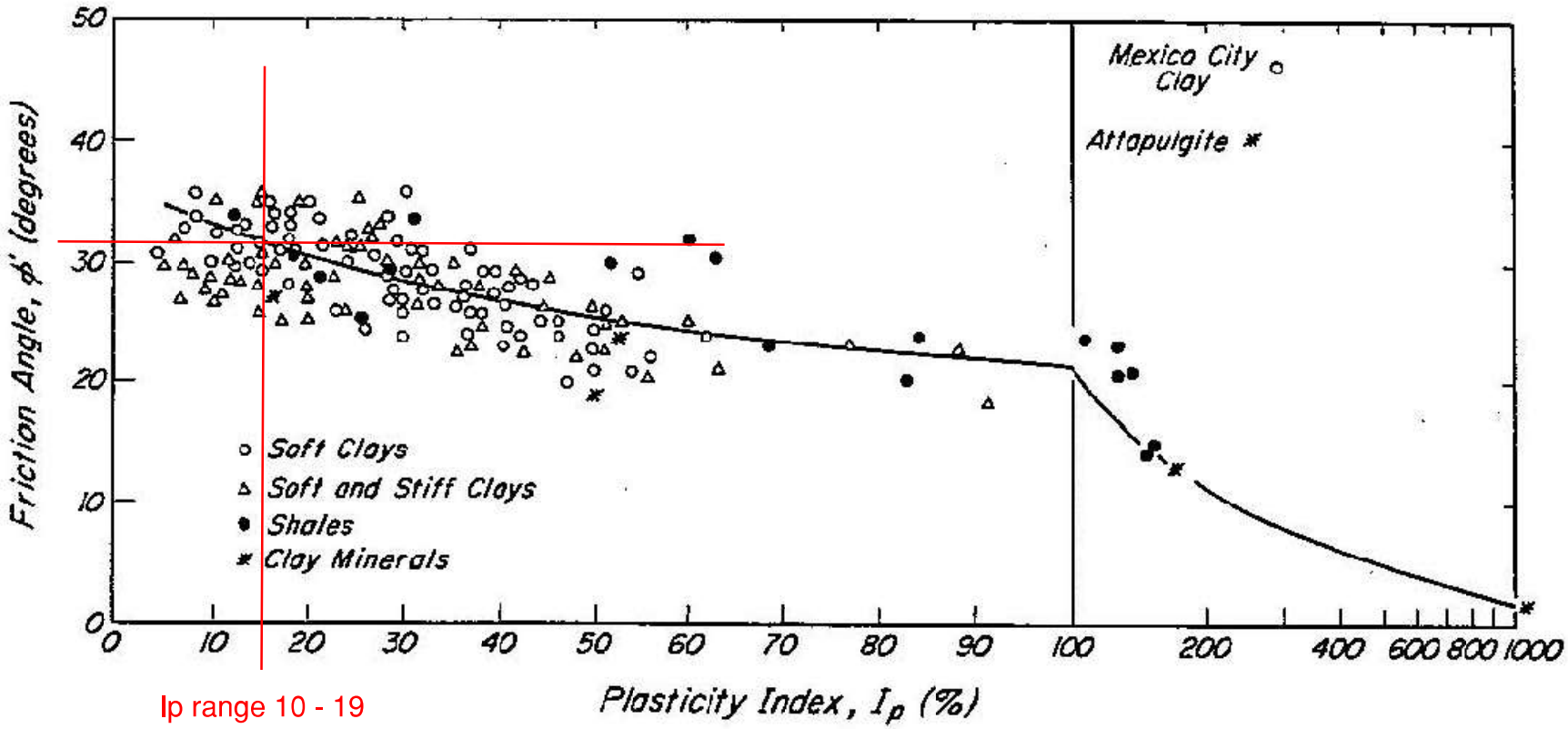
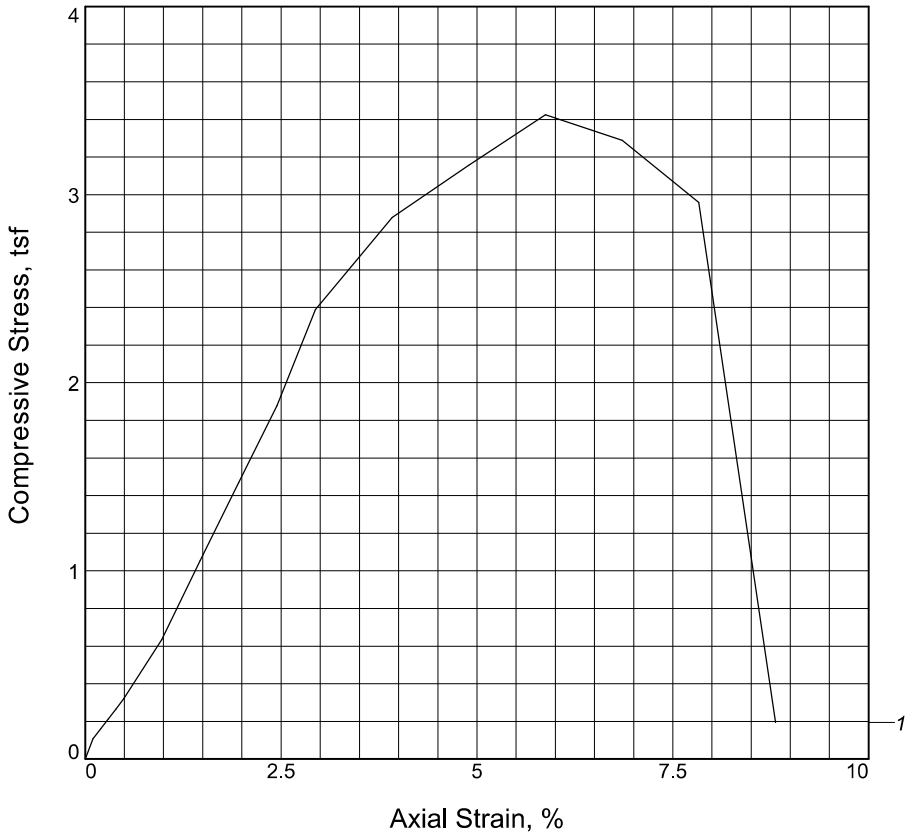


Figure 19.7 Values of friction angle ϕ' for clays of various compositions as reflected in plasticity index.

UNCONFINED COMPRESSION TEST



Sample No.	1			
Unconfined strength, tsf	3.425			
Undrained shear strength, tsf	1.712			
Failure strain, %	5.9			
Strain rate, in./min.	0.050			
Water content, %	35.8			
Wet density, pcf	109.3			
Dry density, pcf	80.5			
Saturation, %	88.0			
Void ratio	1.1017			
Specimen diameter, in.	2.84			
Specimen height, in.	4.08			
Height/diameter ratio	1.44			

Description: Moist Stiff Red Sandy Elastic SILT w/ Clay and Mica

LL = 53	**PL =** 43	**PI =** 10	**GS=** 2.71	**Type:** Shelby Tube

Project No.: 05111037
Date Sampled:
Remarks:

Figure 01

Client:

Project: NCANG

Source of Sample: B-1 **Depth:** 8.0'-10.0'
Sample Number: UD-1

UNCONFINED COMPRESSION TEST
Professional Service Industries, Inc.
5021 W. W.T. Harris Blvd.

Tested By: SP **Checked By:** AS

5021 West W.T. Harris Boulevard
Charlotte, North Carolina 28269
Phone 704-598-2234 · Fax 704-598-2236

intertek psi

LAB ASSIGNMENT FORM

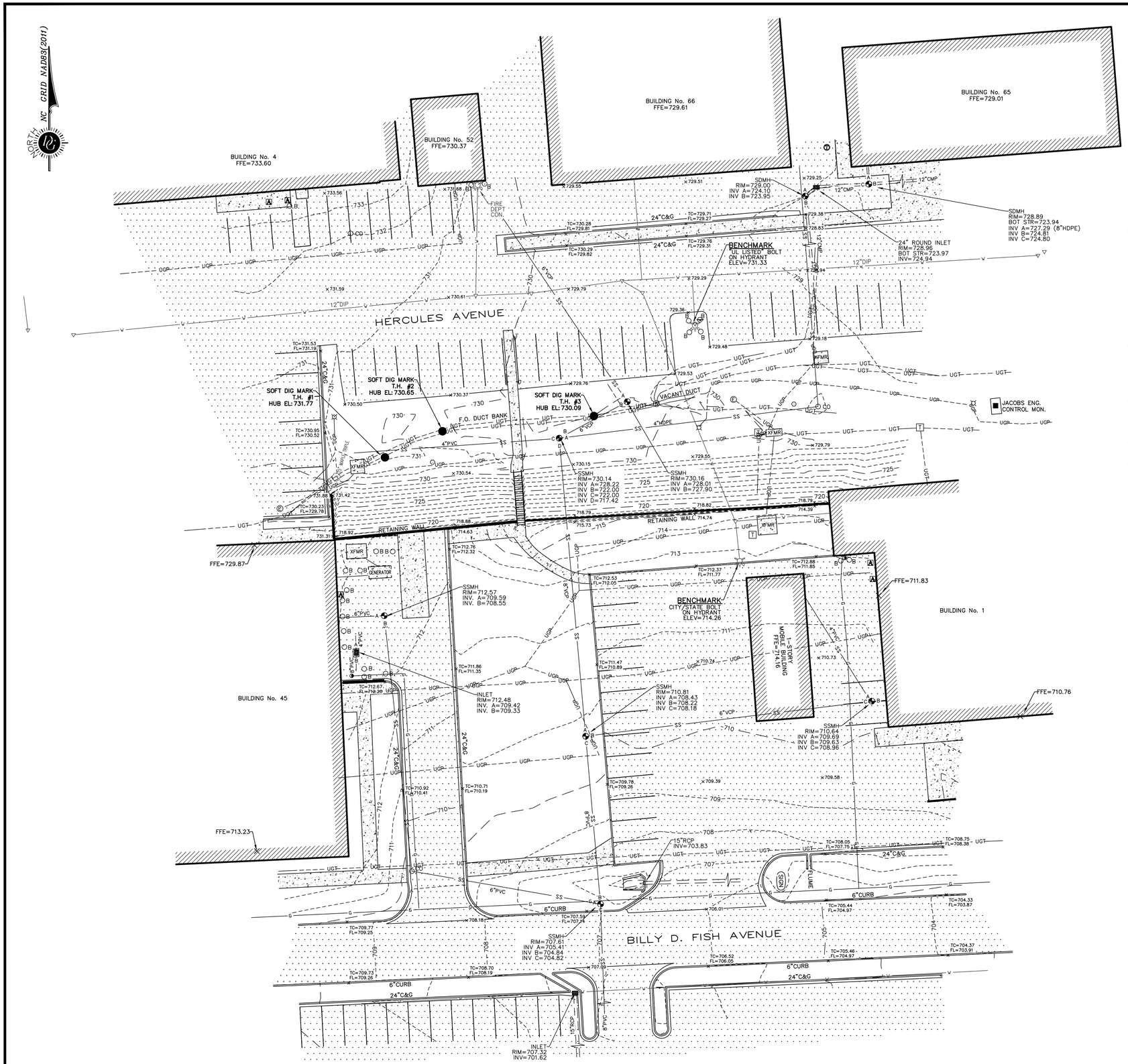
PROJECT NAME:	**NCANG**	**PSI PROJECT NO.:**	**5111037**
DATE ASSIGNED:	**2/28/2320**	**ASSIGNED BY:**	**Drew Steege 704.517.5913**
DATE DUE:	**3/8/2023**	**COMPLETED BY:**	**G. Guse**

Boring / Test Pit No	Sample Number	Sample Type	Sample Depth (Feet)	Moisture Conctent ASTM D2216	Atterberg Limits ASTM D4318			% Finer Than No.200 ASTM D1140	Sieve Analysis, w/ wash 200 ASTM D1140	Specific Gravity ASTM D854	Hydrometer Anaylsis ASTM D422	pH, Chlorides and Sulfates ASTM	Organic Content ASTM D	Lab Resistivity	Unconfined Compression ASTM D2166	- with stress strain measurements	TRIAXIAL SHEAR TEST ASTM D2850	- Unconsolidated, Undrained (UU)	-Consolidated, Undrained (CU)	-Consolidated, Drained (CD)	CBR ASTM D1883	-Unit Weight (pcf) ASTM D7263	-Standard Dry Density (pcf)	-Optimum Mosture Content (%)	Notes
					LL	PL	PI																		
B-1	1	SS	1-2.5	**41.3**	63	44	**19**	**97.1%**																	MH
B-3	1	SS	1-2.5	**19.7**	45	28	**17**	**69.1%**																	ML
B-5	1	SS	1-2.5	**31.1**																					
B-5	2	SS	3.5-5	**29.7**																					
B-5	3	SS	6-7.5	**28.1**	54	39	**15**	**74.4%**																	MH

REMARKS:

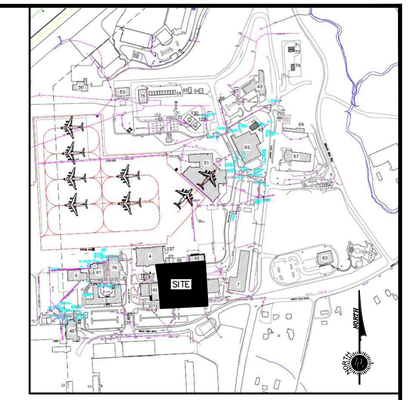
SS = Split Spoon TP = Test Pit A = Auger Cuttings BK = Bulk HA = Hand Auger Cuttings UD = Undisturbed

Docusign Envelope ID: 82AE5BFA-116A-4687-B51E-B918FB3490DD



LEGEND

EXISTING CONTOUR LINE	714
WATER LINE	V
GAS LINE	G
UNDERGROUND POWER LINE	UGP
UNDERGROUND TEL/COM LINE	UGT
SANITARY SEWER LINE	SS
STORM SEWER LINE	18" RCP
GNSS "GPS" CONTROL	
LIGHT POLE	
TELEPHONE PEDESTAL	T
TELEPHONE MANHOLE	
ELECTRIC PEDESTAL	XFMR
ELECTRIC MANHOLE	E
WATER VALVE	
FIRE HYDRANT	
GAS METER	
STORM WATER MANHOLE	SDMH
STORM WATER INLET	INLET
SANITARY SEWER MANHOLE	SSMH
CLEANOUT	CO
BOLLARD	B
SIGN	
TREE (SIZE/TYPE NOTED)	
AIR CONDITIONER / HVAC	A
SPOT ELEVATION	×730.15
ASPHALT	
CONCRETE	



VICINITY MAP
NOT TO SCALE

NOTES

1. DISTANCES SHOWN HEREON ARE HORIZONTAL GROUND DISTANCES UNLESS OTHERWISE NOTED.
2. UNADJUSTED RATIO OF PRECISION 1:73,616.
3. ANY UNDERGROUND UTILITIES SHOWN HAVE BEEN LOCATED FROM FIELD SURVEY INFORMATION AND EXISTING DRAWINGS. THE SURVEYOR MAKES NO GUARANTEE THAT THE UNDERGROUND UTILITIES SHOWN COMPRISE ALL SUCH UTILITIES IN THE AREA, EITHER IN SERVICE OR ABANDONED. THE SURVEYOR FURTHER DOES NOT WARRANT THAT THE UNDERGROUND UTILITIES SHOWN ARE IN THE EXACT LOCATION INDICATED, ALTHOUGH HE DOES STATE THAT THEY ARE LOCATED AS ACCURATELY AS POSSIBLE FROM INFORMATION AVAILABLE. THE SURVEYOR HAS NOT PHYSICALLY LOCATED THE UNDERGROUND UTILITIES. BEFORE BEGINNING ANY CONSTRUCTION OR BORINGS, CONTACT THE UTILITIES PROTECTION CENTER AT 1-800-632-4949.
4. THIS SURVEY IS REFERENCED TO THE NC STATE PLANE COORDINATE SYSTEM, NAD 83(2011).
5. CONTOUR INTERVAL SHOWN IS ONE FOOT. ELEVATIONS ARE REFERENCED TO THE NORTH AMERICAN VERTICAL DATUM OF 1988 (NAVD88).
6. DONALDSON, GARRETT & ASSOCIATES, INC. AND THE LAND SURVEYOR WHOSE SEAL IS AFFIXED HEREON DO NOT GUARANTEE THAT ALL EASEMENTS WHICH MAY AFFECT THIS PROPERTY ARE SHOWN.

