PERFORMANCE WORK STATEMENT (PWS)

Defense Logistics Agency (DLA)

Defense Contracting Services Office (DCSO)

Building Control Systems/Utility Control Systems (BCS/UCS) Maintenance Services

Elevators and Vertical Lifts

Potable Water and Wastewater Systems

Electrical and Lighting Systems

Building Automation System (BAS)/Heating, Ventilation, Air Conditioning, and Refrigeration (HVACR) Systems, and Utility Metering System (UMS)

Electrical Distribution Systems (Site)

Firm Fixed Price (FFP), Indefinite Delivery/Indefinite Quantity (IDIQ) Contract for Routine/Preventive, and Non-Routine/Ad-Hoc Maintenance

TABLE OF CONTENTS

SECTION C – DESCRIPTIONS AND SPECIFICATIONS

C.1 DLA HOST SITES/LOCATIONS
C1.1 DLA HEADQUARTERS COMPLEX, FORT BELVOIR (HQC)
C1.2 DEFENSE SUPPLY CENTER RICHMOND (DSCR)
C1.3 DEFENSE DISTRIBUTION CENTER SUSQUEHANNA, NEW CUMBERLAND, PA (DDSP)
C1.4 DEFENSE SUPPLY CENTER COLUMBUS, OH (DSCC)
C1.5 DLA DISTRIBUTION DEPOT, SAN JOAQUIN, CA (DDJC)

C.2 GENERAL/BACKGROUND REQUIREMENTS INFO
C2.1 DESCRIPTION OF SERVICES/INTRODUCTION
C2.2 BACKGROUND
C2.3 OBJECTIVES
C2.4 DEFINITIONS/ACRONYMS – SEE ATTACHMENT 1
C2.5 ROLES AND RESPONSIBILITIES

C.2A GENERAL INFORMATION
C2.10 CONTRACT INFORMATION
C2.10.1 INDEFINITE DELIVERY/INDEFINITE QUANTITY GUIDELINES
C2.10.2 CLIN STRUCTURE
C2.10.3 PRICING OF TASK ORDERS
C2.10.4 LABOR RATES
C2.10.5 WORK CLASSIFICATION & MINIMUM WAGES
C2.11 PLACE(S) OF PERFORMANCE
C2.12 PERIOD OF PERFORMANCE
C2.13 HOURS OF OPERATION
C2.14 WORK OUTSIDE REGULAR WORKING HOURS
C2.15 FEDERAL GOVERNMENT HOLIDAYS
C2.16 CONTINUITY OF SERVICES
C2.17 DELIVERY, INSPECTION/ACCEPTANCE THE GOVERNMENT AND INVOICING – SEE ATTACHMENT 7
C2.18 COMMON ACCESS CARD PROCEDURES - SEE ATTACHMENT 5

C.2B GOVERNMENT INFORMATION
C2.20 COR
C2.21 GOVERNMENT FURNISHED FACILITIES
C2.22 GOVERNMENT FURNISHED EQUIPMENT
C2.23 GOVERNMENT FURNISHED SERVICES/UTILITIES
C2.24 GOVERNMENT FURNISHED MATERIALS

C.2C CONTRACTOR INFORMATION

C2.32 TRANSITION IN/OUT PERIODS

C2.33 CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES
C2.34 CONTRACTOR FURNISHED MATERIAL
C2.35 CONTRACTOR FURNISHED EQUIPMENT
C2.36 FACILITY SECURITY CLEARANCE(S)
C2.37 SECURITY REQUIREMENTS
C2.37.1 PHYSICAL SECURITY
C2.37.2 KEY CONTROL
C2.37.3 LOCK COMBINATIONS
C2.38 REQUIRED CONTRACTOR TRAINING AND CERTIFICATIONS
C2.39 CONTRACTOR MANAGEMENT OF THE IDIQ CONTRACT
C2.40 CONTRACT PROGRAM MANAGEMENT SUPPORT
C2.40.1 PROGRAM MANAGEMENT PLAN
C2.40.2 POST AWARD CONFERENCE/PERIODIC PROGRESS MEETINGS
C2.41 INTERFACE WITH OTHER CONTRACTORS AND GOVERNMENT PERSONNEL
C2.42 KEY PERSONNEL
C2.43 IDENTIFICATION OF CONTRACTOR EMPLOYEES
C2.44 CONTRACTOR TRAVEL
C2.45 OTHER DIRECT COSTS
C2.46 MATERIAL OVERHEAD RATES

C.2D QUALITY CONTROL
C2.50 QUALITY CONTROL PLAN
C2.51 ISSUE RESOLUTION PROCESS/REPORT
C2.52 QUALITY DEFICIENCIES
C2.53 CPARS

C.2E OTHER INFORMATION
C2.60 DATA RIGHTS
C2.61 ORGANIZATIONAL CONFLICT OF INTEREST

C.3 REQUIREMENTS / SPECIFICATIONS
C3.1 DESCRIPTION OF FACILITIES
C3.2 GENERAL SCOPE AND LOCATION BREAKDOWN
C3.3 REPLACEMENT, MODERNIZATION, RENOVATION
C3.4 ROUTINE/PREVENTIVE MAINTENANCE PROGRAM
C3.5 AS-BUILT DRAWINGS
C3.6 HISTORICAL DATA
C3.7 EQUIPMENT/INVENTORY IDIQ LIST – SEE ATTACHMENT 2
C3.8 DIRECTIVES/APPLICABLE STANDARDS – SEE ATTACHMENT 3

SERVICE ORDERS/AD-HOC TASK ORDERS
C3.10 SERVICE ORDERS/CALLS
C3.11 SERVICE ORDER/CALL CATEGORIES
C3.12 TYPES OF WORK AND MONTHLY REPAIR LOG
C3.13 MINOR WORK OR EQUIPMENT REPLACEMENT (At or Below the discipline threshold – Material Cost Only/No Labor)

C3.14 NON-ROUTINE/AD HOC REPAIRS RESULTING IN TASK ORDERS (At or Above the discipline threshold – Material Cost and Non-Direct Labor Only)
C3.15 PRICING NON-ROUTINE/AD HOC REPAIRS

C.4 SECURITY / CYBERSECURITY
C4.1 PERSONNEL REQUIREMENTS – SEE ATTACHMENT 8
C4.2 PRIVILEGED ACCESS
C4.3 CYBERSECURITY STRENGTH REQUIREMENTS
C4.4 CYBERSECURITY ASSURANCE REQUIREMENTS
C4.5 TASKS AND DELIVERABLES
C4.6 SYSTEM AND NETWORK REQUIREMENTS
C4.7 INFORMATION AND OPERATIONAL TECHNOLOGY INFRASTRUCTURE
C4.8 INSTALLATION SECURITY
C4.9 INFORMATION SECURITY
C4.10 PRIVACY ACT INFORMATION
C4.11 SENSITIVE INFORMATION

C.5 DELIVERABLES
C5.1 MONTHLY STATUS REPORT
C5.2 CYBER DELIVERABLES

C.6 TASKS AND DELIVERABLES (BY SITE)
C6.1 DLA HEADQUARTERS COMPLEX, FORT BELVOIR, VA (HQC)
C6.2 DEFENSE SUPPLY CENTER, RICHMOND, VA (DSCR)
C6.3 DEFENSE DISTRIBUTION CENTER SUSQUEHANNA, NEW CUMBERLAND, PA (DDSP)
C6.4 DEFENSE SUPPLY CENTER COLUMBUS, OH (DSCC)
C6.5 DLA DISTRIBUTION DEPOT, SAN JOAQUIN, CA (DDJC)

LIST OF ATTACHMENTS:

ATTACHMENT 1: DEFINITIONS AND ACRONYMS
ATTACHMENT 2: EQUIPMENT/INVENTORY IDIQ LIST
ATTACHMENT 3: REFERENCES/CODES
ATTACHMENT 4: PERFORMANCE REQUIREMENTS SUMMARY (PRS)
ATTACHMENT 5: COMMON ACCESS CARD (CAC) LANGUAGE
ATTACHMENT 6: INSPECTION REPORT
ATTACHMENT 7: INVOICING AND PAYMENT SCHEDULE
ATTACHMENT 8: CONTRACTOR PERSONNEL SECURITY
ATTACHMENT 9: SITE MAP

SECTION C
DESCRIPTIONS AND SPECIFICATIONS

The Request For Proposal (RFP) is to solicit Offerors to provide preventive maintenance, corrective maintenance, emergency maintenance, and sustainment for associated equipment/ hardware and software to support DLA Headquarters at Ft. Belvoir, VA and four (4) DLA host sites (Defense Supply Center Richmond (DSCR), Richmond, VA; Defense Distribution Center Susquehanna (DDSP) New Cumberland, PA; Defense Supply Center Columbus (DSCC) Columbus, OH; and Defense Distribution Depot San Joaquin (DDJC), Tracy, CA. Furthermore, BCS/UCS may also be tasked with supporting other DLA tenant locations within the Continental United States (CONUS).

C.1 DLA HOST SITES / LOCATIONS

C1.1 DLA HEADQUARTERS COMPLEX, FORT BELVOIR (HQC)

DLA HQ Installation Management description: oversight for installation and facilities management support for all DLA organizations. Advises and assists the Installation Management Director and DLA Director with meeting and sustaining current and future logistics support capabilities for the U.S. military services and other valued customers. The Facilities and Equipment business areas include Military Construction (MilCon); Sustainment, Restoration, and Modernization (SRM); Energy Resource Management (ERM); Real Estate Management; Accountability of Property, Plant, and Equipment (PP&E); and Facility Related Control System (FRCS).

C1.2 DEFENSE SUPPLY CENTER RICHMOND (DSCR)

DLA Weapons Support Richmond: DLA Weapons Support is the aviation demand and supply manager for Defense Logistics Agency with more than 4,300 civilian and military personnel in 22 locations across the United States – and, as of 2023, at Kadena Air Base in Okinawa, Japan – supporting more than 2,341 major weapon systems. The U.S. military relies on us as the integrated aviation material manager for roughly 1.8 million national stock number items, providing direct support through weapons systems management, industrial retail supply and strategic acquisition support operations. DLA Aviation plays a pivotal role in the success of Army, Navy, Marine Corps, Air Force and Space Force by providing targeted solutions and full-spectrum logistics support as part of the Nation's Combat Logistics Support Agency.

C1.3 DEFENSE DISTRIBUTION CENTER SUSQUEHANNA, NEW CUMBERLAND, PA (DDSP)

The mission of DLA Distribution Susquehanna, Pennsylvania, is to provide world-class distribution services to enhance the readiness of the Department of Defense and other customers, through effective and efficient receipt, storage, control, packaging, and shipment of material. We strive to be a value-based team known for workforce excellence and providing superior distribution services on time, every time.

C1.4 DEFENSE SUPPLY CENTER COLUMBUS, OH (DSCC)
Defense Supply Center Columbus hails as the Weapons Support Supply Chain headquarters for the Defense Logistics Agency focusing on the land and maritime supply chain with over 2,700 employees in 30 locations around the world. Today, the Defense Supply Center Columbus hosts 33 tenant organizations on the 520-acre site.

C1.5 DLA DISTRIBUTION DEPOT, SAN JOAQUIN, CA (DDJC)
DLA Distribution San Joaquin, California, receives, stores and ships materiel in support of America's Armed Forces around the clock, around the world. The Distribution Center is in the military readiness business and is the Department of Defense's western strategic distribution platform, serving as a hub of logistics activities for America's Warfighter.

C.2 GENERAL / BACKGROUND INFO

C2.1 Description of Services / Introduction

C2.1.1 This is a regular and Routine/Preventive Maintenance (PM) contract to provide and implement a comprehensive program for the operation, maintenance, repairs, service, testing, inspection and certification of Building Control System (BCS) and Utility Control Systems (UCS) at the following locations:

- Defense Supply Center Columbus, OH (DSCC)
- Defense Supply Center Richmond, VA (DSCR)
- DLA Distribution Depot, San Joaquin, CA (DDJC)
- DLA Distribution Center Susquehanna, PA (DDSP), New Cumberland, Pennsylvania
- DLA Headquarters Complex, Fort Belvoir, VA (HQC)

C2.1.2 The BCS/UCS systems included in this requirement are:

- Elevator and Vertical Lift Systems
- Potable Water and Wastewater Systems
- Electrical and Lighting Systems
- Building Automation System (BAS)/Heating, Ventilation, Air Conditioning, and Refrigeration (HVACR) Systems, and Utility Metering System (UMS)
- Electrical Distribution Systems (Site)

C2.1.3 The Contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform BCS/UCS Systems Maintenance services as defined in this PWS except for those items specified as Government furnished property and services. The Contractor shall perform to the standards in this contract.

Note: There is a mixture of Government and Contractor personnel performing the above services at each site. Some sites/systems are almost exclusively worked by Government personnel, while other sites/systems have a heavier contractor presence. Richmond and New Cumberland/Susquehanna are staffed with Government personnel to do most of the work and will most likely only need the contractor to perform the cyber security work and potentially some minor

ad-hoc maintenance/repair work. DLA Headquarters at Fort Belvoir, Columbus and San Joaquin have less Government staff and will need extensive contractor maintenance and repair support as well as cyber security work.

C2.1.4 In support of these missions, DLA Installation Management (DM) maintains the DLA physical real property infrastructure as the Authority Having Jurisdiction at our host installations, which includes Richmond, VA; New Cumberland, PA; Columbus, OH; and San Joaquin, CA, as well as our DLA Headquarters facility at Ft. Belvoir, VA. DM is responsible for new construction (MILCON or Capital expenditures), and Equipment or System Maintenance of Heating, ventilation, Air conditioning and Refrigeration (HVACR), and Facilities Related Control Systems (FRCS). DM serves as the functional and doctrinal proponent for all real property system requirements, policies, and procedures including industry standards, The American Society of Heating, Refrigeration and Air Conditioning Engineers (ASHRAE), United Facilities Criteria (UFC) and National Fire Protection Association (NFPA), State and Local Codes, and Department of Defense (DoD) installation policy.

C2.1.5 This contract will encompass a wide array of BCS/UCS systems. These control systems ensure the proper function of the systems to meet minimum efficiency and code related criteria. A control system (CS) as it pertains to FRCS can have many levels. The Equipment level can include multiple pieces of factory supplied equipment directly connected to create a manufacturer system to optimize efficiency. The Building Level consists of a building level controller(s), dedicated communication trunks (LON, BACnet, MODBUS, N2, other proprietary communications protocols), field level devices, sensors, actuators, or other devices. The Site level (Installation Wide) is an overarching system that allows a single system to monitor and provide user access to monitor, trend, and operate systems. These systems are currently operated and managed on a site-by-site basis with unique hardware, firmware, and equipment. Sites currently operate multiple disparate FRCS requiring varying levels of support including some legacy systems, which are manufacturer obsolescence and/or unsupported hardware/ firmware systems.

C2.1.6 This PWS contains the broad requirements for supporting numerous sites and disparate systems throughout DLA. In support of these numerous sites and systems, DLA intends to award an IDIQ contract where DLA will issue separate task orders (TOs) to provide specific tailored site-level requirements. This intended Enterprise approach to FRCS allows for the appropriate level of DoD-required cybersecurity measures to be integrated throughout the planning, design, and renovation, and repair of new and existing facility systems based on the CS architecture of the equipment/systems. Each TO will have a detailed Performance Work Statement (PWS) outlining the requirements for the site. The TO PWS will align with the requirements and scope of the IDIQ contract PWS.

C2.2 Background

C2.2.1 The overall technical monitoring and administration of this Performance Work Statement (PWS) will be accomplished by the Defense Logistics Agency (DLA) Information Operations (J6). J6 is responsible for executing program management responsibility through their Enterprise Capabilities Portfolio, Technology Services Program Management Office (PMO), providing enterprise-wide policy, program, and worldwide operational support for DLA's overall need for Building and Utility Automation System as the enterprise solution. The Defense Logistics Agency (DLA) Installation Management (DM) and J6 Enterprise Capabilities (EC) Portfolio Technology Services PMO require Building Controls and Utilities Controls services to include operations and sustainment support for Routine/Preventive maintenance, testing, inspection and unplanned maintenance and repair, service tickets, cybersecurity

support and configuration management.

C2.2.2 The system connects several different types of control systems into a central user operated front end. This configuration shall provide the warfighter with improved operational control and monitoring functional capabilities for all DLA sites infrastructure.

C2.2.3 Over the years, management at each DLA site purchased BCS/UCS technology from different manufacturers to replace faulty components and upgrade equipment/outdated operating systems. Previously, the BCS/UCS programs required multiple contracts and specialized contractor support which led to more oversight by DLA Installation Management. Moreover, the differing equipment forced DLA Installation Management to pursue specialized training to gain proficiency using these additional platforms to perform daily operations. This enterprise solution, as part of the BCS and UCS pillars, is an effort to streamline the program management, sustainment, and lifecycle replacement of DLA's BCS/UCS components and software.

C2.2.4 DLA is seeking to identify the most suitable enterprise solution(s) for integrating building controls and utility controls and monitoring application areas to enable more effective management and improve energy-efficient facility operations. The architecture of buildings at each DLA site will vary. The nature of user needs at each site may require more than one enterprise solution. This initiative is set to implement improved cybersecurity measures in all BCS/UCS platforms within the enterprise.

C2.3 Objectives

C2.3.1 The contractor shall ensure the BCS/UCS Systems at all sites remain in exceptional operating condition to include compliance with current Government cybersecurity standards, optimize equipment performance, and enable the anticipation for repair/replacement of major components prior to equipment failure and to minimize down time due to equipment failure. In the event there are differences in the level of performance prescribed in the PWS or the references associated with this document, the services provided at a minimum shall comply with the most stringent requirement.

C2.3.2 The BCS/UCS Systems at these locations are often integrated with the military service host's BCS/UCS Systems but in some cases are stand-alone. The BCS/UCS at the DLA locations will be evaluated by DLA on a case-by-case basis to determine if that site can be executed/supported under this requirement.

C2.3.3 This acquisition is intended to support BCS/UCS system requirements for the DLA Headquarters at Ft. Belvoir, VA and four (4) DLA host sites (Defense Supply Center Richmond (DSCR), Richmond, VA; Defense Distribution Center Susquehanna (DDSP) New Cumberland, PA; Defense Supply Center Columbus (DSCC) Columbus, OH; and Defense Distribution Depot San Joaquin (DDJC), Tracy, CA. - These duties include, but are not limited to:

- Day-to-day maintenance and sustainment for both equipment and FRCS.
- Performing scheduled preventive, predictive maintenance, unscheduled minor work, and asset management functions to ensure the long-term efficient operation of facility BCS/UCS (BAS, elevator, electrical, HVACR, UMS, and water and wastewater) infrastructure.
- Performing scheduled and unscheduled maintenance, repairs, and replacements as needed on infrastructure components.

- Maintaining operations and maintenance & repair records for all infrastructure components in electronic format.
- Maintaining the inventory and electronic inventory records for the consumable supplies needed for system sustainment and maintenance.
- On-going evolution and development of automated systems and capabilities
- Preparation for anticipated new regulatory requirements
- Information technical networking support (ITNS) of the systems includes but not limited to cybersecurity, networking, server and client administration, database management, and Information System Security Engineering (ISSE), cybersecurity/system administration for the FRCS.

C2.3.4 The operations will be performed to comply with all federal, state, and local laws and regulations. The services shall be provided in a safe, secure, effective, and efficient manner and shall meet the highest standards prevalent in industry.

C2.4 Definitions / Acronyms

See ATTACHMENT 1 DEFINITIONS & ACRONYMS

C2.5 Roles and Responsibilities

C2.5.1 The roles of the Government Personnel are to ensure contract requirements are accepted per the contract terms and conditions. Contractor Personnel are responsible for management and quality control actions to meet the terms of the contract.

Contracting Officer (KO) - A person duly appointed with authority to enter, administer and terminate contracts on behalf of the Government. The KO is the only person who can legally commit the Government and only the KO, as the Government's agent, can modify the contract/order. The KO is the final authority for determining the adequacy of the Contractor's performance. KO decisions arising under or relating to the contract are final.

Contracting Officer's Representatives (CORs) – Individuals designated in writing by the KO to perform specific technical and administrative functions within the scope and limitations of their written appointment (e.g., surveillance of Contractor's performance, accept services). CORs inspect completed requirements and will use the overall inspection results to answer the KO's and Contractor's periodic requests and to complete performance surveys. CORs are not empowered to make any contractual commitments or authorize any changes to the order/contract or in any way obligate additional funds by the Government, such authority rests solely with the KO.

The COR will be designated for each TO and will be a DLA Government representative from J6 and/or DM.

C2.5.2 Program Management Support**.** The Contractor will provide Program Management support at the IDIQ and task orders level to include the following duties:

- Responsible for running complex programs and projects

- Supervises the project team and manages conflicts within different departments
- Plans and sets project goals and milestones and develops risk management strategies
- Defines resources and schedules for the implementation of the program
- Clearly defines requirements and sets targets accordingly
- Recognizes areas for internal improvement and develops plans for implementing the improvements
- Promotes achievement and performance improvement throughout the duration of the contract
- Develops, implements, communicates, and maintains a quality plan to bring the Company's Quality Systems and Policies into compliance with quality system requirements
- Direct the activities of contract personnel to measure key quality characteristics of processes from inception to completion
- Establishes the standards of service for customers or clients
- Provides monthly updates to the Government of status of IDIQ level and TO level work

C.2A GENERAL INFORMATION

C2.10 CONTRACT INFORMATION

C2.10.1 IDIQ Guidelines

C2.10.1.1 Per Far 52-.216-22. This is a Firm Fixed Priced contract with a Non-Routine/Ad Hoc CLIN for the period stated in the schedule. Multiple task orders may be issued under this contract on a Fixed Price basis. Work items for the fixed-price portion are identified in the schedule include all work except that identified as Non-Routine/Ad Hoc work. The fixed price quantities shown in the schedule are considered accurate estimates for this contract period.

C2.10.1.2 The contract consists of a five-year period of performance one (1) 12-month base year and four (4) 12 month option years, which will commence on award.

C2.10.1.3 Work items for the IDIQ contract are identified within the performance work statement of each Task Order.

C2.10.1.4 Task performance shall be made only as authorized by task orders issued in accordance with FAR 52.216-18. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the PWS up to the contract stated maximum. The Contractor shall be responsible for all Routine/Preventive maintenance and Repair work to maintain the system in good operational status, as well as alterations or equipment replacement below the discipline threshold (material and non-direct labor cost only). The cost of these Routine/Preventive maintenance, alterations, repairs, and replacement shall be part of CLINs 0001, 0002, 0003, 0004, 0005 and its corresponding option CLINs.

C2.10.1.5 Except for any limitation of quantities in FAR 52.216-19 or in the PWS, there is no limit on the number of task orders that may be issued.

C2.10.1.6 Any task order issued during the effective period of the IDIQ contract and not completed within that period shall be completed by the Contractor within the time specified in the task order. The contract shall govern the contractor's and government's rights and obligations with respect to that task order to the same extent as if the task order was completed during the contract's effective period.

C2.10.1.7 For Issuing Indefinite Delivery Indefinite Quantity Task Orders. Some of the services under this contract shall be furnished at such times as ordered by the issuance of task orders on SF 1449 by the Contracting Officer. All orders issued hereunder are subject to the terms and conditions of this contract. This contract shall take precedence in the event of conflict with any task order. Any task order issued under this IDIQ contract with a total value of $50,000.00 or less may be issued unilaterally by the Contracting Officer.

C2.10.2 Contract Line Item Number (CLIN) Structure

Refer to solicitation document for detailed CLIN Structure.