GPS REAL TIME KINEMATIC (RTK) NETWORK SUMMARY:

I, John M. Story, certify that this map was drawn under my supervision from an actual GPS survey made under my supervision and the following information was used to perform the survey:

(1) Class of Survey: A
(2) Positional accuracy: HORIZONTAL 0.021' – VERTICAL 0.028'
(3) Type of GPS field procedure: NC REAL TIME NETWORK (RTN)– SP85, 240 CHANNELS GPS L1/L2/L5 GLONASS, BEIDOU, GALILEO, QZSS, SBAS INTEGRATED RECEIVER/ANTENNA (DUAL FREQUENCY RECEIVERS)
(4) Dates of Survey: JANUARY 10, 2022.
(5) Datum/ Epoch: NAD83(2011); NAVD88 / EPOCH 2010.00
(6) Published/ Fixed-control use: "CHARLOTTE CORS ARP"
(7) GEOID Model: GEOID 18
(8) Combined Factor: 0.99983712
(9) Units: U.S. SURVEY FEET (sFT)

SURVEYOR'S CERTIFICATE

"I, JOHN M. STORY, CERTIFY THAT THIS PROJECT WAS COMPLETED UNDER MY DIRECT AND RESPONSIBLE CHARGE FROM AN ACTUAL SURVEY MADE UNDER MY SUPERVISION; THAT THIS SURVEY WAS PERFORMED TO MEET THE REQUIREMENTS FOR A PLANIMETRIC SURVEY TO THE ACCURACY OF CLASS A AND VERTICAL ACCURACY WHEN APPLICABLE TO THE CLASS A STANDARD, AND THAT THE ORIGINAL DATA WAS OBTAINED ON JANUARY 10–11, 2022; THAT THE SURVEY WAS COMPLETED ON JANUARY 26, 2022, LAST REVISED FEBRUARY 26, 2025; AND ALL COORDINATES ARE BASED ON NC GRID 'NAD 83'(2011) AND AND ALL ELEVATIONS ARE BASED ON NAVD 88 (GEOID18); AND THAT THIS MAP MEETS THE REQUIREMENTS OF THE STANDARDS OF PRACTICE FOR LAND SURVEYING IN NORTH CAROLINA (21 NCAC 56.1606)."

WITNESS MY ORIGINAL SIGNATURE, REGISTRATION NUMBER AND SEAL THIS 26TH DAY OF JANUARY A.D. 2022."

DocuSigned by:
JOHN M. STORY NC LAND SURVEYOR L-3840
1AF1982038D84F1...

March 31, 2025
DATE

NORTH CAROLINA PROFESSIONAL SEAL L-3840 LAND SURVEYOR JOHN M. STORY

20 0 20 40 60
GRAPHIC SCALE IN FEET

THIS DRAWING CONTAINS 2 SHEETS AND IS CONSIDERED INCOMPLETE WITHOUT THE 2 SHEETS TOGETHER, SEE SHEET 2 FOR SOFT DIG POT HOLE DETAILS.

TOPOGRAPHIC SURVEY
FOR
AECOM
NORTH CAROLINA AIR NATIONAL GUARD BASE
CHARLOTTE/DOUGLAS INTERNATIONAL AIRPORT

SHEET 1 OF 2 | CHARLOTTE/MECKLENBURG COUNTY | NORTH CAROLINA

02/26/2025 – ADD UTILITY LOCATIONS	DWN.BY: STAFF
03/31/2025 – ADD SOFT DIG LOCATIONS, SHEET 2	CKD.BY JMS
	FIELDBOOK N/A
	PLS NO. L-3840

Donaldson Garrett & Associates, Inc.
MACON • CHARLOTTE
9741-L SOUTHERN PINE BOULEVARD
CHARLOTTE, N.C. 28273
(704) 374-1955
http://www.dg-a.com
John.Story@dg-anc.com
NC CORPORATE LICENSE NO. C-1518

DATE: JANUARY 25, 2022
SCALE: 1"=20'
PROJECT NO. 5292-051-N1
DRAWING NO. NC-009-22-D

THESE DOCUMENTS, AS INSTRUMENTS OF SERVICE, REMAIN THE PROPERTY OF D. G. & A. AND NO PART THEREOF MAY BE USED OR REPRODUCED IN ANY FORM WITHOUT WRITTEN PERMISSION.

S:\Working\5292-AECOM\051 (N1539) CONSTRUCT SECURITY FORCES BUILDING-145TH NCANG\Drawing\N1539 AS-BUILT WITH UTILITIES SHOWING THE 3 POT HOLES 03.31.2025 REV2.dwg
4/2/2025 9:47:34 PM BY: JOHN STORY

Docusign Envelope ID: 82AE5BFA-116A-4687-B51E-B918FB3490DD

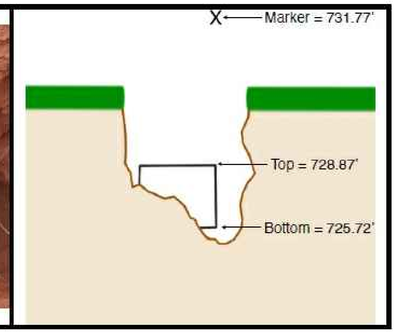
Sweetwater Utility Exploration
Test Hole Data Sheet

5030.055 — Date: 3/20/2025

Project:	NCANG Radio Tower	Test Hole #	1
Utility		**Hole Condition**	
Utility	Telephone Duct Bank	Surface Material	Grass
Size	24" x 36" +/-	Thickness	
Material	Rough Pour Concrete	Condition	
Color	Grey	Soil Type	Clay
Condition	Good	Additional Information	
Width/O.D.	24"		

Depth and Elevation Measurement Information

Surface Marker	Hub & Tack	Utility	Top	Bottom
Set Over	Northern Most Edge	Depth	2.90	6.05
Northing	538588.5407	Elevation	728.87	725.72
Easting	1423514.7304			
Elevation	731.77			



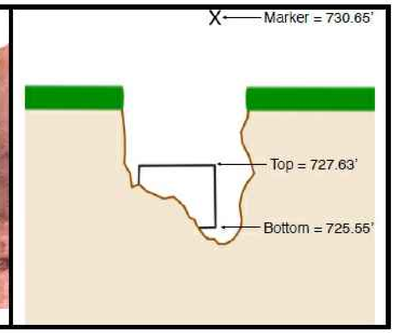
Sweetwater Utility Exploration
Test Hole Data Sheet

5030.055 — Date: 3/20/2025

Project:	NCANG Radio Tower	Test Hole #	2
Utility		**Hole Condition**	
Utility	Telephone Duct Bank	Surface Material	Grass
Size	N/A	Thickness	
Material	Rough Pour Concrete	Condition	
Color	Grey	Soil Type	Clay
Condition	Poor	Additional Information	
Width/O.D.	N/A		

Depth and Elevation Measurement Information

Surface Marker	Hub & Tack	Utility	Top	Bottom
Set Over	Northern Most Edge	Depth	3.02	5.10
Northing	538599.4422	Elevation	727.63	725.55
Easting	1423538.6996	***Crew exposed extremely rough poured concrete at this location. Both vertical and horizontal over pour of cement allowed for only very rough depth and horizontal measurements. Trash was even exposed that was within the concrete.		
Elevation	730.65			



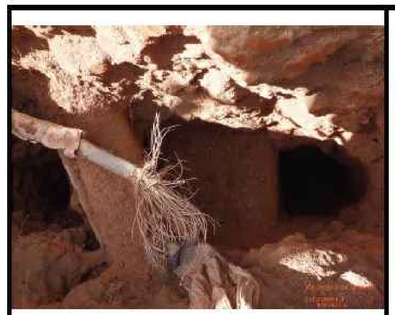
Sweetwater Utility Exploration
Test Hole Data Sheet

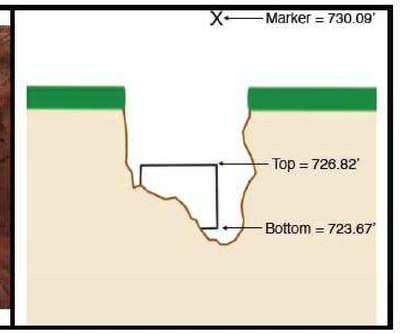
5030.055 — Date: 3/20/2025

Project:	NCANG Radio Tower	Test Hole #	3
Utility		**Hole Condition**	
Utility	Telephone Duct Bank	Surface Material	Grass
Size	24" x 38" +/-	Thickness	
Material	Rough Pour Concrete	Condition	
Color	Grey	Soil Type	Clay
Condition	Poor	Additional Information	
Width/O.D.	24"		

Depth and Elevation Measurement Information

Surface Marker	Hub & Tack	Utility	Top	Bottom
Set Over	Northern Most Edge	Depth	3.27	6.42
Northing	538605.7797	Elevation	726.82	723.67
Easting	1423601.8079	***In addition to the duct bank the crew exposed at this location a know storm drain pipe, a cut copper phone line and trash / debris above the duct bank.		
Elevation	730.09			





THIS DRAWING CONTAINS 2 SHEETS AND IS CONSIDERED INCOMPLETE WITHOUT THE 2 SHEETS TOGETHER.
SEE SHEET 1 FOR THE TOPOGRAPHY, NOTES, AND CERTS.

SURVEYOR'S CERTIFICATE

"I, JOHN M. STORY, CERTIFY THAT THIS PROJECT WAS COMPLETED UNDER MY DIRECT AND RESPONSIBLE CHARGE FROM AN ACTUAL SURVEY MADE UNDER MY SUPERVISION; THAT THIS SURVEY WAS PERFORMED TO MEET THE REQUIREMENTS FOR A PLANIMETRIC SURVEY TO THE ACCURACY OF CLASS A AND VERTICAL ACCURACY WHEN APPLICABLE TO THE CLASS A STANDARD, AND THAT THE ORIGINAL DATA WAS OBTAINED ON JANUARY 10–11, 2022; THAT THE SURVEY WAS COMPLETED ON JANUARY 26, 2022, LAST REVISED FEBRUARY 26, 2025; AND ALL COORDINATES ARE BASED ON NC GRID 'NAD 83'(2011) AND AND ALL ELEVATIONS ARE BASED ON NAVD 88 (GEOID18); AND THAT THIS MAP MEETS THE REQUIREMENTS OF THE STANDARDS OF PRACTICE FOR LAND SURVEYING IN NORTH CAROLINA (21 NCAC 56.1606)."

WITNESS MY ORIGINAL SIGNATURE, REGISTRATION NUMBER AND SEAL THIS 26TH DAY OF JANUARY A.D. 2022."

DocuSigned by:
JOHN M. STORY NC LAND SURVEYOR L–3840
1AF1982038D84F1...

March 31, 2025
DATE

NORTH CAROLINA PROFESSIONAL SEAL L–3840 LAND SURVEYOR JOHN M. STORY

20 0 20 40 60
GRAPHIC SCALE IN FEET

TOPOGRAPHIC SURVEY
FOR
AECOM
NORTH CAROLINA AIR NATIONAL GUARD BASE
CHARLOTTE/DOUGLAS INTERNATIONAL AIRPORT

SHEET 2 OF 2

CHARLOTTE/MECKLENBURG COUNTY — NORTH CAROLINA

02/26/2025 – ADD UTILITY LOCATIONS	DWN.BY: STAFF
03/31/2025 – ADD SOFT DIG LOCATIONS, SHEET 2	CKD.BY JMS
	FIELDBOOK N/A
	PLS NO. L–3840

Donaldson Garrett & Associates, Inc.
MACON • CHARLOTTE
9741-L SOUTHERN PINE BOULEVARD
CHARLOTTE, N.C. 28273
(704) 374–1955
http://www.dg-a-anc.com
John.Story@dg-anc.com
NC CORPORATE LICENSE NO. C–1518

DATE:	JANUARY 25, 2022
SCALE:	1"=20'
PROJECT NO.	5292–051–N1
DRAWING NO.	NC–009–22–D

THESE DOCUMENTS, AS INSTRUMENTS OF SERVICE, REMAIN THE PROPERTY OF D, G & A AND NO PART THEREOF MAY BE USED OR REPRODUCED IN ANY FORM WITHOUT WRITTEN PERMISSION.

S:\Working\5292–AECOM\051 (N1539) CONSTRUCT SECURITY FORCES BUILDING–145TH NCANG\Drawing\N1539 AS–BUILT WITH UTILITIES SHOWING THE 3 POT HOLES 03.31.2025 REV2.dwg
4/2/2025 8:47:36 PM BY: JOHN STORY

SECTION TABLE OF CONTENTS

DIVISION 31 - EARTHWORK

SECTION 31 23 00.00 20

EXCAVATION AND FILL

PART 1 GENERAL

1.1 NCDOT
1.2 SUBMITTALS

-- End of Section Table of Contents --

SECTION 31 23 00.00 20

EXCAVATION AND FILL

PART 1 GENERAL

1.1 NCDOT

Perform work in accordance with NCDOT Standard Specifications for Roads and Structures.

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval.

Provide material submittals for engineer review.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 32 - EXTERIOR IMPROVEMENTS

SECTION 32 12 16.16

ROAD-MIX ASPHALT PAVING

PART 1 GENERAL

1.1 NCDOT
1.2 SUBMITTALS
1.3 ACCEPTANCE
1.3.1 Acceptance Requirements

PART 2 PRODUCTS

PART 3 EXECUTION

3.1 CONTRACTOR QUALITY CONTROL
3.1.1 Quality Control Testing

-- End of Section Table of Contents --

SECTION 32 12 16.16

ROAD-MIX ASPHALT PAVING

PART 1 GENERAL

1.1 NCDOT

Perform work in accordance with NCDOT Standard Specifications for Roads and Structures.

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-03 Product Data

Contractor Quality Control; G

1.3 ACCEPTANCE

1.3.1 Acceptance Requirements

Provide all sampling and testing required for acceptance. Where appropriate, for individual lots of asphalt pavement will be made based on laboratory air voids, in-place density, smoothness, and grade in accordance with the following paragraphs. Surface smoothness and grade determinations will be made on the lot as a whole. Exceptions or adjustments to this will be made in situations where the mix within one lot is placed as part of both the intermediate and surface courses, thus smoothness and grade measurements for the entire lot cannot be made.

PART 2 PRODUCTS

NOT USED

PART 3 EXECUTION

3.1 CONTRACTOR QUALITY CONTROL

3.1.1 Quality Control Testing

Perform all quality control tests applicable to these specifications and as set forth in the Quality Control Program. Use the independent commercial laboratory for acceptance testing in paragraph ACCEPTANCE. Use in-house capabilities or the independent commercial laboratory for quality control testing. Required elements of the testing program include, but are not limited to tests for the control of asphalt content, aggregate gradation, aggregate moisture, moisture in the asphalt mixture, temperatures, VMA, and in-place density. Develop a Quality Control Testing Plan as part of the Quality Control Program.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 32 - EXTERIOR IMPROVEMENTS

SECTION 32 13 13.06

PORTLAND CEMENT CONCRETE PAVEMENT FOR ROADS AND SITE FACILITIES

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 QUALITY CONTROL
1.3.1 Qualifications
1.3.1.1 Laboratory Accreditation
1.3.1.2 Field Technicians
1.3.2 Batch Tickets
1.4 DELIVERY, STORAGE, AND HANDLING
1.5 ACCEPTANCE

-- End of Section Table of Contents --

SECTION 32 13 13.06

PORTLAND CEMENT CONCRETE PAVEMENT FOR ROADS AND SITE FACILITIES

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ASTM INTERNATIONAL (ASTM)

ASTM C94/C94M	(2022a) Standard Specification for Ready-Mixed Concrete
ASTM C1077	(2017) Standard Practice for Agencies Testing Concrete and Concrete Aggregates for Use in Construction and Criteria for Testing Agency Evaluation

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-07 Certificates

Batch Tickets

1.3 QUALITY CONTROL

1.3.1 Qualifications

1.3.1.1 Laboratory Accreditation

Perform sampling and testing using an approved commercial testing laboratory or on-site facilities that are accredited in accordance with ASTM C1077. Do not start work requiring testing until the facilities have been inspected and approved. The Government will inspect all laboratories requiring validation for equipment and test procedures prior to the start of any concreting operations for conformance to ASTM C1077. Schedule and provide payment for laboratory inspections. Additional payment or a time extension due to failure to acquire the required laboratory validation is not allowed. Maintain this certification for the duration of the project.

1.3.1.2 Field Technicians

Provide field technicians meeting one of the following criteria:

a. Have at least one National Ready Mixed Concrete Association (NRMCA) certified concrete craftsman and at least one American Concrete

Institute (ACI) Flatwork Finisher Certified craftsman on site, overseeing each placement crew during all concrete placement.

b. Have no less than three NRMCA certified concrete installers and at least two American Concrete Institute (ACI) Flatwork Finisher Certified installers on site working as members of each placement crew during all concrete placement.

1.3.2 Batch Tickets

Submit batch tickets for each load of ready-mixed concrete in accordance with ASTM C94/C94M.

1.4 DELIVERY, STORAGE, AND HANDLING

Deliver concrete paving in accordance with ASTM C94/C94M.