C2.10.3 Pricing of Task Order(s)

Individual Task Orders (TOs) will be issued as requirements arise and become known. Task Orders will specify work to be performed and will reflect the labor rates of the proposed staff in effect when the task order is issued (in accordance with the provisions contained in the IDIQ contract and the award TOs). The proposed labor rates will be included within the IDIQ contract. The Contractor shall perform all services in accordance with the task order performance work statement/specifications. The terms and conditions set forth in the IDIQ contract will always apply. All TOs will be fixed price.

C2.10.4 Labor Rates

The proposed labor rates shall be used by the contractor as the ceiling labor rates when submitting price proposals in response to requests for TOs issued under this contract. The proposed labor rates of the successful awardee will be included as a separate table with the IDIQ contract. The contractor may propose at or below these labor rates, as each TO award will be negotiated on an individual basis.

C2.10.5 Work Classification & Minimum Wages

C2.10.5.1 All work performed pursuant to this IDIQ contract, firm-fixed price CLINs is subject to the terms of any applicable Collective Bargaining Agreement and FAR Clause 52.222-41, Service Contract Labor Standards (Aug 2018). Work performed under subsequent Task Orders *may* be subject to FAR Clause 52.222-6, Construction Wage Rate Requirements (Aug 2018), depending on the nature of the work. Applicable Department of Labor Wage Determinations are attached to this solicitation. *The Government will determine applicability of FAR 52.222-6 at the Task Order level.*

C2.10.5.2 The McNamara–O'Hara Service Contract Act of 1965 (SCA), codified at 41 U.S.C. §§ 6701–6707, or the Davis-Bacon Act (DBA), Public Law 107–217 (as amended), *may* apply to work performed under this contract, depending on the specific nature of the services required in each Task Order. *The Government will make a determination as to which Act is applicable at the Task Order level.*

C2.11 Place(s) of Performance

Individual task orders will specify the place of performance. However, work under this IDIQ shall be performed predominately at Government facilities to include Defense Supply Center Columbus, OH (DSCC), Defense Supply Center Richmond, VA (DSCR), DLA Distribution Depot, San Joaquin, CA (DDJC), DLA Distribution Center Susquehanna, PA (DDSP), and DLA Headquarters Complex, Fort Belvoir, VA (HQC).

C2.12 Period of Performance

The period of performance shall be for one (1) base year of 12 months and four (4) 12-month option years. for a five-year ordering period.

C2.13 Hours of Operation

Regular Working Hours have historically been from 0600 – 1800 local time. The Government's regular core working hours are Monday through Friday from 0700 – 1530 local time. Contractors must have qualified on-site technician(s) and/or a Designee(s) must be available for emergency responses during the core hours. No regular work shall be done or billed on the weekends or federal holidays. (See C4.15 for federal holiday listings). Additional information about site specific working hours will be provided at the Task Order level.

C2.14 Work Outside Regular Working Hours

C2.14.1 Certain tasks may require the Contractor to work outside of the normal working hours, including weekends and holidays. Any work outside the normal working hours of the installation will require the approval of the COR and shall be included in the contract cost. Any work that is not included in the contract cost will need to be approved in writing by the Contract Officer.

C2.14.2 Additionally, after hours service orders/calls are automatically forwarded to the Police Department or other designee as identified by the COR. The Contractor shall provide to the KO or COR/designee a work reception desk that is manned twenty-four (24) hours a day, seven (7) days a week, including weekends and holidays or a Call Out Roster of personnel to contact for afterhours support. The Contractor shall respond with personnel with the correct skillset to come in and alleviate the emergency. The Contractor shall arrive on-site within the timeframe outlined in the specific T.O. by site from the Government. The Contractor shall notify the Police Department or other designee when they arrive and depart the installation. The Contractor shall keep a log of all Call Outs with the following information:

1. Time employee called
2. Time 1st employee arrived on site
3. Name of employee/s
4. Reason for Call Out
5. Description of work performed to correct the problem
6. Time employee departed the site

C2.15 Federal Government Holidays

The Contractor is not required to perform services on holidays unless an exception is specified in the individual task orders. Federal Government holidays are as follows:

New Years Day	1st day of January
Martin Luther King Jr.'s Birthday	3rd Monday of January
Washington's Birthday	3rd Monday of February
Memorial Day	Last Monday of May
Juneteenth	19th Day of June
Independence Day	4th day of July
Labor Day	1st Monday of September
Columbus Day	2nd Monday of October
Veterans Day	11th day of November
Thanksgiving Day	4th Thursday of November
Christmas Day	25th day of December

C2.16 Continuity of Services

C2.16.1 To ensure continuity of essential services, the Contractor shall be fully prepared to commence work on the start date of this contract and be prepared to accept approximately thirty (30) backlogged service orders/calls. Work must be completed on all assigned backlogged service orders/calls within twenty (20) business days after the contract start date. Correction of defective or deficient work on the backlogged service orders/calls is the responsibility of the Contractor.

C2.16.2 Strike Contingency Plan (SCP)

C2.16.3 The Contractor shall prepare a Strike Contingency Plan to be used in the event of a strike by Contractor employees. The SCP shall be submitted to the COR for approval fifteen (15) days after contract start. At a minimum, the SCP shall include the following information:

1. The names, addresses, telephone numbers, and contact persons of proposed firms the Contractor intends to utilize to provide the services defined in this PWS during strikes by Contractor employees.
2. Copies of current licenses and certifications of experience assuring the Government that all temporary or replacement employees (including Subcontractor employees) will meet the experience and licensing requirements of this contract.

C2.16.4 Contractor Emergency Plan (CEP)

The Government's Occupant Emergency Plan (OEP) and Damage Control Plan (DCP) are used by the Government during building emergencies. The Contractor shall prepare a Contractor Emergency Plan that will define the Contractor's procedures and actions it will take to provide support to the Government's OEP and DCP. The CEP will be provided at the Task Order level. The CEP shall be provided for approval to the COR in writing fifteen (15) calendar days after contract starts. Designated Contractor personnel,

including the On-site Supervisor, shall be thoroughly familiar with the Government's OEP and DCP, and shall be trained by the Contractor to fully understand their responsibilities relative to each emergency plan.

C2.16.5 The Contractor will not be penalized for delay of normal work if the work force has been diverted for emergency support. Additional Contractor costs incurred for emergency situation support are included in the Routine/Preventive work (firm-fixed price) portion of the contract.

C2.16.6 The Contractor shall be required to operate the facility during all emergency situations including, but not limited to; fires; accident and rescue operations; strikes; civil disturbances; natural disasters; utility service outages; and military contingency operations. The Contractor's Emergency Plan shall be submitted to the COR for approval within 15 days of contract start or award and shall include, at a minimum, the following:

1. The Contractor's procedures and actions used to provide support to the Government during emergencies.
2. The name, address, telephone number, and current position of each employee that will participate in the Contractor Emergency Plan.
3. The specific functions that each employee will perform during emergency situations.
4. If temporary or Subcontractor employees are to be used, the same information is required as in the Strike Contingency Plan.

C2.17 Delivery, Inspection/Acceptance

See SCHEDULE for more information.

C2.18 Common Access Card (CAC) Procedures (See Attachment 5 COMMON ACCESS CARD LANGUAGE)

Prior to gaining access to any DLA facility, contractor personnel must be vetted through the local security office. Due to DoD security requirements, foreign nationals and illegal aliens will not be permitted access to any DLA facility. Individuals with outstanding warrants or certain convictions also will be denied access. Contractor personnel must ensure they have the appropriate identification required to access DLA facilities. Contractor personnel entering a DLA facility should anticipate their vehicle will undergo a security check by DLA Security, and should ensure that no drugs, alcohol, or weapons of any kind are found within the vehicle. It is the contractor's responsibility to ensure the personnel performing under this contract can and will meet these requirements for accessing DLA facilities. Names of contractor personnel will be provided to the local POC for vetting purposes no less than one week prior to the class start date.

C.2B GOVERNMENT INFORMATION

C2.20 COR

See Section 2.5 Roles and Responsibilities.

C2.21 Government Furnished Facilities

All Government-furnished property will be provided in accordance with FAR 52.245-1, and FAR 52.245-9, and may include: office / workspace, office supplies, telephone service, computer access, and storage space. Government property shall be used ONLY in the performance of this contract and its task orders. The Contractor shall account for all property provided by the Government and shall be responsible for the security and condition of said property. Serialized items shall be annotated at the time of issue, with a signature of acknowledgement by the individual Contractor(s). All GFP is the property of the U.S. Government and shall not be transferred to any individual, or agency, public or private without the express written approval of the Contracting Officer.

C2.22 Government Furnished Equipment

GFE will be specified in the individual TOs on an as-needed basis with specified delivery dates and in specified condition. Office equipment and office supplies may be provided as GFE at the TO level at the discretion of the Government. Non-expendable equipment shall be returned to the Government upon the conclusion of the TO.

C2.23 GOVERNMENT FURNISHED SERVICES/UTILITIES

See TO PWS for specific information.

C2.24 GOVERNMENT FURNISHED MATERIALS

See TO PWS for specific information.

C.2C CONTRACTOR INFORMATION

C2.32 Transition In/Out Periods

C2.32.1 Phase-In Period

During the transition-in period, the Contractor shall provide a weekly written report to the KO or designee on the status of the tasks outlined in the Transition Plan. The KO or designee may accept the completion of tasks as identified in each weekly report. The Contractor shall complete all tasks required under the Transition-in Plan and provide the KO or designee with a detailed final report outlining all tasks accomplished five (5) working days prior to the conclusion of the transition period. If the KO or designee accepts the Contractor's transition performance, the KO or designee may perform a walkthrough with the Contractor to document completion of the transition plan. The walkthrough will be conducted at the COB on the final workday of the transition period.

C2.32.2 The Contractor shall provide documentation of completion of required training and certifications prior to the end of the transition period IAW the requirements identified in section C.

C2.32.3 The Contractor recognizes the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue the services. The Contractor agrees to:

C2.32.4 1. Furnish phase-in training (for the new contractor/Government employees), see Section C2.38.2 for additional details.

C2.32.5 2. Exercise its best efforts and cooperation to affect an orderly and efficient transition to a successor.

C2.32.6 The Contractor will be allowed to bring their employees on-site up prior to the start of the contract to become familiar with the buildings, equipment locations and to start the process for obtaining security badges and computer access. During and prior to completion of the transition-in period, the KO or designee will continually assess the Contractor's ability to perform the mission and discussions held during transition meetings. The Contractor shall complete the necessary steps for assumption of the facility and equipment during the transition-in period and shall meet all requirements as specified in the contract with the beginning of full performance.

C2.32.7 The Government will determine the carry-over for work-in-process (WIP). Throughout the transition period, the Government will monitor work-in-process and provide the new Contractor weekly WIP reports during the transition. Not later than (NLT) five (5) working days prior to the end of the transition period, the Government will review all work-in-process that is the responsibility of the incumbent Contractor and assess any impact to the new Contractor's performance on the scheduled start date.

C2.32.8 Additionally, if the outgoing Contractor fails to successfully complete all tasks required under transition, the Government reserves the right to extend transition until all tasks are completed or take other remedies available.

C2.32.9 Phase-Out Period

To allow for a smooth and orderly transfer of responsibility from the incumbent Contractor to the new Contractor, the Contractor shall, upon the Contracting Officer's written notice, (1) furnish phase-out services and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure the services called for by this contract are maintained at the required level of proficiency.

C2.32.10 The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor. All costs incurred will be included in the appropriate CLINS for the phase out period.

C2.33 Contractor Furnished Items and Responsibilities

See TO PWS for specific information.

C2.34 Contractor Furnished Material

The Contractor shall furnish all supplies, equipment, facilities, and services required to perform work under this contract that are not already provided by the Government.

C2.35 Contractor Furnished Equipment

See TO PWS for specific information.

C2.36 Facility Security Clearance(s)

This contract is categorized as unclassified however some TOs will require SECRET level clearance to classified areas including, but not limited to, TOs at DLA Headquarters, Ft. Belvoir, VA and San Joaquin, CA. The contractor is required to obtain and maintain the appropriate and favorable Facility Clearance for the level of TO that they will bid upon. The Offeror must possess a favorable Facility Clearance at time of IDIQ award (if contractor does not currently possess a clearance, DLA will sponsor if requested) and submit documentation to work in secure spaces processing classified materials. Most work to be performed under this requirement is unclassified, however, a security clearance will be required for some TOs up to Secret. Security clearance requirements will be further defined at the Task Order level and may require at DD254 Department of Defense Contract Security Classification Specification. Contractor must have available staff with a favorably adjudicated investigation for the level of clearance required in the TO prior to the TO award. This contract does not require the contractor to store, handle, process classified information at their facility. Contractors with a safeguarding requirement will need to be approved for safeguarding at the same or higher level of classification listed in Block 1b of the DD Form 254.

See Attachment 8 CONTRACTOR PERSONNEL SECURITY for specific requirements.

Contractors are required to comply with 32 CFR Part 117 National Industrial Security Program Operating Manual (NISPOM) in the handling, protection, and safeguarding of classified information in their possession. Security requirements outside the scope of the NISPOM if required, will be defined in the accompanying DD Form 254.

The personnel security investigations conducted for access to classified information will be started by the contractor company Facility Security Officer (FSO).

The DD 254 will be housed within the NISP Contract Classification System (NCCS) through the life of the contract. The Contractor shall be registered within NCCS at time of award to gain access to the DD 254. It is incumbent upon the Contractor to ensure that the necessary security paperwork is submitted in sufficient time to enable each individual to be cleared prior to beginning work on this contract. In the event that the NCCS is superseded by another System of Record, the same requirements apply.

C2.37 Security Requirements

C2.37.1 Physical Security

C2.37.1.1 Contractor Control Access

C2.37.1.2 The Contractor shall control access by locking or unlocking the areas or facilities used by the Contractor in the performance of the contract requirements. The Contractor shall lock all overhead doors, cages, vaults, warehouse doors, windows, and other areas for reasons of internal security before leaving an area unattended and prior to the conclusion of any working day.

C2.37.1.3 The Contractor shall operate under the site's approved security plan.

C2.37.1.4 In the event a Contractor area is found unsecured or there is an alarm response during non-duty hours, the Contractor's designated Point of Contact (POC) will be required to secure the area. The Contractor shall inform the KO or designee of the results of the alarm response. The Contractor shall report any facility security violations to the KO or designee within one (1) hour of discovery.

C2.37.1.5 Upon request of the KO or designee, the Contractor shall prepare and provide reports to update progress on all recommended corrective actions stemming from Government inspections or assessments conducted at the site (i.e., Security Program Review (SPR), OPSEC/INFOSEC inspections, Vulnerability Assessments (VA), DoD and DLA regulations or policies etc.)

C2.37.1.6 The Contractor's Security Specialist shall participate in working groups (i.e., Physical Security Anti-terrorism, Force Protection and OPSEC), if requested.

C2.37.2 Key Control

C2.37.2.1 The Contractor shall establish and maintain a Key and Lock Control Program as part of their Physical Security SOP, IAW DLAM 5200.08 DLA Physical Security Manual. The Contractor shall safeguard keys provided by the Government. The Contractor shall designate in writing to the KO or designee a key custodian to manage the key control program by the start of full performance.

C2.37.2.2 The Contractor shall develop and maintain a roster of employees with key or lock access requirements for key control boxes or equivalent system IAW DLAM 5200.08 DLA Physical Security Manual. The Contractor shall provide the KO or designee updated rosters as information changes. At all times the Contractor shall keep all keys within the Key and Lock Control Program under continuous accountability and shall limit the number of individuals authorized to draw keys to the minimum required by security and operational requirements.

C2.37.2.3 The Contractor shall not duplicate keys or allow their use by unauthorized Contractor personnel. The Contractor shall report any deviation from these rules or lost keys to the KO or designee within one (1) hour after discovery of occurrence and submit a detailed written report by close of business (COB) the same working day. If lost keys are discovered at the end of the day, and it is not possible to submit a written report to the KO or designee by COB the same working day, the Contractor shall submit the report within two (2) hours of the beginning of business on the next working day. The Contractor shall reimburse the Government for all costs associated with replacing locks or re-keying as a result of key duplication or loss.

C2.37.3 Lock Combinations

See TO PWS for specific information.

C2.38 Required Contractor Training and Certifications

C2.38.1 The Contractor shall describe how the workforce (management and labor) with the requisite knowledge, skills, abilities, and applicable licenses and certifications to perform the requirements will be trained and/or certifications/licenses obtain to perform PWS requirements and/or the validation of current training from review training records of personnel hired from the preceding contractor/contract. All training certifications must be provided to the COR within the timelines annotated in this PWS or at the Task Order level PWS.

C2.38.2 A phase-in period shall be established to allow the Contractor sufficient time to integrate personnel and transition into duties required to perform the requirements of the contract and ensure employees who will require access to the Installation and DoD Information Technology (IT) systems obtain a Common Access Card (CAC) IAW PWS. Instructions for all Phase in Training are available upon request.

- The phase-in period shall begin at the effective date of the TO and shall not exceed one (1) month, at which time full performance shall commence.
- The Contractor shall ensure that all Contractor personnel are ready to begin working on the first day of full performance including obtaining any account access, permissions, and/or roles required to administer the application software/hardware. Training and documentation such as rules of behavior and cyber awareness are required for access.

C2.38.3 During the phase-in period, Contractor personnel shall complete security and safety training on site. Training will be scheduled through the DLA site's training office and will at a minimum include the following classes. The estimated time to complete is three (3) hours.

- Active Shooter Briefing
- Safety Briefing
- Shelter in Place/Evacuation Awareness Briefing

C2.38.4 During the one-month phase-in period ensure all Contractor personnel know and understand regulations and policy pertaining to physical, information, operations, and personnel security. The Contractor shall provide security and antiterrorism training to all employees in accordance with applicable DoD regulatory requirements. Training, as required by the DLA Issuances and other applicable DoD guidance, will be completed annually for the following on-line training.

- Cyber Awareness Challenge
- Safety Briefing
- Shelter in Place/Evacuation Awareness Briefing
- Antiterrorism (AT) Level 1

- Operations Security (OPSEC)
- Counterintelligence Awareness Training
- Personally Identifiable Information Awareness
- Trafficking in Persons

C2.38.5 The security training is web-based, and access will be provided by the Government. The Contractor shall ensure Contractor personnel have taken the required security training to meet DoD guidance and that the personnel continue to maintain their certifications. The Government may add, delete, or change the annual training requirements.
The Contractor shall provide status and confirmation of completion of Phase-In tasks/training in TO Status Report and provide certificates as needed.

C2.39 Contractor Management of the IDIQ Contract

C2.39.1 The Contractor is fully responsible for efficient, economical, and satisfactory operation, installation, maintenance, inspection, programming, testing, and repair of systems and services covered under this contract.

C2.39.2 The Contractor shall provide all necessary management, administrative, and technical functions necessary for the effective and timely accomplishment of all contract requirement.

C2.39.3 The Contractor shall always employ enough qualified employees in accordance with the Performance Work Statement requirements in this contract.

C2.39.4 The Government will inspect and audit the Contractor's activities, and performance throughout the term of this contract to ensure compliance with all contractual requirements. All matters pertaining to the employment, supervision, or compensation, promotion, and discharge of contract employees shall be the responsibility of the Contractor, who is in all respects their employer.

C2.39.5 The KO may require the immediate dismissal of any Contractor employee and subcontractor employee who is identified as a potential threat to the health, safety, security, general well-being, or operational mission of the building and its population. The KO may also require the immediate removal of any Contractor or subcontractor employee from the HQC who is found objectionable. The removal from the HQC of such person(s) shall not relieve the Contractor of the requirement to provide sufficient personnel to perform all contract requirements. In the event an employee is dismissed or removed, a combination change request for locks accessible by the departing employee shall be submitted upon departure.

C2.39.6 The Contractor shall manage the total work effort associated with the maintenance, repair, minor work, Non-Routine/Ad Hoc IDIQ work, new construction, and all other services required herein to assure fully adequate and timely completion of these services. Included in this function will be a full range of management duties including, but not limited to, planning, scheduling, cost accounting, report preparation, update drawing, establishing and maintaining records, bar coding, update asset inventory for new equipment, and quality control. The Contractor shall provide an adequate staff of personnel with the

necessary management expertise to assure the performance of the work in accordance with sound and efficient management practices.

C2.40 Contract Program Management Support

C2.40.1 The Contractor shall provide complete program management support that fully integrates, manages, controls, and documents all phases of the PWS requirements. The program manager shall be the focal point for all issues in the BCS/UCS effort and shall keep the Government fully informed, both verbally and in writing. The Contractor shall provide all necessary personnel, administrative, financial, and managerial resources necessary for the support of individual TOs. Specific Program Management Support requirements will be provided at the TO level.

C2.40.2 The Contractor shall coordinate a Kick-Off Meeting prior to the execution of each TO. The Contractor will schedule the Kick-Off Meeting at a minimum within a week after contract award. The meeting shall include key personnel from both the prime Contractor and Subcontractor. The purpose of this Kick-Off Meeting is to:

- Aid both the Government and Contractor personnel in achieving a clear and mutual understanding of all requirements. The Contractor shall provide written meeting minutes to the COR within two (2) days after the meeting. Meeting minutes shall include a list of all action items, the party responsible for each item, and the agreed-upon due date. The status of all open action items will be the first topic of discussion at the subsequent meeting.
- Identify and resolve any potential problems. The Contractor shall be prepared to discuss any issues requiring clarification and gather information necessary for the Project Management Plan (PMP), as discussed below. The Kick-Off Meeting will include as a minimum: a program review, existing and planned Applications and Technical Initiatives, and personnel and physical security issues. The Contractor shall develop and submit a close-out report. The report is due 5 workdays prior to each individual TO completion. A close-out is completed when all administrative actions have been completed, issues are resolved, and final payment has been made.

C2.40.3 Project Management Plan

The Contractor shall develop, maintain, and update, throughout an individual TO's period of performance (POP), a process to provide the necessary information to the COR and/or government designee to manage the project.

C2.40.4 Post Award Conference/Periodic Progress Meetings

C2.40.4.1 The Contractor, including all key personnel, shall attend any post award conferences convened by the contracting activity IAW Federal Acquisition Regulation Subpart 42.5, Post Award Orientation, to discuss and develop mutual understandings/standards of contract performance requirements.

C2.40.4.2 The Contractor's Project Manager shall be required to schedule with the COR and subcontractors to discuss contract performance during Periodic Progress Meetings. The frequency of these meetings shall be determined by the COR. These meetings may cover but are not limited to discussions on progress to date, workload, scheduling, job status, project planning actions, and issues/ concerns. The Contractor shall provide Management representatives at the meeting above the level of Project manager at the COR's request to resolve performance issues and to discuss the Contractor's Issue Resolution Plan (Add to Deliverable table section). The Contractor shall provide written meeting minutes to the COR within two (2) days after the meeting. Meeting minutes shall include a list of all action items, the party responsible for each item, and the agreed-upon due date. The status of all open action items will be the first topic of discussion at the subsequent meeting. The Contractor is responsible for all meeting logistics, including scheduling, providing conference facilities or virtual meeting links, and distributing all relevant materials. The Contractor shall provide a draft agenda to the COR for review and approval no later than three (3) business days prior to any scheduled meeting.

C2.41 Interface with Other Contractors and Government Personnel

Other contractors and Government personnel may be engaged in similar and supporting work, which may require cooperation among the Contractor and such other parties.

C2.41.1 The Contractor shall cooperate with all other contractors and avoid conflicts with other contractors' performance and work schedules. Conflicts with other contractors that cannot be resolved between the parties shall be referred to the COR.