1.5 ACCEPTANCE

Work to be performed in accordance with NCDOT Standard Specifications for Roads and Structures.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 32 - EXTERIOR IMPROVEMENTS

SECTION 32 16 19

CONCRETE CURBS, GUTTERS AND SIDEWALKS

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 EQUIPMENT, TOOLS, AND MACHINES
1.3.1 General Requirements
1.3.2 Slip Form Equipment
1.4 ENVIRONMENTAL REQUIREMENTS
1.4.1 Placing During Cold Weather
1.4.2 Placing During Warm Weather

PART 2 PRODUCTS

2.1 CONCRETE
2.1.1 Air Content
2.1.2 Slump
2.1.3 Reinforcement Steel
2.2 CONCRETE CURING MATERIALS
2.2.1 Impervious Sheet Materials
2.2.2 Burlap
2.2.3 White Pigmented Membrane-Forming Curing Compound
2.3 CONCRETE PROTECTION MATERIALS
2.4 JOINT FILLER STRIPS
2.4.1 Contraction Joint Filler for Curb and Gutter
2.4.2 Expansion Joint Filler, Premolded
2.5 JOINT SEALANTS
2.6 FORM WORK
2.6.1 Wood Forms
2.6.2 Steel Forms
2.6.3 Sidewalk Forms
2.6.4 Curb and Gutter Forms
2.6.5 Biodegradable Form Release Agent
2.7 Detectable Warning System

PART 3 EXECUTION

3.1 SUBGRADE PREPARATION
3.1.1 Sidewalk Subgrade
3.1.2 Curb and Gutter Subgrade
3.1.3 Maintenance of Subgrade
3.2 FORM SETTING
3.2.1 Sidewalks
3.2.2 Curbs and Gutters
3.3 SIDEWALK CONCRETE PLACEMENT AND FINISHING
3.3.1 Formed Sidewalks
3.3.2 Concrete Finishing

3.3.3 Edge and Joint Finishing
3.3.4 Surface and Thickness Tolerances
3.4 CURB AND GUTTER CONCRETE PLACEMENT AND FINISHING
3.4.1 Formed Curb and Gutter
3.4.2 Curb and Gutter Finishing
3.4.3 Concrete Finishing
3.4.4 Joint Finishing
3.4.5 Surface and Thickness Tolerances
3.5 SIDEWALK JOINTS
3.5.1 Sidewalk Contraction Joints
3.5.2 Sidewalk Expansion Joints
3.5.3 Reinforcement Steel Placement
3.6 CURB AND GUTTER JOINTS
3.6.1 Contraction Joints
3.6.2 Expansion Joints
3.7 CURING AND PROTECTION
3.7.1 General Requirements
3.7.1.1 Mat Method
3.7.1.2 Impervious Sheeting Method
3.7.1.3 Membrane Curing Method
3.7.2 Backfilling
3.7.3 Protection
3.7.4 Protective Coating
3.7.4.1 Application
3.7.4.2 Precautions
3.8 FIELD QUALITY CONTROL
3.8.1 General Requirements
3.8.2 Concrete Testing
3.8.2.1 Strength Testing
3.8.2.2 Air Content
3.8.2.3 Slump Test
3.8.3 Thickness Evaluation
3.8.4 Surface Evaluation
3.9 SURFACE DEFICIENCIES AND CORRECTIONS
3.9.1 Thickness Deficiency
3.9.2 High Areas
3.9.3 Appearance
3.10 DETECTABLE WARNING SYSTEM

-- End of Section Table of Contents --

SECTION 32 16 19

CONCRETE CURBS, GUTTERS AND SIDEWALKS

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN ASSOCIATION OF STATE HIGHWAY AND TRANSPORTATION OFFICIALS (AASHTO)

AASHTO M 182	(2005; R 2017) Standard Specification for Burlap Cloth Made from Jute or Kenaf and Cotton Mats

ASTM INTERNATIONAL (ASTM)

ASTM A615/A615M	(2022) Standard Specification for Deformed and Plain Carbon-Steel Bars for Concrete Reinforcement
ASTM A1064/A1064M	(2017) Standard Specification for Carbon-Steel Wire and Welded Wire Reinforcement, Plain and Deformed, for Concrete
ASTM C31/C31M	(2022) Standard Practice for Making and Curing Concrete Test Specimens in the Field
ASTM C94/C94M	(2022a) Standard Specification for Ready-Mixed Concrete
ASTM C143/C143M	(2020) Standard Test Method for Slump of Hydraulic-Cement Concrete
ASTM C171	(2020) Standard Specification for Sheet Materials for Curing Concrete
ASTM C172/C172M	(2017) Standard Practice for Sampling Freshly Mixed Concrete
ASTM C173/C173M	(2016) Standard Test Method for Air Content of Freshly Mixed Concrete by the Volumetric Method
ASTM C231/C231M	(2022) Standard Test Method for Air Content of Freshly Mixed Concrete by the Pressure Method
ASTM C309	(2019) Standard Specification for Liquid Membrane-Forming Compounds for Curing Concrete

ASTM C920	(2018) Standard Specification for Elastomeric Joint Sealants
ASTM D1751	(2018) Standard Specification for Preformed Expansion Joint Filler for Concrete Paving and Structural Construction (Nonextruding and Resilient Bituminous Types)
ASTM D1752	(2018) Standard Specification for Preformed Sponge Rubber, Cork and Recycled PVC Expansion Joint Fillers for Concrete Paving and Structural Construction
ASTM D5893/D5893M	(2016) Standard Specification for Cold Applied, Single Component, Chemically Curing Silicone Joint Sealant for Portland Cement Concrete Pavements

INTERNATIONAL CODE COUNCIL (ICC)

ICC A117.1	(2017) Standard And Commentary Accessible and Usable Buildings and Facilities

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-03 Product Data

Concrete

Biodegradable Form Release Agent

SD-06 Test Reports

Field Quality Control

1.3 EQUIPMENT, TOOLS, AND MACHINES

1.3.1 General Requirements

Plant, equipment, machines, and tools used in the work will be subject to approval and must be maintained in a satisfactory working condition at all times. Use equipment capable of producing the required product, meeting grade controls, thickness control and smoothness requirements as specified. Discontinue using equipment that produces unsatisfactory results. Allow the Contracting Officer access at all times to the plant and equipment to ensure proper operation and compliance with specifications.

1.3.2 Slip Form Equipment

Slip form paver or curb forming machines, will be approved based on trial use on the job and must be self-propelled, automatically controlled,

crawler mounted, and capable of spreading, consolidating, and shaping the plastic concrete to the desired cross section in one pass.

1.4 ENVIRONMENTAL REQUIREMENTS

1.4.1 Placing During Cold Weather

Do not place concrete when the air temperature reaches 40 degrees F and is falling, or is already below that point. Placement may begin when the air temperature reaches 35 degrees F and is rising, or is already above 40 degrees F. Make provisions to protect the concrete from freezing during the specified curing period. If necessary to place concrete when the temperature of the air, aggregates, or water is below 35 degrees F, placement and protection must be approved in writing. Approval will be contingent upon full conformance with the following provisions. Prepare and protect the underlying material so that it is entirely free of frost when the concrete is deposited. Heat mixing water and aggregates mixing water aggregates as necessary to result in the temperature of the in-place concrete being between 50 and 85 degrees F. Methods and equipment for heating must be approved. Use only aggregates that are free of ice, snow, and frozen lumps before entering the mixer. Provide covering or other means as needed to maintain the concrete at a temperature of at least 50 degrees F for not less than 72 hours after placing, and at a temperature above freezing for the remainder of the curing period.

1.4.2 Placing During Warm Weather

The temperature of the concrete as placed must not exceed 85 degrees F except where an approved retarder is used. Cool the mixing water and aggregates as necessary to maintain a satisfactory placing temperature. The placing temperature must not exceed 95 degrees F at any time.

PART 2 PRODUCTS

2.1 CONCRETE

Provide concrete conforming to the applicable requirements of Section 03 30 00 CAST-IN-PLACE CONCRETE in accordance with ASTM C94/C94M except as otherwise specified. Concrete must have a minimum compressive strength of 3500 psi at 28 days. Size of aggregate must not exceed 1-1/2 inches. Submit copies of certified delivery tickets for all concrete used in the construction.

2.1.1 Air Content

Use concrete mixtures that have an air content by volume of concrete of 5 to 7 percent, based on measurements made immediately after discharge from the mixer.

2.1.2 Slump

Use concrete with a slump of 3 inches plus or minus 1 inch for hand placed concrete or 1 inch plus or minus 1/2 inch for slipformed concrete as determined in accordance with ASTM C143/C143M.

2.1.3 Reinforcement Steel

Use reinforcement bars conforming to ASTM A615/A615M. Use wire mesh reinforcement conforming to ASTM A1064/A1064M.

2.2 CONCRETE CURING MATERIALS

2.2.1 Impervious Sheet Materials

Use impervious sheet materials conforming to ASTM C171, type optional, except that polyethylene film, if used, must be white opaque.

2.2.2 Burlap

Use burlap conforming to AASHTO M 182.

2.2.3 White Pigmented Membrane-Forming Curing Compound

Use white pigmented membrane-forming curing compound conforming to ASTM C309, Type 2.

2.3 CONCRETE PROTECTION MATERIALS

Use concrete protection materials consisting of a linseed oil mixture of equal parts, by volume, of linseed oil and either mineral spirits, naphtha, or turpentine. At the option of the Contractor, commercially prepared linseed oil mixtures, formulated specifically for application to concrete to provide protection against the action of deicing chemicals may be used, except that emulsified mixtures are not acceptable.

2.4 JOINT FILLER STRIPS

2.4.1 Contraction Joint Filler for Curb and Gutter

Use hard-pressed fiberboard contraction joint filler for curb and gutter.

2.4.2 Expansion Joint Filler, Premolded

Unless otherwise indicated, use 1/2 inch thick premolded expansion joint filler conforming to ASTM D1751 or ASTM D1752.

2.5 JOINT SEALANTS

Use cold-applied joint sealant conforming to ASTM C920 or ASTM D5893/D5893M.

2.6 FORM WORK

Design and construct form work to ensure that the finished concrete will conform accurately to the indicated dimensions, lines, and elevations, and within the tolerances specified. Use wood or steel forms that are straight and of sufficient strength to resist springing during depositing and consolidating concrete.

2.6.1 Wood Forms

Use forms that are surfaced plank, 2 inches nominal thickness, straight and free from warp, twist, loose knots, splits or other defects. Use forms with a nominal length of 10 feet. Radius bends may be formed with 3/4 inch boards, laminated to the required thickness.

2.6.2 Steel Forms

Use channel-formed sections with a flat top surface and welded braces at

each end and at not less than two intermediate points. Use forms with interlocking and self-aligning ends. Provide flexible forms for radius forming, corner forms, form spreaders, and fillers as needed. Use forms with a nominal length of 10 feet and that have a minimum of 3 welded stake pockets per form. Use stake pins consisting of solid steel rods with chamfered heads and pointed tips designed for use with steel forms.

2.6.3 Sidewalk Forms

Use sidewalk forms that are of a height equal to the full depth of the finished sidewalk.

2.6.4 Curb and Gutter Forms

Use curb and gutter outside forms that have a height equal to the full depth of the curb or gutter. Use rigid forms for curb returns, except that benders or thin plank forms may be used for curb or curb returns with a radius of 10 feet or more, where grade changes occur in the return, or where the central angle is such that a rigid form with a central angle of 90 degrees cannot be used. Back forms for curb returns may be made of 1-1/2 inch benders, for the full height of the curb, cleated together. In lieu of inside forms for curbs, a curb "mule" may be used for forming and finishing this surface, provided the results are approved.

2.6.5 Biodegradable Form Release Agent

Use form release agent that is colorless and biodegradable and that is composed of at least 87 percent biobased material. Provide product that does not bond with, stain, or adversely affect concrete surfaces and does not impair subsequent treatments of concrete surfaces. Provide form release agent that does not contain diesel fuel, petroleum-based lubricating oils, waxes, or kerosene.

2.7 Detectable Warning System

Detectable Warning Systems shown on the Contract plans are to meet requirements of ICC A117.1 - Section 705.

PART 3 EXECUTION

3.1 SUBGRADE PREPARATION

Construct subgrade to the specified grade and cross section prior to concrete placement.

3.1.1 Sidewalk Subgrade

Place and compact the subgrade in accordance with Section 31 00 00 EARTHWORK. Test the subgrade for grade and cross section with a template extending the full width of the sidewalk and supported between side forms.

3.1.2 Curb and Gutter Subgrade

Place and compact the subgrade in accordance with Section 31 00 00 EARTHWORK and Section 31 23 00.00 20 EXCAVATION AND FILL. Test the subgrade for grade and cross section by means of a template extending the full width of the curb and gutter. Use subgrade materials equal in bearing quality to the subgrade under the adjacent pavement.

3.1.3 Maintenance of Subgrade

Maintain subgrade in a smooth, compacted condition in conformity with the required section and established grade until the concrete is placed. The subgrade must be in a moist condition when concrete is placed. Prepare and protect subgrade so that it is free from frost when the concrete is deposited.

3.2 FORM SETTING

Set forms to the indicated alignment, grade and dimensions. Hold forms rigidly in place by a minimum of 3 stakes per form placed at intervals not to exceed 4 feet. Use additional stakes and braces at corners, deep sections, and radius bends, as required. Use clamps, spreaders, and braces where required to ensure rigidity in the forms. Remove forms in a manner that will not injure the concrete. Do not use bars or heavy tools against the concrete when removing the forms. Promptly and satisfactorily repair concrete found to be defective after form removal. Clean forms and coat with form oil or biodegradable form release agent each time before concrete is placed. Wood forms may, instead, be thoroughly wetted with water before concrete is placed, except that with probable freezing temperatures, oiling is mandatory.

3.2.1 Sidewalks

Set forms for sidewalks with the upper edge true to line and grade with an allowable tolerance of 1/8 inch in any 10 foot long section. After forms are set, grade and alignment must be checked with a 10 foot straightedge. Sidewalks must have a transverse slope Unless otherwise indicated, construct sidewalks that are located adjacent to curbs with the low side adjacent to the curb. Do not remove side forms less than 12 hours after finishing has been completed.

3.2.2 Curbs and Gutters

Remove forms used along the front of the curb not less than 2 hours nor more than 6 hours after the concrete has been placed. Do not remove forms used along the back of curb until the face and top of the curb have been finished, as specified for concrete finishing. Do not remove gutter forms while the concrete is sufficiently plastic to slump in any direction.

3.3 SIDEWALK CONCRETE PLACEMENT AND FINISHING

3.3.1 Formed Sidewalks

Place concrete in the forms in one layer. When consolidated and finished, the sidewalks must be of the thickness indicated. Use a strike-off guided by side forms after concrete has been placed in the forms to bring the surface to proper section to be compacted. Consolidate concrete by tamping and spading or with an approved vibrator. Finish the surface to grade with a strike off.

3.3.2 Concrete Finishing

After straightedging, when most of the water sheen has disappeared, and just before the concrete hardens, finish the surface with a wood or magnesium float or darby to a smooth and uniformly fine granular or sandy texture free of waves, irregularities, or tool marks. Produce a scored surface by brooming with a fiber-bristle brush in a direction transverse

to that of the traffic, followed by edging.

3.3.3 Edge and Joint Finishing

Finish all slab edges, including those at formed joints, with an edger having a radius of 1/8 inch. Edge transverse joints before brooming. Eliminate the flat surface left by the surface face of the edger with brooming. Clean and solidly fill corners and edges which have crumbled and areas which lack sufficient mortar for proper finishing with a properly proportioned mortar mixture and then finish.

3.3.4 Surface and Thickness Tolerances

Finished surfaces must not vary more than 5/16 inch from the testing edge of a 10-foot straightedge. Permissible deficiency in section thickness will be up to 1/4 inch.

3.4 CURB AND GUTTER CONCRETE PLACEMENT AND FINISHING

3.4.1 Formed Curb and Gutter

Place concrete to the required section in a single lift. Consolidate concrete using approved mechanical vibrators. Curve shaped gutters must be finished with a standard curb "mule".

3.4.2 Curb and Gutter Finishing

Approved slipformed curb and gutter machines may be used in lieu of hand placement.

3.4.3 Concrete Finishing

Float and finish exposed surfaces with a smooth wood float until true to grade and section and uniform in texture. Brush floated surfaces with a fine-hair brush using longitudinal strokes. Round the edges of the gutter and top of the curb with an edging tool to a radius of 1/2 inch. Immediately after removing the front curb form, rub the face of the curb with a wood or concrete rubbing block and water until blemishes, form marks, and tool marks have been removed. Brush the front curb surface, while still wet, in the same manner as the gutter and curb top. Finish the top surface of gutter and entrance to grade with a wood float.

3.4.4 Joint Finishing

Finish curb edges at formed joints as indicated.

3.4.5 Surface and Thickness Tolerances

Finished surfaces must not vary more than 1/4 inch from the testing edge of a 10-foot straightedge. Permissible deficiency in section thickness will be up to 1/4 inch.

3.5 SIDEWALK JOINTS

Construct sidewalk joints to divide the surface into rectangular areas. Space transverse contraction joints at a distance equal to the sidewalk width or 5 feet on centers, whichever is less, and continuous across the slab. Construct longitudinal contraction joints along the centerline of all sidewalks 10 feet or more in width. Construct transverse expansion

joints at sidewalk returns and opposite expansion joints in adjoining curbs. Where the sidewalk is not in contact with the curb, install transverse expansion joints as indicated. Form expansion joints around structures and features which project through or into the sidewalk pavement, using joint filler of the type, thickness, and width indicated. Expansion joints are not required between sidewalks and curb that abut the sidewalk longitudinally.

3.5.1 Sidewalk Contraction Joints

Form contraction joints in the fresh concrete by cutting a groove in the top portion of the slab to a depth of at least one-fourth of the sidewalk slab thickness. Unless otherwise approved or indicated, either use a jointer to cut the groove or saw a groove in the hardened concrete with a power-driven saw. Construct sawed joints by sawing a groove in the concrete with a 1/8 inch blade. Provide an ample supply of saw blades on the jobsite before concrete placement is started. Provide at least one standby sawing unit in good working order at the jobsite at all times during the sawing operations.

3.5.2 Sidewalk Expansion Joints

Form expansion joints using 1/2 inch joint filler strips. Joint filler in expansion joints surrounding structures and features within the sidewalk may consist of preformed filler material conforming to ASTM D1752 or building paper. Hold joint filler in place with steel pins or other devices to prevent warping of the filler during floating and finishing. Immediately after finishing operations are completed, round joint edges using an edging tool having a radius of 1/8 inch. Remove any concrete over the joint filler. At the end of the curing period, clean the top of expansion joints and fill with cold-applied joint sealant. Use joint sealant that is gray or stone in color. Thoroughly clean the joint opening before the sealing material is placed. Do not spill sealing material on exposed surfaces of the concrete. Apply joint sealing material only when the concrete at the joint is surface dry and atmospheric and concrete temperatures are above 50 degrees F. Immediately remove any excess material on exposed surfaces of the concrete and clean the concrete surfaces.