C2.41.2 The Contractor shall be required to assist other contractors in the performance of their work as it pertains to accessing the BCS/UCS systems for purposes such as Fire Alarm smoke detector cleaning, repair, and testing, Fire Suppression repair and any associated testing. All such requirements shall be coordinated with the Contractor giving as much notice as possible for each occurrence. Emergency requirements shall be treated as Emergency Service request calls.

C2.41.3 The Government employs "in-house" experts with Master-level electrical knowledge and skill. These employees serve as technical experts for DLA in all matters pertaining to electrical and fire detection, security alarm, and emergency power work in the DLA locations and are responsible for inspecting all such work to ensure compliance with specifications, safety and this contract. These employees may perform work including, but not limited to, repairs, installations, alterations, maintenance checks and services in accordance with this PWS.

C2.42 Key Personnel

C2.42.1 Groupings Specific Technical Key Personnel – BCS/UCS System/Site specific key personnel will be required at the TO level. Each TO PWS will detail the specific Key Personnel required for each DLA site.

C2.42.2 Supervision of Contractor Employees

This is a non-personal services contract. The Government will not exercise any supervision or control over Contractor or Subcontractor employees while performing work under the contract. Such employees

shall be accountable solely to the Contractor, not the Government. The Contractor, in turn, shall be accountable to the Government for Contractor or Subcontractor employees.

C2.43 Identification of Contractor Employees

C2.43.1 The Homeland Security Presidential Directive 12 (HSPD-12) dated 27 September 2012 has established criteria for Contractors who require a Common Access Card (CAC) for either physical access to an installation or access to government information technology (IT) systems. The Government requires Personnel Security Investigations (PSI) to establish that applicants or incumbents either employed by the Government or working for the Government under contract are suitable for the job and are eligible for a public trust or sensitive position. Upon favorable review and initiation of the PSI, Contractor personnel may be granted temporary access pending final adjudication of the PSI.

C2.43.2 A Contractor Investigative Request (CIR) form annotating the appropriate designation shall be submitted for each contract employee.

C2.44 CONTRACTOR TRAVEL

See TO PWS for specific information.

C2.45 OTHER DIRECT COSTS

See TO PWS for specific information.

C2.46 MATERIAL OVERHEAD RATES

Material Overhead Rate will be a percentage provided for this IDIQ solicitation.

C.2D QUALITY CONTROL

C2.50 Quality Control Plan

C2.50.1 The Contractor shall maintain a QCP to actively identify and correct performance failures for all work performed under this contract. The QCP must identify resources and include procedures and checklists to maximize quality and ensure completion of monthly PM services within the established performance period. The Contractor's organizational structure for its QC process shall be established in a manner that minimizes potential conflicts of interest between the contractor's personnel (or subcontractors) that perform the PM work and the personnel that will inspect the PM work. A more detailed QCP plan may be required at the task order level.

C2.50.2 The Contractor is responsible for maintaining the quality of all work performed under each Task Order (TO). A key deliverable for each TO is the development and maintenance of a robust Quality Control Plan (QCP). The Government will monitor the Contractor's quality control efforts using a Government-developed Quality Assurance Surveillance Plan (QASP), executed by the Contracting Officer's Representative (COR). The primary goal of the Contractor's QCP is to ensure adherence to the

highest standards and expectations DLA requires. The QCP should be dynamic and adaptable, subject to modification as the work progresses to adjust tasks, timelines, or other elements as warranted by changing circumstances. The QCP *must* include a detailed timeline with clearly defined "checkpoints" for monitoring progress and making go/no-go decisions. All changes to the QCP require mutual agreement between the COR and the Contractor, either at task initiation or at designated checkpoints. Furthermore, the Contractor shall develop and implement a comprehensive performance management system with processes to regularly assess and report performance against established metrics to the designated government representative. The Contractor's QCP shall detail the staffing, procedures, and methodologies for self-inspecting and ensuring the quality, timeliness, responsiveness, customer satisfaction, and overall conformance to all performance requirements outlined in this PWS.

C2.51 Issue Resolution Process/Report

The Contractor shall include in the QCP a plan to report problems or potential problems to the COR that affect performance under the TO within 24 hours. The report shall address, at a minimum, the nature and source of problem, Government action required, the impact on delivery schedules, and corrective action(s) needed.

C2.52 Quality Deficiencies

Service orders/calls issued to document Quality deficiencies for deficient or non-performed work shall be re-performed by the Contractor until accepted by the COR. Such Quality Deficiency service orders/calls shall not be considered as additional quantities of work.

C2.53 CPARS

The Government will use the CPARS web-enabled application or appropriate replacement system to collect and manage a library of automated Contractor performance evaluations. The Government will be responsible for the automated Contractor performance evaluations to be completed in accordance with FAR Part 42. FAR Part 42 identifies requirements for documenting Contractor performance for systems and non-systems acquisitions. In general, Contractor performance assessments or evaluations provide a record, both positive and negative, for a given contract during a specified period of time. When evaluating Contractor performance, each assessment or evaluation is based on objective facts and is supported by program and contract management data, such as cost performance reports, customer comments, quality reviews, technical interchange meetings, financial solvency assessments, production management reviews, Contractor operations reviews, functional performance evaluations, and earned contract incentives (where applicable).

C.2E OTHER INFORMATION

C2.60 DATA RIGHTS

See 252.227-7017 Identification and Assertion of Use, Release, or Disclosure Restrictions.

C2.61 ORGANIZATIONAL CONFLICT OF INTEREST

See 52.203-16 Preventing Personal Conflicts of Interest.

C.3 REQUIREMENTS/ SPECIFICATIONS

C3.1 Description of Facilities

Work under this IDIQ shall be performed predominately at Government facilities to include Defense Supply Center Columbus, OH (DSCC), Defense Supply Center Richmond, VA (DSCR), DLA Distribution Depot, San Joaquin, CA (DDJC), DLA Distribution Center Susquehanna, PA (DDSP), and DLA Headquarters Complex, Fort Belvoir, VA (HQC) . Additional facility descriptions will be provided at the Task Order level.

C3.2 General Scope and Location Breakdown

C3.2.1 The contractor is required to provide all the necessary management, services, personnel, and documentation required to accomplish the tasks described within this PWS. This acquisition is intended to support all operations, maintenance and management duties required to ensure efficient and effective operation of BCS/UCS systems at the five DLA locations identified in this PWS. These duties include, but are not limited to:

- Day to day operations and monitoring.
- Performing scheduled preventive, predictive maintenance, unscheduled minor work and asset management functions to ensure the long-term efficient operation of facility BCS/UCS infrastructure.
- Performing scheduled and unscheduled maintenance, repairs, and replacements as needed on infrastructure components.
- Maintaining operations and maintenance & repair records for all infrastructure components in electronic format.
- Maintaining the inventory and electronic inventory records for the consumable supplies needed for system operations and maintenance.
- On-going evolution and development of automated systems and capabilities
- Preparation for anticipated new regulatory requirements
- The operations will be performed to comply with all federal, state, and local laws and regulations. The services shall be provided in a safe, secure, effective, and efficient manner and shall meet the highest standards prevalent in industry.
- Provide a Site Manager who shall attend Government meeting when requested. The Contractor shall permit the Government the right to review and approve the Project Manager whenever a change of persons in this position takes place, which approval shall not be unreasonably withheld.
- Provide staff for operation of the facilities, as required by permit(s), seven (7) days per week, including response to emergency calls 24 hours per day, 7 days per week, within one hour of its

occurrence. The Contractor shall designate, as a minimum, one staff member as standby to respond to such calls.

- Staff the project with enough qualified employees who possess the managerial, administrative, and technical skills to perform the services specified in this Agreement, and where appropriate, the certification requirements mandated by the state where the site is located.
- Certain experienced professional and/or technical personnel are essential for successful accomplishment of the work to be performed under this contract. These "Key Personnel" will be US Citizens and shall be identified by name within the Contractor's proposal and their qualifications shall be submitted for evaluation during the source selection process. The Contractor agrees that such personnel shall not be removed or replaced within the performance of this contract unless the following measures are taken and fully documented in writing.

C3.2.2 Contractor is required to be directly responsible for the BCS/UCS systems. As such the Contractor is required to maintain on site staffing to meet the requirements below within 30 days of notice to proceed. This staff shall be employed on-site, on a full-time basis and shall not be time shared with another project without Contracting Officer written approval.

C3.2.3 The operations will be performed to comply with all federal, state, and local laws and regulations. The Contractor shall also be responsible for operating, maintaining, and managing the BCS/UCS systems pursuant to the requirements in this scope of work. The services shall be provided in a safe, secure, effective, and efficient manner and shall meet the highest standards prevalent in industry.

C3.2.4 Staff the Project with a sufficient number of qualified employees who possess the managerial, administrative, and technical skills to perform the services specified in this PWS, and where appropriate, the certification requirements mandated by the state where the site is located.

C3.2.5 The Contractor is required to maintain required certifications. If the Contractor is unable to meet these requirements, the government will consider such a breach of this contract and cause for termination

C3.2.6 Contract Format. This contract is a Firm-Fixed Price (FFP) Indefinite Delivery Indefinite Quantity (IDIQ) contracts 0001, 0002, 0003, 0004, 0005 and corresponding option CLINs will cover a comprehensive program for the Routine/Preventive maintenance, service, testing, inspection and certification of BCS/UCS systems. In addition, the Contractor will be responsible for all alterations or repairs or equipment replacement below the discipline threshold (material and non-direct labor cost only) or under.

C3.2.6.1 The Non-Routine/Ad-Hoc/unknown portion (CLIN 0006 and corresponding option CLINs) will address Non-Routine/Ad Hoc alterations, repairs or equipment replacement of above the discipline threshold and above (material and non-direct labor cost only) as agreed to by the Government.

C3.2.6.2 This contract encompasses all activities associated with the operation, maintenance, testing, repairs, cleaning, inspection and certification of BCS/UCS Systems at all the applicable sites, and their

associated components. This shall also include the maintenance of all associated sub-systems required for the operation of all applicable BCS/UCS systems.

C3.3 Replacement, Modernization, Renovation

C3.3.1 During the terms of this contract, the Government may operate, repair, replace, renovate or improve equipment, systems, facilities, or components at the Governments expense by means not associated with this contract. All replaced improved, updated, modernized, or renovated equipment, facilities, components or systems shall be maintained by the Contractor at no additional cost to the Government unless such changes result in an increase or decrease in contract requirements. Changes, replacements, or deletions which result in an increase or decrease in contract requirements will result in adjustments to the contract price in accordance with the "CHANGES" clause.

C3.3.2 Equipment Under Manufacturer's or Installer's Warranty. Equipment, components, and parts, other than that installed under this contract, shall not be removed, or replaced or deficiencies corrected while still under warranty of the manufacturer or the installer without prior approval of the Contracting Officer. All defects in material or workmanship, defective parts, or improper installation and adjustments found by the Contractor shall be reported to the Contracting Officer so that necessary action may be taken. The Contractor shall be knowledgeable of the equipment, parts, and components that are covered by warranty and the duration of such warranties. Available warranty information will be furnished to the Contractor by the Contracting Officer.

C3.4 Routine/Preventive Maintenance Program

C3.4.1 The Contractor shall perform PM and repair services in such a manner that all equipment within the scope of this contract operates in accordance with manufacture's recommended specifications and the publications outlined in (Attachment 3 REFERENCES/CODES).

C3.4.2 The Contractor shall manage, schedule, coordinate and perform the emergency repairs and service orders/calls as necessary to ensure an acceptable level of service and continuous safe and effective operation of the equipment.

C3.4.3 The Contractor shall provide a Routine/Preventive Maintenance Plan that outlines the Contractor's approach to testing, maintenance, repair, schedule and include a list of equipment and systems that are to receive these procedures outlined. The plan shall also include a description of the Routine/Preventive maintenance procedure and frequency. The Routine/Preventive Maintenance Plan shall be provided within 5 business days of contract award and re-submitted if significant changes occur.