3.5.3 Reinforcement Steel Placement

Accurately and securely fasten reinforcement steel in place with suitable supports and ties before the concrete is placed.

3.6 CURB AND GUTTER JOINTS

Construct curb and gutter joints at right angles to the line of curb and gutter.

3.6.1 Contraction Joints

Construct contraction joints directly opposite contraction joints in abutting portland cement concrete pavements and spaced so that monolithic sections between curb returns will not be less than 5 feet nor greater than 15 feet in length.

a. Construct contraction joints (except for slip forming) by means of 1/8 inch thick separators and of a section conforming to the cross section of the curb and gutter. Remove separators as soon as practicable

after concrete has set sufficiently to preserve the width and shape of the joint and prior to finishing.

b. When slip forming is used, cut the contraction joints in the top portion of the gutter/curb hardened concrete in a continuous cut across the curb and gutter, using a power-driven saw. Cut the contraction joint to a depth of at least one-fourth of the gutter/curb depth using a 1/8 inch saw blade.

3.6.2 Expansion Joints

Form expansion joints by means of preformed expansion joint filler material cut and shaped to the cross section of curb and gutter. Construct expansion joints in curb and gutter directly opposite expansion joints of abutting portland cement concrete pavement using the same type and thickness of joints as joints in the pavement. Where curb and gutter do not abut portland cement concrete pavement, provide expansion joints at least 1/2 inch in width at intervals not less than 30 feet nor greater than 120 feet. Seal expansion joints immediately following curing of the concrete or as soon thereafter as weather conditions permit. Seal expansion joints and the top 1 inch depth of curb and gutter contraction-joints with joint sealant. Thoroughly clean the joint opening before the sealing material is placed. Do not spill sealing material on exposed surfaces of the concrete. Concrete at the joint must be surface dry and atmospheric and concrete temperatures must be above 50 degrees F at the time of application of joint sealing material. Immediately remove excess material on exposed surfaces of the concrete and clean concrete surfaces.

3.7 CURING AND PROTECTION

3.7.1 General Requirements

Protect concrete against loss of moisture and rapid temperature changes for at least 7 days from the beginning of the curing operation. Protect unhardened concrete from rain and flowing water. All equipment needed for adequate curing and protection of the concrete must be on hand and ready for use before actual concrete placement begins. Protect concrete as necessary to prevent cracking of the pavement due to temperature changes during the curing period.

3.7.1.1 Mat Method

Cover the entire exposed surface with two or more layers of burlap. Overlap mats at least 6 inches. Thoroughly wet the mat with water prior to placing on concrete surface and keep the mat continuously in a saturated condition and in intimate contact with concrete for not less than 7 days.

3.7.1.2 Impervious Sheeting Method

Wet the entire exposed surface with a fine spray of water and then cover with impervious sheeting material. Lay sheets directly on the concrete surface with the light-colored side up and overlapped 12 inches when a continuous sheet is not used. Use sheeting that is not less than 18-inches wider than the concrete surface to be cured. Secure sheeting using heavy wood planks or a bank of moist earth placed along edges and laps in the sheets. Satisfactorily repair or replace sheets that are torn or otherwise damaged during curing. Sheeting must remain on the concrete

surface to be cured for not less than 7 days.

3.7.1.3 Membrane Curing Method

Apply a uniform coating of white-pigmented membrane-curing compound to the entire exposed surface of the concrete as soon after finishing as the free water has disappeared from the finished surface. Coat formed surfaces immediately after the forms are removed and in no case longer than 1 hour after the removal of forms. Do not allow concrete surface to dry before application of the membrane. If drying has occurred, moisten the surface of the concrete with a fine spray of water and apply the curing compound as soon as the free water disappears. Apply curing compound in two coats by hand-operated pressure sprayers at a coverage of approximately 200 square feet/gallon for the total of both coats. Apply the second coat in a direction approximately at right angles to the direction of application of the first coat. The compound must form a uniform, continuous, coherent film that will not check, crack, or peel and must be free from pinholes or other imperfections. If pinholes, abrasion, or other discontinuities exist, apply an additional coat to the affected areas within 30 minutes. Respray concrete surfaces that are subjected to heavy rainfall within 3 hours after the curing compound has been applied by the method and at the coverage specified above. Respray areas where the curing compound is damaged by subsequent construction operations within the curing period. Take precautions necessary to ensure that the concrete is properly cured at sawed joints, and that no curing compound enters the joints. Tightly seal the top of the joint opening and the joint groove at exposed edges before the concrete in the region of the joint is resprayed with curing compound. Use a method used for sealing the joint groove that prevents loss of moisture from the joint during the entire specified curing period. Provide approved standby facilities for curing concrete pavement at a location accessible to the jobsite for use in the event of mechanical failure of the spraying equipment or other conditions that might prevent correct application of the membrane-curing compound at the proper time. Adequately protect concrete surfaces to which membrane-curing compounds have been applied during the entire curing period from pedestrian and vehicular traffic, except as required for joint-sawing operations and surface tests, and from other possible damage to the continuity of the membrane.

3.7.2 Backfilling

After curing, remove debris and backfill, grade, and compact the area adjoining the concrete to conform to the surrounding area in accordance with lines and grades indicated.

3.7.3 Protection

Protect completed concrete from damage until accepted. Repair damaged concrete and clean concrete discolored during construction. Remove and reconstruct concrete that is damaged for the entire length between regularly scheduled joints. Refinishing the damaged portion will not be acceptable. Dispose of removed material as directed.

3.7.4 Protective Coating

Apply a protective coating of linseed oil mixture to the exposed-to-view concrete surface after the curing period, if concrete will be exposed to de-icing chemicals within 6 weeks after placement. Moist cure concrete to receive a protective coating.

3.7.4.1 Application

Complete curing and backfilling operation prior to applying two coats of protective coating. Concrete must be surface dry and clean before each application. Spray apply at a rate of not more than 50 square yards/gallon for first application and not more than 70 square yards/gallon for second application, except that the number of applications and coverage for each application for commercially prepared mixture must be in accordance with the manufacturer's instructions. Protect coated surfaces from vehicular and pedestrian traffic until dry.

3.7.4.2 Precautions

Do not heat protective coating by direct application of flame or electrical heaters and protect the coating from exposure to open flame, sparks, and fire adjacent to open containers or applicators. Do not apply material at ambient or material temperatures lower than 50 degrees F.

3.8 FIELD QUALITY CONTROL

Submit copies of all test reports within 24 hours of completion of the test.

3.8.1 General Requirements

Perform the inspection and tests described and meet the specified requirements for inspection details and frequency of testing. Based upon the results of these inspections and tests, take the action and submit reports as required below, and additional tests to ensure that the requirements of these specifications are met.

3.8.2 Concrete Testing

3.8.2.1 Strength Testing

Take concrete samples in accordance with ASTM C172/C172M not less than once a day nor less than once for every 250 cubic yards of concrete placed. Mold cylinders in accordance with ASTM C31/C31M for strength testing by an approved laboratory. Each strength test result must be the average of 2 test cylinders from the same concrete sample tested at 28 days, unless otherwise specified or approved. Concrete specified on the basis of compressive strength will be considered satisfactory if the averages of all sets of three consecutive strength test results equal or exceed the specified strength, and no individual strength test result falls below the specified strength by more than 500 psi.

3.8.2.2 Air Content

Determine air content in accordance with ASTM C173/C173M or ASTM C231/C231M. Use ASTM C231/C231M with concretes and mortars made with relatively dense natural aggregates. Make two tests for air content on randomly selected batches of each class of concrete placed during each shift. Make additional tests when excessive variation in concrete workability is reported by the placing foreman or the Government inspector. Notify the placing foreman if results are out of tolerance. The placing foreman must take appropriate action to have the air content corrected at the plant. Additional tests for air content will be performed on each truckload of material until such time as the air content is within the tolerance

specified.

3.8.2.3 Slump Test

Perform two slump tests on randomly selected batches of each class of concrete for every 250 cubic yards, or fraction thereof, of concrete placed during each shift. Perform additional tests when excessive variation in the workability of the concrete is noted or when excessive crumbling or slumping is noted along the edges of slip-formed concrete.

3.8.3 Thickness Evaluation

Determine the anticipated thickness of the concrete prior to placement by passing a template through the formed section or by measuring the depth of opening of the extrusion template of the curb forming machine. If a slip form paver is used for sidewalk placement, construct the subgrade true to grade prior to concrete placement. The thickness will be determined by measuring each edge of the completed slab.

3.8.4 Surface Evaluation

Provide finished surfaces for each category of the completed work that are uniform in color and free of blemishes and form or tool marks.

3.9 SURFACE DEFICIENCIES AND CORRECTIONS

3.9.1 Thickness Deficiency

When measurements indicate that the completed concrete section is deficient in thickness by more than 1/4 inch the deficient section will be removed, between regularly scheduled joints, and replaced.

3.9.2 High Areas

In areas not meeting surface smoothness and plan grade requirements, reduce high areas either by rubbing the freshly finished concrete with carborundum brick and water when the concrete is less than 36 hours old or by grinding the hardened concrete with an approved surface grinding machine after the concrete is 36 hours old or more. The area corrected by grinding the surface of the hardened concrete must not exceed 5 percent of the area of any integral slab, and the depth of grinding must not exceed 1/4 inch. Remove and replace pavement areas requiring grade or surface smoothness corrections in excess of the limits specified.

3.9.3 Appearance

Exposed surfaces of the finished work will be inspected by the Contracting Officer and deficiencies in appearance will be identified. Remove and replace areas which exhibit excessive cracking, discoloration, form marks, or tool marks or which are otherwise inconsistent with the overall appearances of the work.

3.10 DETECTABLE WARNING SYSTEM

Install Detectable Warning Systems required by Contract plans in accordance with ICC A117.1, Section 705, and by manufacturers' installation instructions.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 32 - EXTERIOR IMPROVEMENTS

SECTION 32 17 23

PAVEMENT MARKINGS

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 QUALITY ASSURANCE
1.3.1 Regulatory Requirements
1.3.2 Qualifications
1.4 DELIVERY AND STORAGE
1.5 PROJECT/SITE CONDITIONS
1.5.1 Environmental Requirements
1.5.1.1 Weather Limitations for Application
1.5.1.2 Weather Limitations for Removal of Pavement Markings on Roads and Automotive Parking Areas
1.5.2 Traffic Controls
1.5.3 Lighting

PART 2 PRODUCTS

2.1 EQUIPMENT
2.1.1 Surface Preparation and Paint Removal
2.1.1.1 Surface Preparation Equipment for Roads and Automotive Parking Areas
2.1.1.1.1 Sandblasting Equipment
2.1.1.1.2 Waterblasting Equipment
2.1.2 Application Equipment
2.1.2.1 Paint Application Equipment
2.1.2.1.1 Hand-Operated, Push-Type Machines
2.1.2.1.2 Self-Propelled or Mobile-Drawn Spraying Machines
2.1.2.1.2.1 Hand Application
2.1.2.2 Thermoplastic Application Equipment
2.1.2.2.1 Application Equipment
2.1.2.2.2 Mobile Application Equipment
2.1.2.2.3 Portable Application Equipment
2.2 MATERIALS

PART 3 EXECUTION

3.1 EXAMINATION
3.1.1 Testing for Moisture
3.1.2 Surface Preparation Demonstration
3.1.3 Test Stripe Demonstration
3.1.4 Application Rate Demonstration
3.1.5 Level of Performance Demonstration
3.2 EXTERIOR SURFACE PREPARATION
3.3 APPLICATION
3.3.1 Paint

3.3.1.1 Solventborne Paint
3.3.2 Cleanup and Waste Disposal
3.4 FIELD QUALITY CONTROL
3.4.1 Material Inspection
3.4.2 Dimensional Tolerances
3.4.3 Bond Failure Verification
3.4.4 Reflective Media and Coating Application Verification

-- End of Section Table of Contents --

SECTION 32 17 23

PAVEMENT MARKINGS

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to in the text by the basic designation only.

ASTM INTERNATIONAL (ASTM)

ASTM D6628	(2003; R 2015) Standard Specification for Color of Pavement Marking Materials

SOCIETY OF AUTOMOTIVE ENGINEERS INTERNATIONAL (SAE)

SAE AMS-STD-595A	(2017) Colors used in Government Procurement

U.S. FEDERAL HIGHWAY ADMINISTRATION (FHWA)

MUTCD	(2009; Rev 2012) Manual on Uniform Traffic Control Devices

U.S. GENERAL SERVICES ADMINISTRATION (GSA)

FS TT-B-1325	(Rev D; Notice 1; Notice 2 2017) Beads (Glass Spheres) Retro-Reflective (Metric)

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-03 Product Data

Surface Preparation Equipment List; G

Application Equipment List; G

Exterior Surface Preparation

Safety Data Sheets; G

SD-07 Certificates

Qualifications; G

Volatile Organic Compound, (VOC); G

1.3 QUALITY ASSURANCE

1.3.1 Regulatory Requirements

Submit certificate stating that the proposed pavement marking paint meets the Volatile Organic Compound, (VOC) regulations of the local Air Pollution Control District having jurisdiction over the geographical area in which the project is located. Submit Safety Data Sheets for each product.

1.3.2 Qualifications

Submit documentation certifying that pertinent personnel are qualified for equipment operation and handling of applicable chemicals. The documentation should include experience on five projects of similar size and scope with references for all personnel.

1.4 DELIVERY AND STORAGE

Deliver paint materials, thermoplastic compound materials, and reflective media in original sealed containers that plainly show the designated name, specification number, batch number, color, date of manufacture, manufacturer's directions, and name of manufacturer.

Provide storage facilities at the job site for maintaining materials at temperatures recommended by the manufacturer.

1.5 PROJECT/SITE CONDITIONS

1.5.1 Environmental Requirements

1.5.1.1 Weather Limitations for Application

Apply pavement markings to clean, dry surfaces, and unless otherwise approved, only when the air and pavement surface temperature is at least 5 degrees F above the dew point and the air and pavement temperatures are within the limits recommended by the pavement marking manufacturer. Allow pavement surfaces to dry after water has been used for cleaning or rainfall has occurred prior to striping or marking. Test the pavement surface for moisture before beginning work each day and after cleaning. Do not commence marking until the pavement is sufficiently dry and the pavement condition has been approved by the Contracting Officer. Employ the "plastic wrap method" to test the pavement for moisture as specified in paragraph TESTING FOR MOISTURE.

1.5.1.2 Weather Limitations for Removal of Pavement Markings on Roads and Automotive Parking Areas

Pavement surface must be free of snow, ice, or slush; with a surface temperature of at least 40 degrees F and rising at the beginning of operations, except those involving shot or sand blasting or grinding. Cease operation during thunderstorms, or during rainfall, except for waterblasting and removal of previously applied chemicals. Cease waterblasting where surface water accumulation alters the effectiveness of material removal.

1.5.2 Traffic Controls

Place warning signs conforming to MUTCD near the beginning of the worksite

and well ahead of the worksite for alerting approaching traffic from both directions. Place small markers along newly painted lines or freshly placed raised markers to control traffic and prevent damage to newly painted surfaces or displacement of raised pavement markers. Mark painting equipment with large warning signs indicating slow-moving painting equipment in operation.

When traffic must be rerouted or controlled to accomplish the work, provide necessary warning signs, flag persons, and related equipment for the safe passage of vehicles.

1.5.3 Lighting

When night operations are necessary, provide all necessary lighting and equipment. Direct or shade lighting to prevent interference with aircraft, the air traffic control tower, and other base operations. Provide lighting and related equipment capable of being removed from the runway within 15 minutes of notification of an emergency. Night work must be coordinated with the Flight Operations Manager or Airfield Manager and approved in advance by the Contracting Officer. The Government reserves the right to accept or reject night work on the day following night activities by the Contractor.

PART 2 PRODUCTS

2.1 EQUIPMENT

2.1.1 Surface Preparation and Paint Removal

2.1.1.1 Surface Preparation Equipment for Roads and Automotive Parking Areas

Submit a surface preparation equipment list by serial number, type, model, and manufacturer. Include descriptive data indicating area of coverage per pass, pressure adjustment range, tank and flow capacities, and safety precautions required for the equipment operation. Mobile equipment must allow for removal of markings without damaging the pavement surface or joint sealant. Maintain machines, tools, and equipment used in the performance of the work in satisfactory operating condition.

2.1.1.1.1 Sandblasting Equipment

Use mobile sandblasting equipment capable of producing a pressurized stream of sand and air that effectively removes paint from the surface without filling voids with debris in asphalt or tar pavements or removing joint sealants in Portland cement concrete pavements. Include with the equipment and air compressor, hoses, and nozzles of adequate size and capacity for removing paint. Equip the compressor with traps and coalescing filters that maintain the compressed air free of oil and water.

2.1.1.1.2 Waterblasting Equipment

Use mobile waterblasting equipment capable of producing a pressurized stream of water that effectively removes paint from the pavement surface without significantly damaging the pavement. Provide equipment, tools, and machinery which are safe and in good working order at all times.