C3.4.4 Routine/Preventive Maintenance Guide(s) - The Contractor shall perform maintenance, inspections testing, and repairs as required by the Government's Routine/Preventive Maintenance (PM) Computer Maintenance Management System (CMMS) on all applicable BCS/UCS equipment to industry standards as required. The Government will provide training on the CMMS software to necessary Contractor employees. The CMMS training will be at the facilities within thirty (30) days after the start of the contract. All annual and monthly schedules and completed PMs shall be entered into the CMMS as completed within two (2) business days after completion. The Contractor shall implement

all necessary work control procedures to ensure timely accomplishment of all maintenance and repair work requirements, as well as to permit tracking of all work in progress. The Contractor shall plan and schedule all work to ensure material, labor, tools and equipment are available to complete maintenance or repair work within the specified time limits and in accordance with the quality standards. The status of any work shall be provided within one (1) hour of the inquiry during regular working hours. The contractor's Project Manager shall schedule a monthly walkthrough with the COR to ensure that all aspects of contract, maintenance, repair, safety codes and procedures or any other contractual concerns are being addressed.

C3.5 As-Built Drawings

C3.5.1 The Government will provide access to as-built drawings, manufacturers' requirements and other maintenance related documents and manuals as needed, after contract award. However, the Contractor is responsible for field verifications as well as accuracy of all government provided materials as requested by the Government.

C3.5.2 In the event that while performing the work contained in this PWS the contractor constructs or installs any new structure or equipment, as-built drawings shall be provided to the Government prior to acceptance by the COR. More information on requirements for As-Built drawings will be provided in the TO PWS.

C3.6 Historical Data

Over the years, management at each DLA site purchased BCS/UCS technology from different manufacturers to replace faulty components and upgrade equipment/outdated operating systems. Previously, the BCS/UCS programs required multiple contracts and specialized contractor support which led to more oversight by DLA Installation Management. Moreover, the differing equipment forced DLA Installation Management to pursue specialized training to gain proficiency using these additional platforms to perform daily operations. This enterprise solution, as part of the BCS/UCS pillars, is an effort to streamline the program management, sustainment, and lifecycle replacement of DLA's BCS/UCS components and software.

C3.7 Equipment/Inventory Lists

Site specific inventory lists will be provided at the TO level.

C3.8 Directives/Applicable Standards

See **CODES for** more information.

SERVICES ORDERS/AD-HOC TASK ORDERS

C3.10 Service Orders/Calls

C3.10.1 A service order/call is defined as maintenance work which involves the repair or replacement of components which have failed or broken down and were discovered and then approved/requested by the Government. All service orders/calls (emergency, urgent or Routine/Preventive) with an estimated value below the discipline threshold (material and non-direct labor cost only) each shall be included in the firm fixed price of the contract. Upon identification/notification of a repair or replacement needing to be done, the Contractor will prepare and submit a service order/call documenting the issue and what is needed to rectify/fix the issue. The COR will review and either approve or disapprove with rationale. Once approved by the COR the Contractor will complete the service order/call. The process for service orders/calls will be clearly defined in any task orders to represent that task order's equipment and/or site-specific requirements.

C3.10.2 All alterations or repairs or equipment replacement with an estimated material/non-direct labor value greater than the discipline threshold (material and non-direct labor cost only) will be considered a Non-Routine/Ad Hoc repair and requires a separate Ad-Hoc Task Order. The Government is responsible for funding all Ad-Hoc Task orders above the discipline threshold)

Chart C3.10.2 Normal Service Order/Call Timeline

Steps	Alteration, Repair or Equipment Replacement	Time Period
1	Issue/need identified, and COR/Gov't notified	Day 1
2	Resolution/Fix determined and priced out	Bus Days 1 - 5
3	Service Order (Itemizing all costs w/Material quotes) submitted to COR	Bus Day 6
4	COR reviews and approves or sends back to Contractor for adjustments/additional info.	Bus Days 6 - 8
5	Once approved, Contractor completes work identified on the service order/call	Bus Days 8-15

C3.11 Service Order/Call Categories

A service order/call is classified into three categories as determined by the Government:

C3.11.1 Emergency Service Orders (ESO) – will be classified by the COR as emergency when the work consists of correcting failures which constitute an immediate danger to personnel or threaten to damage property or compromise physical security. All ESOs are included in the firm fixed price portion of the contract. The contractor shall respond to emergency repair calls and/or trapped calls via a Government provided radio within the timeframe specified at each TO level as it will vary by site, but after notification during normal business hours and within the timeframe specified at each TO level for after notification at times other than normal business hours. All emergency repair service order/calls and maintenance work shall be included in the monthly contract cost and shall be accomplished in accordance with normal commercial practices using parts specified by the elevator manufacturer or items of equal or better quality. Downtime of the systems will be kept to an absolute minimum and operational service percentage requirements will be provided at the Task Order level. The contractor shall notify the COR of all projected downtime of the system, or its components, and the estimated time for repair. The contractor shall prepare and submit a written report within two (2) business days after the emergency repair to the COR. The report shall include the date and time of the service order/call, the location of the service order, the repairs performed, and the name of the technician performing the repairs.

C3.11.2 Urgent Service Orders (USO) – will be classified by the COR as urgent when the work is deemed mission essential or when the work consists of failures in services which do not immediately endanger personnel, threaten to damage property, or disrupt operations and/or training missions, but would soon inconvenience and affect the health or wellbeing of personnel, damage property, or disrupt operations and/or training missions. All USOs are included in the firm fixed price portion of the contract. During regular working hours, the Contractor shall respond to Urgent service orders/calls within thirty (30) minutes. Response time for Urgent service order/calls at other than regular working hours shall be no more than two (2) hours. At a minimum, the Contractor shall work continuously and without interruption and shall arrest the urgent condition before departing the job site. If further labor and material (follow-up work) are required to complete the repair, a second service order/call will be initiated, classified as Routine/Preventive, and the corresponding completion time will be applied.

C3.11.3 Routine/Preventive Service Orders - A Routine/Preventive service order/call is a call other than an ESO or USO call and is defined as a situation where a piece of equipment breaks or fails to perform as designed, but its services can be performed by another piece of equipment. Upon receiving a Routine/Preventive service order/call, the Contractor shall respond to the location as directed within one (1) hour after a call from the COR. The Contractor shall assess the condition of the affected piece of equipment and report back to the COR with the findings and proposed corrective actions. This service order/call may result in placing a piece of equipment out of service for a short period of time until the situation is corrected. The Contractor shall complete all necessary repairs to return the affected equipment to service in accordance with the requirements of this PWS.

C3.11.4 The Contractor shall respond to all service orders/calls requested by the Contracting Officer's Representative (COR) or his/her designee within the timeframes established in the TO PWS.

C3.12 Types of Work and Monthly Repair Log

The types of work included in this requirement are the following:

- **C3.12.1 Routine/Preventive Maintenance** - the regularly scheduled and Routine/Preventive maintenance of the BCS/UCS systems to keep them running in exceptional operating condition and prevent any costly unplanned downtime from unexpected equipment failure. This work is covered under CLIN 0001, 0002, 0003, 0004, 0005 Routine/Preventive Maintenance and Repairs. This work is completed in accordance with the Routine/Preventive Maintenance Plan developed in Section C3.4.3 Routine/Preventive Maintenance Program.
- **C3.12.2 Repair Work, Minor Work or equipment replacement** - limited to individual alteration/new work tasks or repair work wherein the material costs do not exceed the discipline threshold (material and non-direct labor cost only) per job. Minor work includes but is not limited to work such as installation of equipment, reconfiguration of systems and minor facility alterations. See Section C**3**.1**6** Minor Work or equipment replacement At or Below the discipline threshold (material and non-direct labor cost only). For repair work under the discipline threshold, the Contractor must receive COR approval and submit a service order/call.

- **C3.12.3 <u>Non-Routine/Ad Hoc Repairs</u>** - Maintenance, repair, equipment replacement, alteration work requirements beyond the scope of the services performed under the CLIN 0001, 0002, 0003, 0004, 0005 Routine/Preventive Maintenance, Alterations, Minor Repairs, and Equipment Replacement and corresponding option CLIN(s). This work is over the discipline threshold and requires a Task Order to be issued by the Contracting office for work to commence. See Section C3.17 Non-Routine/Ad Hoc Repairs Resulting in Task Orders (At or Above the discipline threshold – material cost only/no labor).

C3.12.4 The process for delineating between the types of work and process for work approval is detailed below in Chart 1: Approval Process for Routine/Preventive repairs, Alterations, Equipment Replacement, and Non-Routine/Ad Hoc Work:

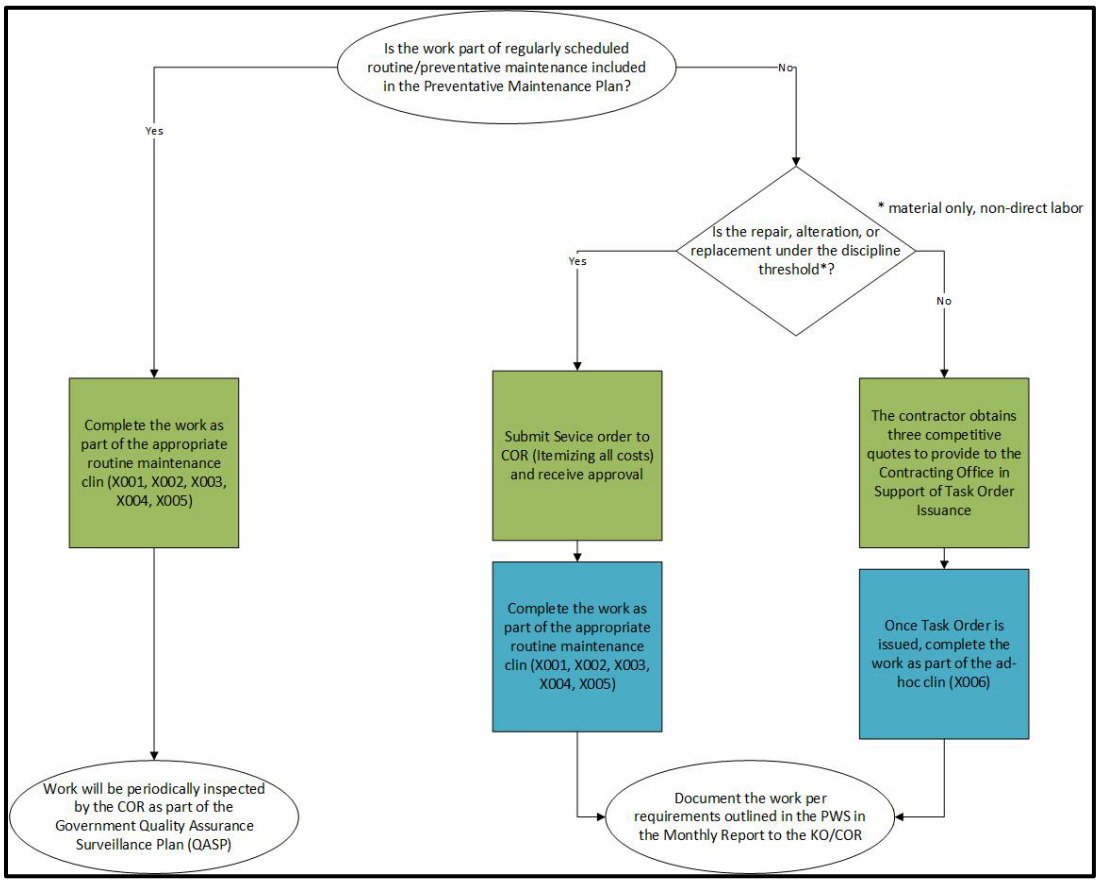


Chart 1: Approval Process for Routine/Preventive repairs, Alterations, Equipment Replacement, and Non-Routine/Ad Hoc Work with a discipline threshold of $3,000

C3.12.5 The Contractor shall maintain a record of all work performed for the month in a Repair Log and submit in the Monthly Report due to the KO/COR by the 5th.