2.1.2 Application Equipment

Submit application equipment list appropriate for the material(s) to be used. Include manufacturer's descriptive data and certification for the planned use that indicates area of coverage per pass, pressure adjustment range, tank and flow capacities, and all safety precautions required for operating and maintaining the equipment. Provide and maintain machines, tools, and equipment used in the performance of the work in satisfactory operating condition, or remove them from the work site. Provide mobile and maneuverable application equipment to the extent that straight lines can be followed and normal curves can be made in a true arc.

2.1.2.1 Paint Application Equipment

2.1.2.1.1 Hand-Operated, Push-Type Machines

Provide hand-operated push-type applicator machine of a type commonly used for application of water based paint or two-component, chemically curing paint, thermoplastic, or preformed tape, to pavement surfaces for small marking projects, such as legends and cross-walks, automotive parking areas, or surface painted signs. Provide applicator machine equipped with the necessary tanks and spraying nozzles capable of applying paint uniformly at coverage specified. Hand operated spray guns may be used in areas where push-type machines cannot be used.

2.1.2.1.2 Self-Propelled or Mobile-Drawn Spraying Machines

Provide self-propelled or mobile-drawn spraying machine with suitable arrangements of atomizing nozzles and controls to obtain the specified results. Provide machine having a speed during application capable of applying the stripe widths indicated at the paint coverage rate specified herein and of even uniform thickness with clear-cut edges.

2.1.2.1.2.1 Hand Application

Provide spray guns for hand application of paint in areas where the mobile paint applicator cannot be used.

2.1.2.2 Thermoplastic Application Equipment

2.1.2.2.1 Application Equipment

a. Provide application equipment capable of continuous mixing and agitation of the material, with conveying parts which prevent accumulation and clogging between the main material reservoir and the extrusion shoe or spray gun. All parts of the equipment which come into contact with the material must be easily accessible and exposed for cleaning and maintenance. All mixing and conveying parts up to and including the extrusion shoes and spray guns must maintain the material at the required temperature with heat-transfer oil or electrical-element-controlled heat.

b. Provide application equipment constructed to ensure continuous uniformity in the dimensions of the stripe. Provide an applicator with a means for cleanly cutting off stripe ends squarely and providing a method of applying "skiplines." Provide equipment capable of applying varying widths of traffic markings.

c. Provide mobile and maneuverable application equipment allowing

straight lines to be followed and normal curves to be made in a true arc. Provide equipment used for the placement of thermoplastic pavement markings of two general types: mobile applicator and portable applicator.

d. Equip the applicator with a pressurized or drop-on type bead dispenser capable of uniformly dispensing reflective glass spheres at controlled rates of flow. The bead dispenser must operate automatically to begin flow prior to the flow of binder to assure that the strip is fully reflectorized.

2.1.2.2.2 Mobile Application Equipment

Provide a truck-mounted, self-contained pavement marking machine that is capable of hot applying thermoplastic by either the extrusion or spray method.

a. Equip the unit to apply the thermoplastic marking material at temperatures according to the manufacturer's instructions, at widths varying from 3 to 12 inches, with an automatic pressurized or drop-on bead dispensing system, capable of operating continuously, and of installing a minimum of 20,000 lineal feet of longitudinal markings in an 8-hour day.

b. Equip the mobile unit with a melting kettle which holds a minimum of 6000 pounds of molten thermoplastic material; capable of heating the thermoplastic composition to temperatures as recommended by the manufacturer. Use a thermostatically controlled heat transfer liquid. Heating of the composition by direct flame is not allowed. Oil and material temperature gauges must be visible at both ends of the kettle.

c. Equip mobile units for application of extruded markings with a minimum of two extrusion shoes; located one on each side of the truck, capable of marking simultaneous edge line and centerline stripes; each being a closed, oil-jacketed unit; holding the molten thermoplastic at a temperature as recommended by the manufacturer; and capable of extruding a line of 3 to 8 inches in width; and at a thickness of not less than 0.120 inch nor more than 0.190 inch, of generally uniform cross section.

d. Equip mobile units for application of spray markings with a spray gun system capable of marking simultaneous edgeline and centerline stripes. Surround (jacket) the spray system with heating oil to maintain the molten thermoplastic at a temperature of 375 to 425 degrees F, capable of spraying a stripe of 3 to 12 inches in width, and in thicknesses varying from 0.060 inch to 0.098 inch, of generally uniform cross section.

e. Equip the mobile unit with an electronic programmable line pattern control system, capable of applying skip or solid lines in any sequence, through any and all of the extrusion shoes, or the spray guns, and in programmable cycle lengths. In addition, equip the mobile unit with an automatic counting mechanism capable of recording the number of lineal feet of thermoplastic markings applied to the pavement surface with an accuracy of 0.5 percent.

2.1.2.2.3 Portable Application Equipment

Provide portable hand-operated equipment, specifically designed for placing special markings such as crosswalks, stop bars, legends, arrows, and short lengths of lane, edge and centerlines; and capable of applying thermoplastic pavement markings by the extrusion method. Equip the portable applicator with all the necessary components, including a materials storage reservoir, bead dispenser, extrusion shoe, and heating accessories, capable of holding the molten thermoplastic at the temperature recommended by the manufacturer, and of extruding a line of 3 to 12 inches in width, and in thickness of not less than 0.120 inch nor more than 0.190 inch and of generally uniform cross section.

2.2 MATERIALS

Use non-reflectorized waterborne or solventborne paint for automotive parking areas. The maximum allowable VOC content of pavement markings is 150 grams per liter. Color of markings are indicated on the drawings and must conform to ASTM D6628 for roads and automotive parking areas and SAE AMS-STD-595A for airfields. Provide materials conforming to the requirements specified herein.

PART 3 EXECUTION

3.1 EXAMINATION

3.1.1 Testing for Moisture

Test the pavement surface for moisture before beginning pavement marking after each period of rainfall, fog, high humidity, or cleaning, or when the ambient temperature has fallen below the dew point. Do not commence marking until the pavement is sufficiently dry and the pavement condition has been approved by the Contracting Officer or authorized representative.

Employ the "plastic wrap method" to test the pavement for moisture as follows: Cover the pavement with a 12 inch by 12 inch section of clear plastic wrap and seal the edges with tape. After 15 minutes, examine the plastic wrap for any visible moisture accumulation inside the plastic. Do not begin marking operations until the test can be performed with no visible moisture accumulation inside the plastic wrap. Re-test surfaces when work has been stopped due to rain.

3.1.2 Surface Preparation Demonstration

Prior to surface preparation, demonstrate the proposed procedures and equipment. Prepare areas large enough to determine cleanliness, adhesion of remaining coating and rate of cleaning. Perform a demonstration removal of pavement marking in an area designated by the Contracting Officer. Approved demonstration area establishes the standard for the remainder of the work.

3.1.3 Test Stripe Demonstration

Prior to paint application, demonstrate test stripe application within the work area using the proposed materials and equipment. Apply separate test stripes in each of the line widths and configurations required herein using the proposed equipment. Make the test stripes long enough to determine the proper speed and operating pressures for the vehicle(s) and machinery, but not less than 50 feet long.

3.1.4 Application Rate Demonstration

During the Test Stripe Demonstration, demonstrate compliance with the application rates specified herein. Document the equipment speed and operating pressures required to meet the specified rates in each configuration of the equipment and provide a copy of the documentation to the Contracting Officer prior to proceeding with the work.

3.1.5 Level of Performance Demonstration

The Contracting Officer will be present at the application demonstrations to observe the results obtained and to validate the operating parameters of the vehicle(s) and equipment. If accepted by the Contracting Officer, the test stripe is the measure of performance required for this project. Do not proceed with the work until the demonstration results are satisfactory to the Contracting Officer.

3.2 EXTERIOR SURFACE PREPARATION

Allow new pavement surfaces to cure for a period of not less than 30 days before application of marking materials. Thoroughly clean surfaces to be marked before application of the paint. Remove dust, dirt, and other granular surface deposits by sweeping, blowing with compressed air, rinsing with water, or a combination of these methods as required. Remove rubber deposits, existing paint markings, residual curing compounds, and other coatings adhering to the pavement by water blasting or approved chemical removal method.

3.3 APPLICATION

Apply pavement markings to dry pavements only.

3.3.1 Paint

Apply paint with approved equipment at rate of coverage specified herein. Provide guidelines and templates as necessary to control paint application. Take special precautions in marking numbers, letters, and symbols. Manually paint numbers, letters, and symbols. Sharply outline all edges of markings. The maximum drying time requirements of the paint specifications will be strictly enforced, to prevent undue softening of bitumen, and pickup, displacement, or discoloration by tires of traffic. If there is a deficiency in drying of the markings, painting operations must cease until the cause of the slow drying is determined and corrected.

3.3.1.1 Solventborne Paint

Apply paint at a minimum wet film thickness of 15 mils. Apply FS TT-B-1325 Type I (Gradation A) beads at a minimum rate of 6 pounds of glass spheres per gallon.

3.3.2 Cleanup and Waste Disposal

Keep the worksite clean and free of debris and waste from the removal and application operations. Dispose of debris at approved sites.

3.4 FIELD QUALITY CONTROL

3.4.1 Material Inspection

Examine material at the job site to determine that it is the material referenced in the report of test results or certificate of compliance. Provide test results substantiating conformance to the specified requirements with each certificate of compliance.

3.4.2 Dimensional Tolerances

Apply all markings in the standard dimensions provide in the drawings. New markings may deviate a maximum of 10 percent larger than the standard dimension. The maximum deviation allowed when painting over an old marking is up to 20 percent larger than the standard dimensions.

3.4.3 Bond Failure Verification

Inspect newly applied markings for signs of bond failure based on visual inspection and comparison to results from Test Stripe Demonstration paragraph.

3.4.4 Reflective Media and Coating Application Verification

Use a wet film thickness gauge to measure the application of wet paint. Use a microscope or magnifying glass to evaluate the embedment of glass beads in the paint. Verify the glass bead embedment with approximately 50 percent of the individual bead spheres embedded and 50 percent of the individual bead spheres exposed.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 32 - EXTERIOR IMPROVEMENTS

SECTION 32 34 13

FABRICATED PEDESTRIAN BRIDGES

PART 1 GENERAL

1.1 REFERENCES
1.2 GENERAL REQUIREMENTS
1.3 STRUCTURAL PERFORMANCE
1.3.1 Design Loads
1.3.1.1 Dead Loads
1.3.1.2 Pedestrian Live Load
1.3.1.3 Wind Loads
1.3.1.4 Top Chord Railing Loads
1.3.1.5 Safety Rails
1.3.1.6 Railing Infill
1.3.2 Design Limitations
1.3.2.1 Vertical Deflection
1.3.2.2 Horizontal Deflection
1.3.2.3 Vibration
1.3.2.4 Minimum Thickness of Metal
1.4 SUBMITTALS
1.5 QUALITY ASSURANCE
1.5.1 Qualifications
1.5.1.1 Fabricator's Qualifications
1.5.1.2 Engineer's Qualifications
1.5.2 Fabrication Drawing Requirements
1.5.3 Structural Calculations
1.5.4 Certifications
1.5.4.1 Welding Procedures and Qualifications

PART 2 PRODUCTS

2.1 MATERIALS
2.1.1 Unpainted Weathering Steel
2.1.2 Painted Steel
2.1.3 Galvanized Steel
2.1.4 Bolts
2.1.5 Concrete Deck
2.2 GENERAL DESIGN FEATURES
2.2.1 Span
2.2.2 Width
2.2.3 Truss Style
2.2.4 Maximum Weight
2.2.5 Member Components
2.2.6 Safety Rails
2.2.7 Camber
2.2.8 Elevation Difference
2.2.9 Stairs and Railings
2.3 FABRICATION

2.3.1 Bearing Devices
2.3.2 Foundations
2.4 FINISHING
2.4.1 Blast Cleaning
2.4.2 Painting
2.4.3 Galvanizing

PART 3 EXECUTION

3.1 CONNECTIONS
3.1.1 Welded Tubular Connections
3.2 WELDING
3.3 DELIVERY AND ERECTION

-- End of Section Table of Contents --

SECTION 32 34 13

FABRICATED PEDESTRIAN BRIDGES

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN ASSOCIATION OF STATE HIGHWAY AND TRANSPORTATION OFFICIALS (AASHTO)

AASHTO LRFD	(8th Edition; 2017) Bridge Design Specifications

AMERICAN INSTITUTE OF STEEL CONSTRUCTION (AISC)

AISC 325	(2017) Steel Construction Manual
AISC 360	(2016) Specification for Structural Steel Buildings

AMERICAN WELDING SOCIETY (AWS)

AWS A5.28	(2020) Specification For Low-Alloy Steel Electrodes and Rods for Gas Shielded Arc Welding
AWS D1.1/D1.1M	(2015) Structural Welding Code - Steel

ASTM INTERNATIONAL (ASTM)

ASTM A36/A36M	(2014) Standard Specification for Carbon Structural Steel
ASTM A123/A123M	(2017) Standard Specification for Zinc (Hot-Dip Galvanized) Coatings on Iron and Steel Products
ASTM A153	(2023) Standard Specification for Zinc Coating (Hot-Dip) on Iron and Steel Hardware
ASTM A242	(2024) Standard Specification for High-Strength Low-Alloy Structural Steel
ASTM A500	(2023) Standard Specification for Cold-Formed Welded and Seamless Carbon Steel Structural Tubing in Rounds and Shapes
ASTM A525	(2017) Standard Specification for General Requirements for Steel Sheet, Zinc-Coated

	(Galvanized) by the Hot-Dip Process
ASTM A572	(2021) Standard Specification for High-Strength Low-Alloy Columbium-Vanadium Structural Steel
ASTM A588	(2024) Standard Specification for High-Strength Low-Alloy Structural Steel, up to 50 ksi (345 MPa) Minimum Yield Point, with Atmospheric Corrosion Resistance
ASTM A606	(2023) Standard Specification for Steel, Sheet and Strip, High-Strength, Low-Alloy, Hot-Rolled and Cold-Rolled, with Improved Atmospheric Corrosion Resistance
ASTM A847	(2021) Standard Specification for Cold-Formed Welded and Seamless High-Strength, Low-Alloy Structural Tubing with Improved Atmospheric Corrosion Resistance
ASTM A992/A992M	(2011; Reapproved 2015) Standard Specification for Structural Steel Shapes
ASTM F3125	(2025) Standard Specification for High Strength Structural Bolts and Assemblies, Steel and Alloy Steel, Heat Treated, Inch Dimensions 120 ksi, 144 ksi, and 150 ksi Minimum Tensile Strength, and Metric Dimensions 830 MPa and 1040 MPa Minimum Tensile Strength
ASTM G101	(2020) Standard Guide for Estimating the Atmospheric Corrosion Resistance of Low-Alloy Steels

SOCIETY FOR PROTECTIVE COATINGS (SSPC)

SSPC-SP 7	(2006) Brush-off Blast Cleaning

1.2 GENERAL REQUIREMENTS

Design and construct a fabricated pedestrian bridge of size, shape, height, siting, and configuration indicated. Coordinate foundations, bearing devices, and such other items as may be necessary for a complete, functional bridge.

1.3 STRUCTURAL PERFORMANCE

Deisgn and construct a fabricated pedestrian bridge capable of withstanding the effects of gravity loads and the following loads and stresses within the limits and conditions indicated.

Structural design of the bridge shall be performed by or under the direct supervision of a professional engineer licensed within the project state, and in accordance with recognized engineering practices and principles.

Determine any additional loads (i.e. earth pressure, stream force on abutments, wind loads other than those applied perpendicular to the long axis of the bridge, etc.) and load combinations required for design of the foundations and abutments.

1.3.1 Design Loads

In considering design and fabrication issues, this structure shall be assumed to be statically loaded. No dynamic analysis shall be required nor shall fabrication issues typically considered for dynamically loaded structures be considered for this bridge.

1.3.1.1 Dead Loads

The bridge structure shall be designed considering its own dead load (superstructure and original decking) only. No additional dead loading shall be considered.

1.3.1.2 Pedestrian Live Load

Main supporting members, including girders, trusses and arches shall be designed for a pedestrian live load of ninety pounds (90lbs) per square foot of bridge walkway area. The pedestrian live load shall be applied to those areas of the walkway so as to produce maximum stress in the member being designed. Pedestrian live loads shall NOT be reduced.

Secondary members such as bridge decks and supporting floor systems, including secondary stringers, floor beams, and their connections to main supporting members shall be designed for a live load of ninety pounds (90lbs) per square foot, with no reduction allowed.

1.3.1.3 Wind Loads

Horizontal Forces: The bridge shall be designed for a wind load as specified by AASHTO LRFD Guide Specifications for the Design of Pedestrian Bridges, latest edition. The wind load shall be applied horizontally at right angles to the longitudinal axis of the structure. The wind load shall be considered both in the design of the lateral load bracing system and in the design of the truss vertical members, floor beams, and their connections.

Overturning Forces: The effect of forces tending to overturn structures shall be calculated assuming that the wind direction is at right angles to the longitudinal axis of the structure. In addition, an upward force shall be applied at the windward quarter point of the transverse superstructure width. This force shall be twenty pounds (20lbs) per square foot of deck.

1.3.1.4 Top Chord Railing Loads

The top chord, truss verticals, and floor beams shall be designed for lateral wind loads, and for any loads required to provide top chord stability. In no case shall the load be less than fifty pounds (50lbs) per lineal foot and a two hundred pound (200lb) point load, acting concurrently, applied in any direction at any point along the top chord, or at the top of the safety system (42" or 54" above the deck level) if higher than the top chord.

1.3.1.5 Safety Rails

Designed for loading of a two hundred pound (200 lbs) point load and fifty pounds per lineal foot (50plf) acting currently applied horizontally at right angles.

1.3.1.6 Railing Infill

Designed for infill loads of 50 pounds per square foot (50psf), applied horizontally at right angles.

1.3.2 Design Limitations

1.3.2.1 Vertical Deflection

The vertical deflection of the main trusses due to service pedestrian Live Load shall not exceed one three-sixtieth (1/360) of the span. The vertical deflection of cantilever spans of the structure due to service pedestrian Live Load shall not exceed one two-twentieth (1/220) of the cantilever arm length. The deflection of the floor beams due to service pedestrian Live Load shall not exceed one three-sixtieth (1/360) of its span. The deflection of the deck and stringers due to service pedestrian Live Load shall not exceed one three-sixtieth (1/360) of their respective spans. The service pedestrian Live Load shall NOT be reduced for deflection checks.

1.3.2.2 Horizontal Deflection

The horizontal deflection of the structure due to lateral wind loads shall not exceed one three-sixtieth (1/360) of the span.

1.3.2.3 Vibration

The fundamental frequency of the unloaded pedestrian bridge shall be no less than 3.0 Hz to avoid the first harmonic.

1.3.2.4 Minimum Thickness of Metal

The minimum thickness of all main structural steel members shall be one-quarter of an inch (1/4") nominal and be in accordance with the AISC 325 Manual of Steel Constructions "Standard Mill Practice Guidelines". For ASTM A500 and ASTM A847 tubing, the section properties used for design shall be per the Steel Tube Institute of North America, Hollow Structural Sections, "Dimensions and Section Properties".

1.4 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Qualifications; G

SD-02 Shop Drawings

Fabrication Drawings; G

SD-03 Product Data

Painting; G

SD-04 Samples

Polyurethane Topcoat; G

SD-05 Design Data

Structural Calculations; G

SD-07 Certificates

Welding Procedures And Qualifications; G

Welding Procedure Specifications (Wps)

1.5 QUALITY ASSURANCE

1.5.1 Qualifications

1.5.1.1 Fabricator's Qualifications

Pedestrian Bridge Fabricator must have a minimum of five years experience as a qualified manufacturer of pededstrian bridges similar in design and size to that indicated for this Project.

1.5.1.2 Engineer's Qualifications

Provide engineering services by an authorized currently licensed professional engineer, having a minimum of four years experience as an engineer knowledgeable in pedestrian bridge design analysis.

1.5.2 Fabrication Drawing Requirements

Submit fabrication drawings for approval prior to fabrication. Fabrication drawings must not be reproductions of contract drawings. Sign and seal fabrication drawings by a registered professional engineer. All relative design information such as member size, material specification, bridge reactions, dimensions, general notes, and required critical welds shall be clearly shown on the drawings. Include complete information for the fabrication and erection of the structure's components, including all relevant bridge dimensions, bridge cross sections, sufficient detailing, member cross sections, general notes indicating material specifications, weld details, detail of bolted splices, and camber details. Use standard welding symbols. Clearly highlight any deviations from the details shown on the contract drawings highlighted on the fabrication drawings. Explain the reasons for any deviations from the contract drawings.

1.5.3 Structural Calculations

Structural Calculations for the bridge superstructure shall be submitted by the bridge manufacturer. All calculations shall be signed and sealed by a Professional Engineer licensed within the project state. The calculations shall include all design information necessary to determine the structural adequacy of the bridge. A stamped electronic soft copy shall be provided. Hard copies may be provided at additional costs. At minimum the following criteria must be included for approval:

Applied loads and conditions for all load combinations
All resistance checks for axial, bending, and shear in each critical member type (i.e. top chord, bottom chord, vertical, floor beam, etc.)
Truss and Floor Deflection Checks
FEA Boundary Conditions
FEA Data Input
FEA Results and Supplementary Calculations for all Stress & Deflection Analyses
FEA Results for Frequency Analysis
U-Frame Stiffness Checks
Bolted Splice Connections (if applicable)
Bearing Plate Analysis
Critical weld connection check for each truss member type (i.e. vertical, diagonal)
Welded Tubular Connections (see section 4.3.4 of this document for design check requirements)
Bridge Reactions
Expansion and Contraction Requirements and/or Induced Loads

1.5.4 Certifications

1.5.4.1 Welding Procedures and Qualifications

Prior to welding, submit certification for each welder stating the type of welding and positions qualified for, the code and procedure qualified under, date qualified, and the firm and individual certifying the qualification tests. If the qualification date of the welder or welding operator is more than 6 months old, the welding operator's qualification certificate must be accompanied by a current certificate by the welder attesting to the fact that he has been engaged in welding since the date of certification, with no break in welding service greater than 6 months.

Conform to all requirements specified in AWS D1.1/D1.1M.

PART 2 PRODUCTS

2.1 MATERIALS

2.1.1 Unpainted Weathering Steel

Bridges which are not to be painted or hot-dip galvanized shall be fabricated from high strength, low alloy, and atmospheric corrosion resistant ASTM A847 cold-formed welded square and rectangular tubing and/or ASTM A588, ASTM A242, or ASTM A606 plate and structural steel shapes. Steel shall have a minimum yield strength of 50ksi. The minimum corrosion index of atmospheric corrosion resistant steel, as determined in accordance with ASTM G101, shall be 6.0.

2.1.2 Painted Steel

Bridges which are to be painted shall be fabricated from ASTM A36/A36M, ASTM A572, or ASTM A992/A992M and tubular sections from ASTM A500 GR B or C.

2.1.3 Galvanized Steel

Bridges which are to be galvanized shall be fabricated from ASTM A36/A36M, ASTM A572, or ASTM A992/A992M and tubular sections from ASTM A500 GR B or

C.

2.1.4 Bolts

Field splices shall be fully bolted with ASTM F3125 high strength bolts in accordance with the AASHTO Specifications for Structural Joints. Type 3 hardware shall be used for weathering steel bridge. Type 1 hardware shall be used for painted or galvanized finishes.

2.1.5 Concrete Deck

The bridge shall be furnished with a stay-in place galvanized steel form deck suitable for pouring a reinforced concrete slab. The form deck shall be designed to carry the dead load of the wet concrete, weight of form decking, plus a construction load of 20 psf or a 150 pound concentrated load on a 1'-0" wide section of deck.

The form deck shall be either smooth or composite. Composite decking shall not be used as reinforcing when designing for concentrated loads (wheel loads). The decking shall be galvanized in accordance with ASTM A525 (G60). Concrete deck design shall be performed by the Bridge manufacturer.

Concrete decks shall be designed for concentrated load as specified. The wheel loads used for deck design shall be distributed per AASHTO LRFD Bridge Design Specifications and using Steel Deck Institute C-2017 Standard for Composite Steel Floor Deck-Slabs.

2.2 GENERAL DESIGN FEATURES

2.2.1 Span

The bridge span shall be as shown on Drawings. The span shall be a straight line dimension measured from each end of the bridge structure

2.2.2 Width

The bridge width shall be as shown on Drawings. The width shall be the clear width to structural members or accoutrements to the structure as measured at deck level.

2.2.3 Truss Style

The bridge shall be designed as a half-through Pratt truss with one (1) diagonal per panel and square ended vertical members. All vertical members, unless specified otherwise, shall be plumb or perpendicular as determined during design.

Bridges may be designed utilizing an H-Section configuration where the floor beams are placed up inside the trusses or utilizing a U-Section configuration where the floor beam is welded to the bottom of the bottom chord.

The distance from the top of the deck to the top and bottom truss members shall be determined by the bridge fabricator based upon structural and/or shipping requirements. When the bridge is in the floodplain, the overall height of the truss and distance from the deck to the bottom chord shall be minimized as much as possible.

The top of the top chord shall not be less than forty-two inches (42")

above the deck measured from the high point of the walking surfaces.

2.2.4 Maximum Weight

The bridge shall be designed to such that the maximum shipped weight does not exceed 7,000 lbs to ensure the most cost-effective support structure and installation.

2.2.5 Member Components

All members of the vertical trusses (top and bottom chords, verticals, and diagonals) shall be fabricated from square and/or rectangular structural steel tubing. Other structural members and bracing shall be fabricated from structural steel shapes or square and rectangular structural steel tubing.

2.2.6 Safety Rails

Horizontal safety rails shall be placed on the structure up to a minimum height of forty-two inches (42") above the deck surfaces. Safety rails shall be placed so as to prevent a four-inch (4") sphere from passing through the truss. Safety rails shall be welded to the inside or outside of the structure. Safety rails shall have their ends sealed and ground smooth so as to produce no sharp edges if safety rails are placed on the inside of the structure.

2.2.7 Camber

The bridge shall have a vertical camber dimension at midspan equal to one hundred percent (100%) of the full dead load deflection.

2.2.8 Elevation Difference

The bridge abutments shall be constructed at the same elevation on both ends of the bridge or as required by the contract documents. Bridge shall have plumb verticals and flat base plates in all scenarios.

2.2.9 Stairs and Railings

Stairs shall match those specified in Section 05 51 00 METAL STAIRS.

Guardrail and Handrail materials, configurations, infills, and finishes shall match those specified in Section 05 52 00 METAL RAILINGS.

2.3 FABRICATION

Drain HoleS: When the collection of water inside a structural tube is a possibility, either during construction or during service, the tube shall be provided with a drain hole at its lowest point to let water out.

Bolt Holes:Unless otherwise specified, standard holes shall be used in high-strength bolted connections. Oversize holes may be used in any or all plies of slip-critical connections. They shall not be used in bearing-type connections. Cut, drill, mechanically thermal cut, or punch bolt holes perpendicular to metal surfaces. Do not enlarge bolt holes by burning.

Bearing Holes/Slots: Cut, drill, mechanically thermal cut, or punch bearing holes/slots perpendicular to steel surfaces.

2.3.1 Bearing Devices

Bridge bearings shall consist of a setting or slide plate placed on the abutment or grout pad. The bridge bearing plate which is welded to the bridge structure shall bear on this setting plate. One end of the bridge will be fixed by fully tightening the nuts on the anchor bolts at that end. The opposite end will have finger tight only nuts to allow movement under thermal expansion or contraction.

2.3.2 Foundations

Bridge manufacturer shall determine the number, diameter, minimum grade and finish of all anchor bolts. The anchor bolts shall be designed to resist all horizontal and uplift forces to be transferred by the superstructure to the supporting foundations. Engineering design of the bridge supporting foundations (abutment, pier, bracket and/or footings), including design of anchor bolt embedments, shall be the responsibility of the foundation engineer. The contractor shall provide all materials for (including anchor bolts) and construction of the bridge supporting foundations. The contractor shall install the anchor bolts in accordance with the manufacturer's bridge bearing dimensions.

Minimum 28-day strength for the abutment concrete shall be 4,500 PSI. The bearing seat shall be a minimum of 16" wide. The step height (from bottom of bearing to top-of-deck) shall be determined by the bridge manufacturer.

Information as to bridge support reactions and anchor bolt locations will be furnished by the bridge manufacturer after receipt of order and after the bridge design is complete.

2.4 FINISHING

2.4.1 Blast Cleaning

All Blast Cleaning shall use Best Management Practices and exercise environmentally friendly blast media recovery systems. To aid in providing a uniformly "weathered" appearance, all exposed surfaces of a weathering steel bridge shall be blast cleaned in accordance with Steel Structures Painting Council Surface Preparation Specifications No. 7 Brush-Off Blast Cleaning, SSPC-SP 7 latest edition. Exposed surfaces of steel shall be defined as those surfaces seen from the deck and from outside of the structures. Stringers, floor beams, lower brace diagonals and the inside face of the truss below deck and bottom face of the bottom chord shall not be blasted. All finishing shall be completed in manufacturer's shop prior to shipping.

2.4.2 Painting

All exterior surfaces of steel shall be painted utilizing a 2-coat system with an epoxy midcoat and a polyurethane topcoat. All exterior surfaces of steel shall be abrasively blast cleaned in accordance with SSPC-SP6 prior to application of the primer. Bridges shall be provided with paint for touch up after erection.

2.4.3 Galvanizing

Proper drainage and venting shall be provided for the galvanization process. All structural steel shall be zinc coat (hot-dip) galvanized per

the specifications listed in ASTM A123/A123M. Hardware shall be zinc coat (hot-dip) galvanized per the specifications listed in ASTM A153.

PART 3 EXECUTION

3.1 CONNECTIONS

Except as modified in this section, design connections indicated in accordance with AISC 360. Do not tighten anchor bolts set in concrete with impact torque wrenches. Holes must not be cut or enlarged by burning. Bolts, nuts, and washers must be clean of dirt and rust, and lubricated immediately prior to installation.

3.1.1 Welded Tubular Connections

All welded tubular connections shall be checked, when within applicable limits, for the limiting failure modes outlined in the AWS D1.1/D1.1M Structural Welding Code.

When outside the "validity range" defined in these design guidelines, the following limit states or failure modes shall be checked:

Chord Wall Plastification
Shear Yielding (Punching)
Local Yielding of Chord Sidewalls
Local Crippling of Chord Sidewalls
Local Yielding of Branch Due to Uneven Load Distribution

All tubular joints shall be plain unstiffened joints and fabricated without the use of reinforcing plates, except as follows:

Floor beams hung beneath the lower chord of the structure may be constructed with or without stiffener (or gusset) plates, as required by design.

Floor beams which frame directly into the truss verticals (H-Section bridges) may be designed with or without end stiffening plates as required by design.

Where chords, end floor beams and in high profiles the top end struts weld to the end verticals, the end verticals (or connections) may require stiffening to transfer the forces from these members into the end vertical.

3.2 WELDING

Welding must be in accordance with AWS D1.1/D1.1M. Provide AWS D1.1/D1.1M qualified welders, welding operators, and tackers.

Develop and submit the Welding Procedure Specifications (WPS) for all welding, including welding done using prequalified procedures. Submit for approval all WPS, whether prequalified or qualified by testing.

Filler metal shall comply with the applicable AWS Filler Metal Specification (i.e. AWS A5.28 for the GMAW Process). For exposed, bare, unpainted applications of corrosion resistant steels (i.e. ASTM A588 and ASTM A847), the filler metal shall comply with AWS D1.1/D1.1M, Section 3.7.3.

3.3 DELIVERY AND ERECTION

Bridges will be delivered by truck to a location nearest to the site accessible by roads. Hauling permits and freight charges are the responsibility of the manufacturer.

The manufacturer will advise the Contractor of the actual lifting weights, attachment points and all necessary information to install the bridge. Lifting procedure submittals shall be the responsibility of the bridge erector. Unloading, splicing, bolting, and proper lifting equipment is the responsibility of others

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 32 - EXTERIOR IMPROVEMENTS

SECTION 32 92 19

SEEDING

PART 1 GENERAL

1.1 REFERENCES
1.2 DEFINITIONS
1.2.1 Stand of Turf
1.3 SUBMITTALS
1.4 DELIVERY, STORAGE, AND HANDLING
1.4.1 Delivery
1.4.1.1 Seed Protection
1.4.1.2 Fertilizer, Gypsum, Sulfur, Iron, and Lime Delivery
1.4.2 Storage
1.4.2.1 Seed, Fertilizer, Gypsum, Sulfur, Iron, and Lime Storage
1.4.2.2 Topsoil
1.4.2.3 Handling
1.5 TIME RESTRICTIONS AND PLANTING CONDITIONS
1.5.1 Restrictions
1.6 TIME LIMITATIONS
1.6.1 Seed

PART 2 PRODUCTS

2.1 SEED
2.1.1 Classification
2.2 TOPSOIL
2.2.1 On-Site Topsoil
2.2.2 Off-Site Topsoil
2.2.3 Composition
2.3 SOIL CONDITIONERS
2.3.1 Lime
2.3.2 Aluminum Sulfate
2.3.3 Sulfur
2.3.4 Iron
2.3.5 Peat
2.3.6 Sand
2.3.7 Perlite
2.3.8 Composted Derivatives
2.3.8.1 Particle Size
2.3.8.2 Nitrogen Content
2.3.9 Gypsum
2.3.10 Calcined Clay
2.4 FERTILIZER
2.4.1 Granular Fertilizer
2.4.2 Hydroseeding Fertilizer
2.5 MULCH
2.5.1 Straw
2.5.2 Hay

2.5.3 Wood Cellulose Fiber Mulch
2.6 WATER
2.7 EROSION CONTROL MATERIALS
2.7.1 Erosion Control Blanket
2.7.2 Erosion Control Fabric
2.7.3 Erosion Control Net
2.7.4 Hydrophilic Colloids
2.7.5 Erosion Control Material Anchors

PART 3 EXECUTION

3.1 PREPARATION
3.1.1 EXTENT OF WORK
3.1.1.1 Topsoil
3.1.1.2 Soil Conditioner Application Rates
3.1.1.3 Fertilizer Application Rates
3.2 SEEDING
3.2.1 Seed Application Seasons and Conditions
3.2.2 Seed Application Method
3.3 RESTORATION

-- End of Section Table of Contents --

SECTION 32 92 19

SEEDING

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ASTM INTERNATIONAL (ASTM)

ASTM C602	(2020) Agricultural Liming Materials
ASTM D4427	(2018) Standard Classification of Peat Samples by Laboratory Testing
ASTM D4972	(2018) Standard Test Methods for pH of Soils

U.S. DEPARTMENT OF AGRICULTURE (USDA)

AMS Seed Act	(1940; R 1988; R 1998) Federal Seed Act
DOA SSIR 42	(1996) Soil Survey Investigation Report No. 42, Soil Survey Laboratory Methods Manual, Version 3.0

1.2 DEFINITIONS

1.2.1 Stand of Turf

95 percent ground cover of the established species.