C3.12.6 The Repair Log shall include, as a minimum, a description of the equipment, repairs performed, labor hours, labor cost, cost of materials and a running total for the COR's review. All Routine/Preventive and repairs are included in the monthly PM fixed-priced CLIN as part of Routine/Preventive maintenance. The Contractor is required to submit to the KO a report of activity from the preceding month which itemizes (by cost category) all Alterations and Repairs (submitted and approved) as well as all Ad-Hoc Task Orders (awarded).

C3.13 Minor Work or Equipment Replacement (At or Below the Discipline Threshold – material cost only/no labor)

C3.13.1 Minor Work or Equipment Replacement will be limited to individual alteration/new work tasks wherein the material and non-direct labor costs do not exceed the discipline threshold (material cost only/no direct labor) per job. It includes but is not limited to work such as installation of equipment, reconfiguration of systems and minor facility alterations. Time frames for completion of these alterations will be established by the COR/COTR when the service order/call is issued. Before beginning any Minor Work or Equipment Replacement under the discipline threshold, the Contractor must submit a service order/call (itemizing all costs) and receive COR approval.

C3.13.2 The Contractor shall correct all deficiencies discovered during the performance of maintenance activities.

C3.14 Non-Routine/Ad Hoc Repairs Resulting in Task Orders (At or Above the Discipline Threshold – material cost and non-direct labor only)

Non-Routine/Ad Hoc repairs resulting in separate Task Orders are defined as Non-Routine/Ad Hoc maintenance repairs, alterations, equipment replacement, or service order/calls beyond the scope of the services performed under the fixed price portion of the contract (CLINs 0001, 0002, 0003, 0004, 0005 and corresponding option CLINs). All Non-Routine/Ad Hoc repair work exceeding the discipline threshold will be executed via issuance of task orders under the IDIQ CLIN of the contract (CLIN 0006 and corresponding option CLINs).

C3.15 Pricing Non-Routine/Ad Hoc Repairs

The Contractor's Proposal **shall contain three competitive quotes for all parts/material needed to complete the repair**. In the event obtaining three competitive quotes is not practicable, the Contractor shall submit, in writing (as part of the task order proposal), documenting relevant reasons (e.g. market availability, sole source, etc.) why the submission of three competitive quotes was not performed. Proposals for Non-Routine/Ad Hoc work shall be constructed using a template provided by the Government. The Proposal shall be broken out to the task level, identifying both non-direct labor and materials associated with each task of the overall project. Contractors shall use Direct Labor personnel currently onsite as part of the Firm Fixed Price portion of the contract to perform the labor for Ad-Hoc Task Orders as available but may not include the labor cost for these personnel as part of the proposal. Proposals should explain the usage of any proposed personnel.

Cost Range, Proposal Submission Time:

$3,000.01 (material cost only/no labor) - $50,000, 5 Business Days
$50,000.01 - $100,000, 10 Business Days
$100,000.01 - $300,000, 15 Business Days
$300,000.01 - $1,000,000, 20 Business Days

C.4 SECURITY / CYBERSECURITY

The contractor shall provide cybersecurity (CS) in accordance with all current policies, procedures, and statutes, to include all references located in Attachment 3 REFERENCES/CODES. The requirements may vary based upon the site and network configuration since each system is different across the five sites. More specific information will be provided in each T.O. PWS.

C4.1 Personnel Requirements

C4.1.1 Language in this section mainly applies to 8140 personnel as indicated but some also applies to other/all contractor personnel (non-8140 personnel, etc.)

C4.1.2 Information given to the Contractor during the life of this contract shall only be used for the purpose of carrying out the provisions of this contract. Agency marked "Controlled Unclassified (CUI)" or bearing other sensitivity markings shall be handled in accordance with (IAW) Agency information security program regulations and shall not be divulged or disclosed without Agency permission in writing. Requests for disclosure shall be addressed to the Contracting Officer (KO).

C4.1.3 The Contractor shall provide skilled, experienced, professional and/or technical personnel consistent with the task requirements of this PWS, with staffing plans in the Contractor's technical proposal. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoW Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program upon contract and/or MOD awards.

NOTE: DLA's minimum certification required for the System Administrator (451) work role is the CompTIA A+, Network+, Security+ or Certified Network Defender (CND) certification. Individuals must also complete 20-hours of continuous education annually, or the number of hours required to maintain certification; whichever is greater.

C4.1.4 The Contractor is responsible to provide qualified personnel, as specified, and as required by the PWS, and shall bear all cost for training of its personnel as it relates to 8140 certification training and any system specific required certifications. The Government will not reimburse the Contractor for the cost of training Contractor personnel.

The DoD 8140, Information Assurance Workforce Improvement Programs requires training and certification for cybersecurity duties performed. All contract employees performing cyber-IA functions shall meet the requirements in accordance with DoW/DLA guidance. In support of DoD Manual 8140.03 Cyberspace Workforce Qualification & Management Program, provide, at a minimum, two personnel supporting cybersecurity requirements per site. The Offeror must provide a list of personnel that currently have 8140 certifications who will be supporting the PWS, as well as copies of those certifications at the time of contract award. (451) System Administrator is required, and the basic level, as a minimum. Security + is preferred over A+. The contractor must provide at least one each of the following 8140 certified personnel in support of each TO:

C4.1.4.1 SENIOR APPLICATION ADMINISTRATOR - Serves as the primary technical support role for one or more applications. Works closely with server administrators and database administrators, but maintains a level of separation, to facilitate segregation of duties. Installs, configures, and maintains all software products utilized by the application. This includes, but is not limited to, the installation/upgrade of software versions, installation of software patches, support for data center migrations, identifying application specific firewall/network requirements, setup/administration of interfaces & APIs, technical support for break/fix incidents, and support of application requirements being driven by organizational transformation initiatives. Responsible for both pre-production & production environments and directly supports the application's code release process. Leads in implementing any applicable application-based Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs), to include providing any required STIG/SRG output in support of the program. Researches and implements resolution of cybersecurity vulnerabilities discovered because of routine scanning.
Minimum Requirements:
• Seven (7) years of relevant experience
• BS, BA, or four (4) additional years of related experience
• Must possess minimum of Tier 3 (T3) and be 8140 Certified at time of proposal submission.

C4.1.4.2 INDUSTRIAL CONTROL SYSTEM (ICS) SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SPECIALIST - Applies Information Technology (IT) and Operational Technology (OT) security strategies such as the application of the National Institute of Standards and Technology (NIST) security controls, exploitation techniques and methods, continuous monitoring, and ICS acquisition life cycle as outlined in the NIST Special Publication (SP) 800-82 (Current version).
Minimum Requirements:
• Five (5) years of experience in control system network and security design.
• Global Industrial Cyber Security Professional (GICSP)
• Ten (10) years of practical industry, government and/or consulting experience in information technology management.
• Ten (10) years of relevant Certification and Accreditation (C&A) experience
• IT project management experience using various Microsoft tools.
• Knowledge and experience in managing information technology services and strategies.
• Proficiency in basic analytical software such as Microsoft Excel and Access, proficiency with the Microsoft Office suite, to include Word, PowerPoint, and SharePoint.
• Experience and broad knowledge of Utility Control System (UCS), Utility Monitoring and Control System (CS), Manufacturing and Distribution, and other types of control systems operating in different

modes than ICS such as Emergency Management Systems, Public Safety Communication Systems utilizing system specific protocols, ports, and services.
• National Institute of Standards and Technology (NIST) C&A experience
• DOD Cybersecurity experience
• Required to possess a DOD SECRET Clearance and be eligible for a minimum of Tier 3 (T3) and be 8140 certified upon assignment.

C4.1.5 The Contractor shall provide a monthly DoD 8140.03 deliverable report as specified by the COR that includes a list of applicable key personnel.

C4.1.6 If a certification becomes obsolete during the life of the contract, the Contractor shall be responsible for ensuring applicable personnel obtain an acceptable replacement certification prior to the IT/OT product's end of support or end of life.

C4.1.7 The provisions of this PWS shall be fully applicable to all subcontractors.

C4.1.8 Information given to the Contractor during the life of this contract shall only be used for the purpose of carrying out the provisions of this contract. Agency marked "Controlled Unclassified (CUI)" or bearing other sensitivity markings shall be handled in accordance with (IAW) Agency information security program regulations and shall not be divulged or disclosed without Agency permission in writing. Requests for disclosure shall be addressed to the Contracting Officer (KO).

C4.1.9 Personnel Security Requirements

Most work to be performed under this requirement is unclassified, however, a security clearance may be required. All CONUS Contractor personnel performing IT II/Moderate Risk duties require a Tier 3 (T3) investigation. Contractors performing IT I/High Risk duties require a Tier 5 (T5) investigation. an IT-I, a clearance requiring a Single Scope Background Investigation, prior to the work commencing. All positions requiring access to the Government network, computing environment, system(s), subsystem(s), and components will require a minimum of Moderate Risk IT clearance category eligibility (IT eligibility categories are defined in the table below) commensurate to the services rendered. The Contractor shall submit a CIR and a DD Form 2875 (see CIR and System Authorization Access Requests (SAAR) document in Technical Library) for temporary Moderate Risk IT eligibility, with final IT eligibility contingent upon receiving favorable adjudication. DLA retains the right to request removal of Contractor

personnel, regardless of prior clearance or adjudication status, whose actions, while assigned to this contract, clearly conflict with the interest of the Government. The reason for removal shall be documented in writing by the KO. When and if such removal occurs, the Contractor shall within a two to four-week timeframe, assign qualified personnel to vacancy(s) thus created regardless of whether the individual was in a key or non-key personnel position. Current personnel security investigations conducted for access to classified information may satisfy investigation requirements for sensitive information access position Personnel security investigations for sensitive information access will be initiated by the DLA Personnel Security Office.

TIERED INVESTIGATION STANDARDS

Tiered Investigation Standards					
Position	Low-Risk	Moderate Risk		High Risk	
		Confidential	Secret	Top Secret	SCI
Position Sensitivity	Non-Sensitive	Non-Critical Sensitive		Critical Sensitive	Special Sensitive
Investigation	Tier 1/NACI	Tier 3/NACLC/ANACI		Tier 5/SSBI	
Formerly Known As	IT-III or IT-3	IT-II or IT-2		IT-I or IT-1	

As outlined in DoDM5200.02, the Investigative Requirements and Civilian Positions are as follows:

Special-sensitive and Critical-sensitive. Civilian personnel in special-sensitive and critical-sensitive positions require a favorably adjudicated SSBI or its equivalent.

INVESTIGATIVE REQUIREMENTS.

DoDM 5200.02, April 3, 2017, Change 1, October 29, 2020, a. A non-U.S. citizen, including immigrant alien, may be issued an LAA (Limited Access Authorization) to systems and information under direct government supervision) investigative requirements of that country. b. A favorably completed and adjudicated SSBI (within the immediately preceding 5 years) is required before granting an LAA. If the SSBI cannot provide full investigative coverage, a polygraph examination (if there are no applicable host country prohibitions) to resolve the remaining personnel security issues will be favorably completed in accordance with DoDD 5210.48 before granting access.

If geographical, political, or medical situations prevent the full completion of the SSBI or prevent the polygraph examination to supplement a less than full SSBI, an LAA may be granted only with approval of the DDI(I&S).

If an LAA is withdrawn and the person subsequently is again considered for a new LAA, an SSBI and polygraph examination may be required. The scope of the SSBI will cover the period from the previous investigation or 10 years, whichever is shorter.

A PR will be conducted on every person with an LAA 5 years from the closing date of the previous SSBI or SSBI-PR, as appropriate. For both OT and IT system support and roles must Identify the role with the required IT 1,2,3 designation and the system/mission sensitivity Activities or roles are Identified in DoDM 5200.02 4.1.