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-03 Product Data

Wood Cellulose Fiber Mulch

Fertilizer

Include physical characteristics, and recommendations.

SD-06 Test Reports

Topsoil Composition Tests (reports and recommendations).

SD-07 Certificates

State Certification and Approval for Seed

SD-08 Manufacturer's Instructions

Erosion Control Materials

1.4 DELIVERY, STORAGE, AND HANDLING

1.4.1 Delivery

1.4.1.1 Seed Protection

Protect from drying out and from contamination during delivery, on-site storage, and handling.

1.4.1.2 Fertilizer, Gypsum, Sulfur, Iron, and Lime Delivery

Deliver to the site in original, unopened containers bearing manufacturer's chemical analysis, name, trade name, trademark, and indication of conformance to state and federal laws. Instead of containers, fertilizer, gypsum, sulphur, iron, and lime may be furnished in bulk with certificate indicating the above information.

1.4.2 Storage

1.4.2.1 Seed, Fertilizer, Gypsum, Sulfur, Iron, and Lime Storage

Store in cool, dry locations away from contaminants.

1.4.2.2 Topsoil

Prior to stockpiling topsoil, treat growing vegetation with application of appropriate specified non-selective herbicide. Clear and grub existing vegetation three to four weeks prior to stockpiling topsoil.

1.4.2.3 Handling

Do not drop or dump materials from vehicles.

1.5 TIME RESTRICTIONS AND PLANTING CONDITIONS

1.5.1 Restrictions

Do not plant when the ground is frozen, snow covered, muddy, or when air temperature exceeds 90 degrees Fahrenheit.

1.6 TIME LIMITATIONS

1.6.1 Seed

Apply seed within twenty four hours after seed bed preparation.

PART 2 PRODUCTS

2.1 SEED

2.1.1 Classification

Provide State-certified seed of the latest season's crop delivered in original sealed packages, bearing producer's guaranteed analysis for percentages of mixtures, purity, germination, weedseed content, and inert material. Label in conformance with AMS Seed Act and applicable state seed laws. Wet, moldy, or otherwise damaged seed will be rejected. Field mixes will be acceptable when field mix is performed on site in the presence of the Contracting Officer.

2.2 TOPSOIL

2.2.1 On-Site Topsoil

Surface soil stripped and stockpiled on site and modified as necessary to meet the requirements specified for topsoil in paragraph COMPOSITION. When available topsoil must be existing surface soil stripped and stockpiled on-site in accordance with Section 31 00 00 EARTHWORK and 31 23 00.00 20 EXCAVATION AND FILL.

2.2.2 Off-Site Topsoil

Conform to requirements specified in paragraph COMPOSITION. Additional topsoil must be furnished by the Contractor.

2.2.3 Composition

Containing from 5 to 10 percent organic matter as determined by the topsoil composition tests of the Organic Carbon, 6A, Chemical Analysis Method described in DOA SSIR 42. Maximum particle size, 3/4 inch, with maximum 3 percent retained on 1/4 inch screen. The pH must be tested in accordance with ASTM D4972. Topsoil must be free of sticks, stones, roots, and other debris and objectionable materials. Other components must conform to the following limits:

Silt	25-50 percent
Clay	10-30 percent
Sand	20-35 percent
pH	5.5 to 7.0
Soluble Salts	600 ppm maximum

2.3 SOIL CONDITIONERS

Add conditioners to topsoil as required to bring into compliance with "composition" standard for topsoil as specified herein.

2.3.1 Lime

Commercial grade hydrate or burnt limestone containing a calcium carbonate equivalent (C.C.E.) as specified in ASTM C602.

2.3.2 Aluminum Sulfate

Commercial grade.

2.3.3 Sulfur

100 percent elemental

2.3.4 Iron

100 percent elemental

2.3.5 Peat

Natural product of peat moss derived from a freshwater site and conforming to ASTM D4427. Shred and granulate peat to pass a 1/2 inch mesh screen and condition in storage pile for minimum 6 months after excavation.

2.3.6 Sand

Clean and free of materials harmful to plants.

2.3.7 Perlite

Horticultural grade.

2.3.8 Composted Derivatives

Ground bark, nitrolized sawdust, humus or other green wood waste material free of stones, sticks, and soil stabilized with nitrogen and having the following properties:

2.3.8.1 Particle Size

Minimum percent by weight passing:

No. 4 mesh screen	95
No. 8 mesh screen	80

2.3.8.2 Nitrogen Content

Minimum percent based on dry weight:

Fir Sawdust	0.7
Fir or Pine Bark	1.0

2.3.9 Gypsum

Coarsely ground gypsum comprised of calcium sulfate dihydrate 80 percent, calcium 18 percent, sulfur 14 percent; minimum 96 percent passing through 20 mesh screen, 100 percent passing thru 16 mesh screen.

2.3.10 Calcined Clay

Calcined clay must be granular particles produced from montmorillonite clay calcined to a minimum temperature of 1200 degrees F. Gradation: A minimum 90 percent must pass a No. 8 sieve; a minimum 99 percent must be retained on a No. 60 sieve; and material passing a No. 100 sieve must not

exceed 2 percent. Bulk density: A maximum 40 pounds per cubic foot.

2.4 FERTILIZER

2.4.1 Granular Fertilizer

Organic or synthetic, granular controlled release fertilizer.

2.4.2 Hydroseeding Fertilizer

Controlled release fertilizer, to use with hydroseeding and composed of pills coated with plastic resin to provide a continuous release of nutrients for at least 6 months.

2.5 MULCH

Mulch must be free from noxious weeds, mold, and other deleterious materials.

2.5.1 Straw

Stalks from oats, wheat, rye, barley, or rice. Furnish in air-dry condition and of proper consistency for placing with commercial mulch blowing equipment. Straw must contain no fertile seed.

2.5.2 Hay

Air-dry condition and of proper consistency for placing with commercial mulch blowing equipment. Hay must be sterile, containing no fertile seed.

2.5.3 Wood Cellulose Fiber Mulch

Use recovered materials of either paper-based (100 percent post-consumer content) or wood-based (100 percent total recovered content) hydraulic mulch. Processed to contain no growth or germination-inhibiting factors and dyed an appropriate color to facilitate visual metering of materials application. Composition on air-dry weight basis: 9 to 15 percent moisture, pH range from 5.5 to 8.2 . Use with hydraulic application of grass seed and fertilizer.

2.6 WATER

Source of water must be approved by Contracting Officer and of suitable quality for irrigation, containing no elements toxic to plant life.

2.7 EROSION CONTROL MATERIALS

Erosion control material must conform to the following:

2.7.1 Erosion Control Blanket

100 percent agricultural straw stitched with a degradable nettings, designed to degrade within 12 months.

2.7.2 Erosion Control Fabric

Fabric must be knitted construction of polypropylene yarn with uniform mesh openings 3/4 to 1 inch square with strips of biodegradable paper. Filler paper strips must have a minimum life of 6 months.

2.7.3 Erosion Control Net

Net must be heavy, twisted jute mesh, weighing approximately 1.22 pounds per linear yard and 4 feet wide with mesh openings of approximately one inch square.

2.7.4 Hydrophilic Colloids

Hydrophilic colloids must be physiologically harmless to plant and animal life without phytotoxic agents. Colloids must be naturally occurring, silicate powder based, and must form a water insoluble membrane after curing. Colloids must resist mold growth.

2.7.5 Erosion Control Material Anchors

Erosion control anchors must be as recommended by the manufacturer.

PART 3 EXECUTION

3.1 PREPARATION

3.1.1 EXTENT OF WORK

Provide soil preparation prior to planting (including soil conditioners as required), fertilizing, seeding, and surface topdressing of all newly graded finished earth surfaces, unless indicated otherwise, and at all areas inside or outside the limits of construction that are disturbed by the Contractor's operations.

3.1.1.1 Topsoil

Provide 4 inches of off-site topsoil or approved on-site topsoil to meet indicated finish grade. After areas have been brought to indicated finish grade, incorporate fertilizer, pH adjusters, and soil conditioners into soil a minimum depth of 4 inches by disking, harrowing, tilling or other method approved by the Contracting Officer. Remove debris and stones larger than 3/4 inch in any dimension remaining on the surface after finish grading. Correct irregularities in finish surfaces to eliminate depressions. Protect finished topsoil areas from damage by vehicular or pedestrian traffic.

3.1.1.2 Soil Conditioner Application Rates

Apply soil conditioners at rates as determined by laboratory soil analysis of the soils at the job site.

3.1.1.3 Fertilizer Application Rates

Apply fertilizer at rates as determined by laboratory soil analysis of the soils at the job site.

3.2 SEEDING

3.2.1 Seed Application Seasons and Conditions

Immediately before seeding, restore soil to proper grade. Do not seed when ground is muddy frozen snow covered or in an unsatisfactory condition for seeding. If special conditions exist that may warrant a variance in the

above seeding dates or conditions, submit a written request to the Contracting Officer stating the special conditions and proposed variance. Apply seed within twenty four hours after seedbed preparation. Sow seed by approved sowing equipment. Sow one-half the seed in one direction, and sow remainder at right angles to the first sowing.

3.2.2 Seed Application Method

Seeding method must be broadcasted and drop seeding, drill seeding, or hydroseeding.

3.3 RESTORATION

Restore to original condition existing turf areas which have been damaged during turf installation operations at the Contractor's expense. Keep clean at all times at least one paved pedestrian access route and one paved vehicular access route to each building. Clean other paving when work in adjacent areas is complete.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 33 - UTILITIES

SECTION 33 11 00

WATER UTILITY DISTRIBUTION PIPING

PART 1 GENERAL

1.1 DEFINITIONS
1.1.1 Water Transmission Mains
1.1.2 Water Mains
1.1.3 Water Service Lines
1.1.4 Additional Definitions
1.2 SUBMITTALS
1.3 City of Charlotte

-- End of Section Table of Contents --

SECTION 33 11 00

WATER UTILITY DISTRIBUTION PIPING

PART 1 GENERAL

1.1 DEFINITIONS

1.1.1 Water Transmission Mains

Water transmission mains include water piping having diameters greater than 14 inch, specific materials, methods of joining and any appurtenances deemed necessary for a satisfactory system.

1.1.2 Water Mains

Water mains include water piping having diameters 4 through 14 inch, specific materials, methods of joining and any appurtenances deemed necessary for a satisfactory system.

1.1.3 Water Service Lines

Water service lines include water piping from a water main to a building service at a point approximately 5 feet from building or the point indicated on the drawings, specific materials, methods of joining and any appurtenances deemed necessary for a satisfactory system.

1.1.4 Additional Definitions

For additional definitions refer to the definitions in the applicable referenced standard.

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval.

1.3 City of Charlotte

Work to be performed in accordance with City of Charlotte Standard Specifications.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 33 - UTILITIES

SECTION 33 30 00

SANITARY SEWERAGE

PART 1 GENERAL

1.1 SUBMITTALS
1.2 City of Charlotte

-- End of Section Table of Contents --

SECTION 33 30 00

SANITARY SEWERAGE

PART 1 GENERAL

1.1 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval.

1.2 City of Charlotte

Work to be performed in accordance with City of Charlotte Standard Specifications.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 33 - UTILITIES

SECTION 33 40 00

STORMWATER UTILITIES

PART 1 GENERAL

1.1 SUBMITTALS
1.2 NCDOT

-- End of Section Table of Contents --

SECTION 33 40 00

STORMWATER UTILITIES

PART 1 GENERAL

1.1 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval.

1.2 NCDOT

Work to be performed in accordance with NCDOT Standard Specifications for Roads and Structures

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 33 - UTILITIES

SECTION 33 46 13

FOUNDATION DRAINAGE

PART 1 GENERAL

1.1 REFERENCES
1.2 SYSTEM DESCRIPTION
1.2.1 Extent
1.2.2 Outlet Connections
1.2.3 Drainage Lines
1.2.4 Outlet Lines
1.3 SUBMITTALS
1.4 DELIVERY, STORAGE, AND HANDLING

PART 2 PRODUCTS

2.1 MATERIALS
2.1.1 Plastic Pipe
2.1.1.1 Corrugated Polyethylene (PE) Drainage Pipe
2.1.1.2 Polyvinyl Chloride (PVC) Pipe
2.1.1.3 Circular Perforations in Plastic Pipe
2.1.1.4 Slotted Perforations in Plastic Pipe
2.1.2 Fittings
2.1.3 Cleanouts and Piping Through Walls
2.1.4 Cover and Wrapping Materials for Open Joints in Drain Tile
2.1.5 Bedding and Pervious Backfill for Foundation Drains
2.1.6 Protective Covering for Pervious Backfill

PART 3 EXECUTION

3.1 INSTALLATION
3.1.1 Trenching and Excavation
3.1.2 Bedding
3.1.3 Pipe Laying
3.1.4 Jointing
3.1.4.1 Perforated and Porous Pipes
3.1.4.2 PVC Pipe
3.1.4.3 Corrugated Polyethylene
3.1.5 Outlet Lines
3.1.6 Cleanouts
3.2 Backfilling

-- End of Section Table of Contents --

SECTION 33 46 13

FOUNDATION DRAINAGE

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN ASSOCIATION OF STATE HIGHWAY AND TRANSPORTATION OFFICIALS (AASHTO)

AASHTO M 252	(2009; R 2017) Standard Specification for Corrugated Polyethylene Drainage Pipe
AASHTO M 294	(2021) Standard Specification for Corrugated Polyethylene Pipe, 300- to 1500-mm (12- to 60-in.) Diameter

ASTM INTERNATIONAL (ASTM)

ASTM D3034	(2016) Standard Specification for Type PSM Poly(Vinyl Chloride) (PVC) Sewer Pipe and Fittings
ASTM D3212	(2020) Standard Specification for Joints for Drain and Sewer Plastic Pipes Using Flexible Elastomeric Seals
ASTM F667/F667M	(2016; R 2021) Standard Specification for 3 through 24 in. Corrugated Polyethylene Pipe and Fittings
ASTM F758	(2014) Smooth-Wall Poly(Vinyl Chloride) (PVC) Plastic Underdrain Systems for Highway, Airport, and Similar Drainage
ASTM F949	(2020) Standard Specification for Poly(Vinyl Chloride) (PVC) Corrugated Sewer Pipe with a Smooth Interior and Fittings

1.2 SYSTEM DESCRIPTION

1.2.1 Extent

Furnish and install foundation drainage as a complete system to 5 feet beyond the building .

1.2.2 Outlet Connections

Connect foundation pipe to the storm drainage system as shown and specified in Section 33 40 00 STORMWATER UTILITIES.

1.2.3 Drainage Lines

Construct drainage lines of drain tile, perforated pipe, or porous pipe.

1.2.4 Outlet Lines

Construct outlet lines of closed-joint nonperforated, nonporous pipe.

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-04 Samples

Materials.

SD-07 Certificates

Materials.

1.4 DELIVERY, STORAGE, AND HANDLING

Protect materials placed in storage from the weather, humidity and temperature variations, dirt and dust, or other contaminants. Do not expose plastic pipe to direct sunlight for more than 6 months from time of manufacturer to installation.

PART 2 PRODUCTS

2.1 MATERIALS

Provide pipe for foundation drainage system of the type and size indicated. Use appropriate transitions, adapters, or joint details where pipes of different types or materials are connected. Submit two randomly selected samples of each type of pipe and fitting, prior to delivery of materials to the site, and certifications from the manufacturers attesting that materials meet specification requirements.

2.1.1 Plastic Pipe

Provide plastic pipe containing ultraviolet inhibitor to provide protection from exposure to direct sunlight.

2.1.1.1 Corrugated Polyethylene (PE) Drainage Pipe

Furnish AASHTO M 252 for pipe 3 to 10 inches in diameter or AASHTO M 294 for pipe 12 to 24 inches in diameter. Furnish pipe manufacturer's standard fittings and conforming to the indicated specification.

2.1.1.2 Polyvinyl Chloride (PVC) Pipe

ASTM F758, Type PS 46, ASTM D3034, or ASTM F949 with a minimum pipe stiffness of46 psi.

2.1.1.3 Circular Perforations in Plastic Pipe

Cleanly cut circular holes no more than 5/16 inch or less than 3/16 inch in diameter, and arrange in rows parallel to the longitudinal axis of the pipe. Place perforations approximately 3 inches apart, center-to-center, along rows. Place rows approximately 1-1/2 inches apart and arrange in a staggered pattern so that all perforations lie at the midpoint between perforations in adjacent rows. Space rows no more than 155 degrees of circumference. Do not perforate the spigot or tongue end of the pipe for a length equal to the depth of the socket and continue perforations at uniform spacing over the entire length of the pipe. Manufacturer's standard perforated pipe which essentially meets these requirements may be used with prior approval of the Contracting Officer.

2.1.1.4 Slotted Perforations in Plastic Pipe

Cleanly cut circumferential slots so as not to restrict the inflow of water and uniformly spaced along the length and circumference of the tubing. Width of slots exceeding 1/8 inch or less than 1/32 inch is not permitted. Length of individual slots exceeding 1-1/4 inches on 3 inch diameter tubing is not permitted; 10 percent of the tubing inside nominal circumference on 4 to 8 inch diameter tubing; and 2-1/2 inches on 10 inch diameter tubing. Symmetrically space rows of slots so that they are fully contained in quadrants of the pipe. Center slots in the valleys of the corrugations of profile wall pipe. Provide water inlet area consisting of a minimum of 0.5 square inch/linear foot of tubing. Manufacturer's standard perforated pipe which essentially meets these requirements may be used with prior approval of the Contracting Officer.

2.1.2 Fittings

Provide fittings consisting of compatible materials for pipe, of corresponding weight and quality, and as specified herein.

2.1.3 Cleanouts and Piping Through Walls

Provide cleanout pipe and fittings and piping through walls and footings consisting of cast-iron soil pipe. Each cleanout must have a brass ferrule and a cast-brass screw-jointed plug with socket or raised head for wrench.

2.1.4 Cover and Wrapping Materials for Open Joints in Drain Tile

Cover material may be tar paper, roofing paper, reinforced building paper, glass fiber fabric, or other similar type material. Wrapping material must be 18-14 mesh, 0.01 inch diameter nonferrous wire cloth.

2.1.5 Bedding and Pervious Backfill for Foundation Drains

Provide bedding and pervious backfill in accordance with Section 31 00 00 EARTHWORK or as indicated on Drawings.

2.1.6 Protective Covering for Pervious Backfill

Provide roll type, nonperforated, water permeable mat with thickness between 1/4 and 1/2 inch and density of 3/4 pcf filter fabric conforming to Section 33 46 16 SUBDRAINAGE SYSTEM.

PART 3 EXECUTION

3.1 INSTALLATION

3.1.1 Trenching and Excavation

Perform required trenching and excavation in accordance with Section 31 00 00 EARTHWORK. Keep trenches dry during installation of drainage system. Make changes in direction of drain lines with 1/8 bends. Use wye fittings at intersections.

3.1.2 Bedding

Place graded bedding, minimum 6 inches in depth, in the bottom of trench for its full width and length compacted as specified prior to laying of foundation drain pipe. Rest each section firmly upon the bedding, through the entire length, with recesses formed for bell joints. Except for recesses for bell joints, fully support the lower quadrant of the pipe.

3.1.3 Pipe Laying

Lay drain lines to true grades and alignment with a continuous fall in the direction of flow. Face bells of pipe sections upgrade. Clean interior of pipe thoroughly before being laid. When drain lines are left open for connection to discharge lines, temporarily close the open ends and mark the location with wooden stakes. Lay perforated pipe with perforations facing down. Remove and relay any length that has had its grade or joints disturbed at no additional cost to the Government. Install perforated corrugated polyethylene drainage tubing and plastic piping in accordance with manufacturer's specifications and as specified herein. Do not install tubing and piping with physical imperfections.

3.1.4 Jointing

3.1.4.1 Perforated and Porous Pipes

Lay perforated and porous types of drain pipes with closed joints.

3.1.4.2 PVC Pipe

Furnish PVC pipe joints in accordance with ASTM D3034, ASTM D3212, or ASTM F949.

3.1.4.3 Corrugated Polyethylene

Furnish corrugated polyethylene (PE) pipe joints in accordance with ASTM F667/F667M or ASTM F667/F667M.

3.1.5 Outlet Lines

The outlet end of drain lines connecting with an open gutter or outfall must be covered with a removable wire basket of 16-mesh copper or bronze wire cloth fastened with brass or wire straps.

3.1.6 Cleanouts

Provide cleanouts in locations indicated and at each building corner. Set cleanouts in unpaved areas in 12 by 12 by 4 inch concrete blocks.

3.2 Backfilling

After joints and connections have been inspected and approved, place the specified pervious backfill material a minimum width of 6 inches on each side of the pipe or tile for the full width of the trench and full width between pipe and adjacent walls and 12 inches above the top of the pipe. Place the backfill preventing displacement of or injury to the pipe or tile. Place a protective covering, as specified, over the pervious backfill for the full width of the trench before regular backfill is placed. Compact backfill as specified in Section 31 00 00 EARTHWORK.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 33 - UTILITIES

SECTION 33 46 16

SUBDRAINAGE PIPING

PART 1 GENERAL

1.1 REFERENCES
1.2 SUBMITTALS
1.3 DELIVERY, STORAGE, AND HANDLING
1.3.1 Delivery and Storage
1.3.2 Handling

PART 2 PRODUCTS

2.1 PIPE FOR SUBDRAINS
2.1.1 Plastic
2.1.1.1 Polyvinyl Chloride (PVC) and Fittings
2.1.1.2 Corrugated Polyethylene (PE) and Fittings
2.1.1.3 Pipe Perforations
2.1.1.3.1 Circular Perforations in Plastic Pipe
2.1.1.3.2 Slotted Perforations in Plastic Pipe
2.2 GEOTEXTILE
2.3 SUBDRAIN FILTER AND BEDDING MATERIAL
2.4 DRAINAGE STRUCTURES
2.4.1 Mortar
2.4.2 Manholes and Appurtenances
2.4.2.1 Precast Reinforced Concrete Manhole Risers and Tops
2.4.2.2 Precast Concrete Manhole Bases
2.4.2.3 Frames and Covers or Gratings
2.4.2.4 Steel Ladder

PART 3 EXECUTION

3.1 EXCAVATION AND BEDDING FOR SUBDRAIN SYSTEMS
3.2 MANHOLES AND FLUSHING AND OBSERVATION RISERS
3.2.1 Manholes
3.2.2 Flushing and Observation Risers
3.3 INSTALLATION OF GEOTEXTILE AND PIPE FOR SUBDRAINS
3.3.1 Installation of Geotextile
3.3.1.1 Trench Lining and Overlaps
3.3.2 Installation of Pipe for Subdrains
3.3.2.1 Pipelaying
3.4 INSTALLATION OF MATERIAL AND BACKFILLING FOR PERFORATED SUBDRAINS
3.5 INSTALLATION OF BEDDING AND BACKFILL FOR NON-PERFORATED SUBDRAIN OUTFALL PIPE
3.5.1 Plastic Pipe

-- End of Section Table of Contents --

SECTION 33 46 16

SUBDRAINAGE PIPING

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN ASSOCIATION OF STATE HIGHWAY AND TRANSPORTATION OFFICIALS (AASHTO)

AASHTO M 252	(2009; R 2017) Standard Specification for Corrugated Polyethylene Drainage Pipe
AASHTO M 288	(2021) Standard Specification for Geosynthetic Specification for Highway Applications

ASTM INTERNATIONAL (ASTM)

ASTM A27/A27M	(2020) Standard Specification for Steel Castings, Carbon, for General Application
ASTM A47/A47M	(1999; R 2018; E 2018) Standard Specification for Ferritic Malleable Iron Castings
ASTM A48/A48M	(2003; R 2021) Standard Specification for Gray Iron Castings
ASTM A123/A123M	(2017) Standard Specification for Zinc (Hot-Dip Galvanized) Coatings on Iron and Steel Products
ASTM C33/C33M	(2018) Standard Specification for Concrete Aggregates
ASTM C136/C136M	(2019) Standard Test Method for Sieve Analysis of Fine and Coarse Aggregates
ASTM C478	(2018) Standard Specification for Circular Precast Reinforced Concrete Manhole Sections
ASTM D2321	(2020) Standard Practice for Underground Installation of Thermoplastic Pipe for Sewers and Other Gravity-Flow Applications
ASTM D3034	(2016) Standard Specification for Type PSM Poly(Vinyl Chloride) (PVC) Sewer Pipe and Fittings

ASTM D4632/D4632M	(2015a) Grab Breaking Load and Elongation of Geotextiles
ASTM F758	(2014) Smooth-Wall Poly(Vinyl Chloride) (PVC) Plastic Underdrain Systems for Highway, Airport, and Similar Drainage
ASTM F949	(2020) Standard Specification for Poly(Vinyl Chloride) (PVC) Corrugated Sewer Pipe with a Smooth Interior and Fittings

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-04 Samples

Geotextile

Pipe and Pipe Fittings

SD-07 Certificates

Geotextile

Pipe and Pipe Fittings

1.3 DELIVERY, STORAGE, AND HANDLING

1.3.1 Delivery and Storage

Inspect materials delivered to site for damage; unload, and store with minimum handling. Do not store materials directly on the ground. Keep the inside of pipes and fittings free of dirt and debris. Keep, during shipment and storage, geotextile wrapped in burlap or similar heavy duty protective covering. Protect the geotextile from mud, soil, dust, and debris. Do not store geotextile materials in direct sunlight. Install plastic pipe within 6 months from the date of manufacture unless otherwise approved.

1.3.2 Handling

Handle materials in such a manner as to ensure delivery to the trench in sound undamaged condition. Carry pipe to the trench.

PART 2 PRODUCTS

2.1 PIPE FOR SUBDRAINS

Submit samples of pipe and pipe fittings, before starting the work. Provide type and sizes of subdrain pipe indicated. Submit certifications from the manufacturers attesting that materials meet specification requirements. Certificates are required for drain pipe and fittings.

2.1.1 Plastic

Provide plastic pipe containing ultraviolet inhibitor to provide protection from exposure to direct sunlight. Provide pipe with bell and spigot or solvent cement joints. Provide manufacturer's standard type fittings conforming to the indicated specification.

2.1.1.1 Polyvinyl Chloride (PVC) and Fittings

ASTM D3034, ASTM F949 or ASTM F758, Type PS 46.

2.1.1.2 Corrugated Polyethylene (PE) and Fittings

AASHTO M 252, Type S or SP as indicated.

2.1.1.3 Pipe Perforations

Provide pipe perforations with a minimum water inlet area of 0.5 square inch per linear foot and as specified below.

2.1.1.3.1 Circular Perforations in Plastic Pipe

Cleanly cut circular holes not more than 3/8 inch or less than 3/16 inch in diameter and arrange in rows parallel to the longitudinal axis of the pipe. Provide pipe with perforations spaced uniformly along rows. Unless otherwise recommended by the pipe manufacturer, provide pipe with rows approximately 1-1/2 inches apart and arranged in a staggered pattern so that all perforations lie at the midpoint between perforations in adjacent rows. Space the rows over not more than 155 degrees of circumference. Provide pipe that is not perforated for a length equal to the depth of the socket at the spigot or tongue end and provide perforations that continue at uniform spacing over the entire length of the pipe.

2.1.1.3.2 Slotted Perforations in Plastic Pipe

Cleanly cut circumferential slots so as not to restrict the inflow of water and uniformly spaced along the length and circumference of the pipe. Provide pipe with slots not exceeding 1/8 inch nor less than 1/32 inch in width. Provide pipe with individual slot lengths not exceeding 10 percent of the pipe inside nominal circumference on 6 to 8 inch diameter pipe, and 2-1/2 inches on 10 inch diameter pipe. Symmetrically space rows of slots so that they are fully contained in 2 quadrants of the pipe. Center slots in the valleys of the corrugations of profile wall pipe.

2.2 GEOTEXTILE

Provide geotextile conforming to AASHTO M 288 and meeting the subsurface drainage requirements. Provide geotextile that is a nonwoven pervious sheet of polymeric material consisting of long-chain synthetic polymers composed of at least 95 percent by weight polypropylene (PP) or polyester (PET). The use of woven slit film geotextiles (i.e. geotextiles made from yarns of a flat, tape-like character) will not be allowed. Add stabilizers and/or inhibitors to the base polymer, as needed, to make the filaments resistant to deterioration by ultraviolet light, oxidation, and heat exposure. The minimum grab strength will be 160 pounds in accordance with ASTM D4632/D4632M. Provide geotextile with filaments constructed so as to retain their relative position with respect to each other. Selvage, overlap, or otherwise finish the edges of the geotextile to prevent the outer material from pulling away from the fabric.

Submit samples of geotextile and certifications from the manufacturers attesting that geotextile meets specification requirements.

2.3 SUBDRAIN FILTER AND BEDDING MATERIAL

Provide subdrain filter and bedding material composed of washed sand, sand and gravel, crushed stone, crushed stone screenings, or slag composed of hard, tough, durable particles free from adherent coatings, as indicated on Drawings. Filter material may not contain corrosive agents, organic matter, or soft, friable, thin, or elongated particles. Provide filter material that is evenly graded between the limits specified in TABLE I. Gradation curves will exhibit no abrupt changes in slope denoting skip or gap grading. Provide filter materials that are clean and free from soil and foreign materials. Remove and replace filter blankets found to be dirty or otherwise contaminated with material meeting the specific requirements, at no additional cost to the Government.

TABLE I

	Type I Gradation E 11 ASTM C33/C33M	Type II Gradation 57 ASTM C33/C33M	Type III Gradation 67 ASTM C33/C33M
ASTM C136/C136M Sieve Size	Percent Passing	Percent Passing	Percent Passing
1-1/2 inch	--	100	--
1 inch	--	90 - 100	90-100
1/2 inch	--	25-60	--
3/8 inch	100	--	20-55
No. 4	95 - 100	5 - 40	0-10
No. 8	--	0 - 20	0-5
No. 16	45 - 80	--	--

2.4 DRAINAGE STRUCTURES

In accordance with NCDOT standard specifications.

2.4.1 Mortar

In accordance with NCDOT standard specifications.

Provide mortar for connections to drainage structures that is composed of one part by volume of portland cement and two parts of sand. Provide sufficient quantity of water in the mixture to produce a stiff workable mortar. Use water that is clean and free of injurious acids, alkalies, and organic impurities. Use the mortar within 30 minutes from the time the ingredients are mixed with water.

2.4.2 Manholes and Appurtenances

2.4.2.1 Precast Reinforced Concrete Manhole Risers and Tops

ASTM C478.

2.4.2.2 Precast Concrete Manhole Bases

ASTM C478. Provide bases that allow suitable connection with influent and effluent lines and to provide a suitable base structure for riser sections.

2.4.2.3 Frames and Covers or Gratings

Except as otherwise permitted, provide frames and gratings, or frames and covers of either cast iron with tensile strength test not less than ASTM A48/A48M Class 25 or steel conforming to ASTM A27/A27M, Class 65-35. Required weight, shape, and size are indicated on the drawings. Frames and covers not subjected to vehicular traffic or storage may be of malleable iron where indicated. Provide malleable-iron frames and covers conforming to ASTM A47/A47M and of the weight, shape, and size indicated.

2.4.2.4 Steel Ladder

Provide a steel ladder where the depth of a manhole exceeds 12 feet. The ladder will be not less than 16 inches in width, with 3/4 inch diameter rungs spaced 12 inches apart. Provide two stringers that are a minimum 3/8 inch thick and 2 inches wide. Adequately anchor ladder to the wall by means of steel inserts spaced not more than 6 feet apart vertically, and install so as to provide at least 6 inches of space between the wall and the rungs. Galvanize ladders and inserts after fabrication in conformance with ASTM A123/A123M.

PART 3 EXECUTION

3.1 EXCAVATION AND BEDDING FOR SUBDRAIN SYSTEMS

Excavate trenches, including the removal of rock and unstable material, in accordance with Section 31 00 00 EARTHWORK and 31 23 00.00 20 EXCAVATION AND FILL. Place bedding material in the trench as indicated or as required as replacement materials used in those areas where unstable materials were removed. Compact bedding material as specified for cohesionless material in Section 31 00 00 EARTHWORK.

3.2 MANHOLES AND FLUSHING AND OBSERVATION RISERS

3.2.1 Manholes

Install manholes complete with frames and covers or gratings at the locations and within the limits and sizes indicated. Construct manholes of one of the materials specified for manholes in paragraph DRAINAGE STRUCTURES. Completely fill precast concrete manhole joints so that they are smooth and free of surplus mortar or mastic on the inside of the structure. Use either precast or cast-in-place concrete manhole bases.

3.2.2 Flushing and Observation Risers

Install flushing and observation riser pipes with frames and covers at the locations indicated. Construct risers of non-perforated plastic pipe. Join riser pipes to the subdrain system as indicated.

3.3 INSTALLATION OF GEOTEXTILE AND PIPE FOR SUBDRAINS

3.3.1 Installation of Geotextile

3.3.1.1 Trench Lining and Overlaps

Grade trenches to be lined with geotextile to obtain smooth side and bottom surfaces so that the geotextile will not bridge cavities in the soil or be damaged by projecting rock. Lay the geotextile flat but not stretched on the soil, and secure it with anchor pins in accordance with manufacturer's instructions. Overlap at least 6 to 12 inches, and secure with anchor pins along the overlaps.

3.3.2 Installation of Pipe for Subdrains

3.3.2.1 Pipelaying

Install pipe in accordance with the manufacturer's recommendations. Thoroughly examine each section of pipe before being laid; do not use defective or damaged pipe. Do not lay pipe when the trench conditions or weather is unsuitable for such work. Remove water from trenches by sump pumping or other approved methods. Lay the pipe to the grades and alignment as indicated. Bed the pipe to the established gradeline. Center perforations on the bottom of the pipe. Lay bell-and-spigot type with the bell ends upstream. Approval of all in-place pipes by the Contracting Officer is required prior to backfilling.

3.4 INSTALLATION OF MATERIAL AND BACKFILLING FOR PERFORATED SUBDRAINS

After perforated pipe for subdrains has been laid, inspected, and approved, place material around and over the pipe to the depth indicated. Place the material in layers not to exceed 8 inches thick. Thoroughly compact each layer using mechanical tampers or rammers.

3.5 INSTALLATION OF BEDDING AND BACKFILL FOR NON-PERFORATED SUBDRAIN OUTFALL PIPE

3.5.1 Plastic Pipe

Place and compact pipe embedment for plastic pipe in accordance with ASTM D2321. Use Class IB or II embedment materials.

-- End of Section --