Not all systems have the same criticality, moderate risk duties on a critical system are not the same as moderate duties on a non-critical system. The Impact to information and availability are different.

OCONUS INVESTIGATION STANDARDS

The following OCONUS countries require the investigation standards below for contractors:

Germany:

Local National Screening Program (LNSP) database, instructions for processing and access are all on the home page https://lnsp.ext.eur.army.mil/. Access must be requested via the Garrison. This is a generalized breakdown of the process for Germany.

* AR 604-1B
* Führungszeugnis (German Police Good Conduct Certificate (PGCC))
* Ausweis (Photo ID) front & back
* Individual must have lived in Germany for a minimum of 12 months leading up to the check.
* For non-German citizens from the EU, registration from the local German Rauthaus is required as proof of residents.

Italy:

Italian Air Force checks which include Interpol/Caribinieri and arrest checks. (Initial and 3 year (childcare) or 5 years (non-childcare). Additionally, prior to employment the local national provides a "Certificato Penale" which is like a local police check.

Italy/Spain/Greece/Poland/Romania do NOT issue CACs for LN's CACs are authorized for LN/HN in AFRICOM theater (CLDJ/Bahrain/Isa) after completion of the base vetting requirements.

SENSITIVE INFORMATION ACCESS

Sensitive information access positions are designated based on access to government networks and IT systems and may exceed classified access requirements for this contract.

Note that sensitive information access does not imply or convey access to classified information or DOW systems access where sensitive information is stored.

For sensitive information access positions, the required investigation shall be completed, or interim access granted for individuals assigned to sensitive duties. The provisions outlined above apply to the prime contractor and any subcontractors the prime contractor may employ during the course of the contract. In lieu of the correct investigations being completed when contract employees start, a waiver interim clearance may be submitted if no issues exist within the National Background Investigation Services (NBIS) Questionnaire (SF 85) for Non-Sensitive Positions or Questionnaire (SF 86) for National Security Positions. The contractor shall have the NBIS form completed, with any other requirements (fingerprints taken and, if required, an OF306), and reviewed by DLA Intelligence before officially hiring any contractor employee into sensitive information access positions Declarations for investigation to non-sensitive, sensitive CUI and system access, critical information and related systems access need to be properly Identified. All foreign nationals must be cleared by the correct type of investigation depending on information access and system access. Reference DLAI 5210.01 Effective: February 4, 2021, DoDM 5200.02.

Please note that physical access to DoW installations is not the same as access to sensitive information or DoW sensitive systems access and is covered under DOD M 5200.08 Volume 3.

ACCESS TO CLASSIFIED INFORMATION

Most work to be performed under this requirement is unclassified; however, a higher security clearance may be required for some TO PWSs. Contractor must have available staff with a favorably adjudicated investigation prior to the contract award. Contractors shall not be required to store, handle, or process classified information at their facility. Contractors with a safeguarding requirement will need to be approved for safeguarding at the same or higher level of classification listed in Block 1b of DD Form 254.

Contractors are required to comply with 32 CFR Part 117 National Industrial Security Program Operating Manual (NISPOM) in the handling, protection, and safeguarding of classified information in their possession. Security requirements outside the scope of the NISPOM if required, will be defined in the accompanying DD Form 254.

The personnel security investigations conducted for access to classified information will be started by the contractor company Facility Security Officer (FSO).

C4.1.10 Citizenship

Each Contractor employee shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence, or who presents evidence from the Immigration and Naturalization Service that employment will not affect his immigration status.

C4.1.11 Identification Badges

Contractor employees (including those of subcontractors) requiring physical access to the contractual place of performance and/or access to the DLA network/system for successful contract performance will be required to obtain a Common Access Card (CAC) prior to starting work. Lost or stolen CACs must be promptly reported by the Contractor to the KO or their authorized representative and to the appropriate Government security personnel. The Government will retain sole decisional authority on the issuance of a replacement CAC.

C4.2 Privileged Access

C4.2.1 The Contractor shall provide skilled, experienced, professional and/or technical personnel consistent with the task requirements of this PWS, with staffing plans in the Contractor's technical proposal. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoW Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program upon contract and/or MOD awards. The Contractor is responsible to provide qualified personnel, as specified, and as required by the PWS, and shall bear all cost for training of its personnel as it relates to 8140 certification training and any system specific required certifications. The Government will not reimburse the Contractor for the cost of training Contractor personnel. All contract employees shall have acquired the necessary certifications, per the DoDM 8140.03, and remain in good standing for the duration of the contract. These certification requirements are not based on position title; they are based on duties. All Contractor personnel requiring elevated/privileged access to any network or OT system, subsystem, or components, either during provisioning or post award, shall satisfy any necessary and/or applicable requirements to meet DLA account provisioning, system administration, and personnel certification standards.

C4.2.2 The DoDM 8140.03, Cybersecurity Workforce Improvement Programs requires training and certification for Cybersecurity duties and Cybersecurity duties performed. All contract employees performing cyber-IA functions shall meet the requirements in accordance with DoW/DLA guidance.

C4.2.3 Additionally, all contract employees shall be certified in operating systems on any system on which system administration duties are performed. System specific certifications may be required as well and will be outlined as part of the minimum contract requirements. Proof of certification shall be provided before privileged access is granted, at time of proposal/resume submission; this includes, but is not limited to, system administration access,

network administration access, router/switch access, or firewall access. All documentation required for security certification will be maintained by both the Contractor and the Government. Available upon request, the DLA approved Cybersecurity (CS) Computing Environment (CE) list will be provided with information on the required role-based certifications.

C4.2.5 The Contractor shall provide a copy of all current certifications to the Contracting Officer at time of award and remain in good standing during the contract period of performance. The Contractor shall provide the monthly DoDM 8140.03 deliverable report to the COR/COTR that includes a list of applicable DoDM 8140.03 key personnel. If a certification becomes obsolete during the life of the contract, the Contractor shall be responsible for ensuring applicable personnel obtain an acceptable replacement certification prior to the IT/OT product's end of support or end of life. The Contractor is responsible for all PWS requirements and shall provide skilled, experienced, professional, or technical personnel consistent with the task-specific requirements.

C4.2.6 DoDM 8140.03 baseline certifications can be found here:

DoDM 8140.03 (Manual) Cyberspace Workforce Qualification and Management Program: https://dl.dod.cyber.mil/wp-content/uploads/cyber-workforce/pdf/unclass-dod-manual-8140_03.pdf

The Contractor shall provide a monthly DoDM 8140.03 deliverable report as specified by the COR, that includes a list of applicable key personnel. The following information shall be provided in the report, due by the 5th business day of each month:

Work Role
Work Role Task
Company
Contract Name/Description
COR Name
Contract #
Primary Foundational Qualification Personnel Certification Held and Expiration Date
Primary Foundational Qualification Personnel Certification Status (Current or Past Due)

C4.2.7 To maintain DLA base user accounts and elevated privileged accounts, Contractor employees must login to their DLA base user account, elevated privileged account, and DLA

email on the 1st and 15th of the month to maintain active account status. The Contractor shall send an email to the COR/KO or designee from their DLA email upon signing in on the 1st and 15th of the month verifying successful login to the base/elevated account. Contractor employees must also complete all initial and annual mandatory training requirements within 5 business days of request. Contractors will be notified by DLA email of all expiring mandatory training requirements. Courses are accessed through the Skillport website located at: https://j6enterprise.skillport.com.

C4.2.8 Contractors shall login to their DLA account through Government Furnished Equipment (GFE) or Remote VDI Access located at: https://www.dla.mil/Remote-VDI/. Remote VDI access requires a CAC card and CAC reader to utilize. Logging into the privileged account utilizing account token will require a secondary card reader. All CAC readers must comply with DLA Cyber Emergency Response Team (CERT) policy and can be acquired through a Computer Accessory Request in the DLA Service Portal.

C4.3 Cybersecurity Strength Requirements

C4.3.1 The Contractor shall satisfy the Risk Management Framework (RMF) requirements of subchapter III of chapter 35 of Title 44, United States Code (U.S.C.), also known as the "Federal Information Security Management Act (FISMA) of 2002 (Modernization 2014)".

C4.3.2 The Contractor shall enable DLA to meet the standards required by the Office of Management and Budget (OMB) and the Secretary of Commerce, pursuant to FISMA and section 11331 of Title 40, U.S.C.
FIPS 199 / CNSSI 1253 Security Categorization: The Contractor shall participate in categorization discussions with the DLA J6 PM, functional lead, and the Information System Security Manager (ISSM) and provide all required FIPS 199 documentation as requested to support security categorization.

C4.3.3 The Contractor shall collaborate with the Government Program Manager on system categorization based on sound technical expertise in accordance with FIPS 199 then work in coordination with the prescribed DLA System Owner (SO) and ISSM to support the categorization IAW FIPS 199, CNSSI 1253 and Office of the Secretary of War (OSW) Facility Related Control Systems (FRCS) Master List including DLA specific systems, then document the results of the security categorization in the System DLA FIPS 199 document and the Concept of Operations (CONOPs).

C4.3.4 Assigned DLA J6 PM will coordinate with the Contractor to identify and document Confidentiality, Availability, Integrity (CIA) of the system in a DLA FIPS 199 document for approval by DLA ISSM personnel.

C4.4 Cybersecurity Assurance Requirements

C4.4.1 The Contractor shall design, develop, and integrate cybersecurity solutions supporting the Department of War and all other applicable Government agencies.

C4.4.2 This will be achieved through abiding by all applicable cybersecurity policies, regulations, and directives to ensure a favorable Assessment and Authorization (A&A), Assessment and Incorporate (A&I), or FRCS Assess Only Risk Assessment decision, as well as obtaining an Authority to Connect (ATC) to DLA's network. The Contractor shall mitigate risk identified through the RMF authorization process down to a level acceptable to the DLA Authorizing Official (AO).

C4.4.3 Application and software development and use for security. The Contractor shall provide documentation of development practices and standards applied to Government approved Contractor-written control system software, including firmware, used to ensure a high level of defense against unauthorized access. For any software development, the contractor shall provide the Government with software bill of materials (SBOM). See the following link which includes the table of minimum elements data fields for the SBOM:

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cisa.gov/sites/default/files/2025-08/2025_CISA_SBOM_Minimum_Elements.pdf

C4.4.4 The solution shall comply with the security control requirements documented in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53r5, "Security and Privacy Controls for Federal Information Systems and Organizations" and NIST 800-82r3, "Guide to Industrial Control Systems (ICS) Security". The Contractor shall provide details of any alternative, but equally effective security measures used to compensate for the inability to satisfy a particular derived security requirement (mitigation to control compliance findings). This information shall be submitted in writing to the DLA J6 PM for cybersecurity approval as soon as the alternative is identified. All vulnerabilities associated with solutions must be reported to the DLA J6 PM with a Plan of Action and Milestones (POA&M) for remediation.

C4.4.5 Zero Trust (ZT) (Future)

The contractor shall enable DLA to meet requirements aligned with Zero Trust (ZT) implementation and compliance, in accordance with NDAA 2022 and EO 14028. They will implement and maintain all required ZT for OT Activities and Capabilities for any applicable devices, systems, applications, services, and data supported or developed by the contractor as outlined in the DoW ZT Strategy and supporting documentation to meet the end of FY2030 DoW mandate for "Target" level ZT for OT and FY2035 to reach "Advanced" level ZT for OT. The contractor must provide support, as required, to allow DLA managed services to be added, removed, or modified in the environment to meet DoW ZT requirements. This support may also require facilitating internal and external assessments, audit, and other evaluations of ZT implementation status, effectiveness, and compliance. The contractor must remediate any findings from these assessments, audits, and evaluations for applicable devices, systems, applications, services, and data supported or developed by the contractor.

The contractor shall enable DLA to meet requirements for Identity, Credential, and Access Management (ICAM) which aligns to the Seven Pillars of Zero Trust (ZT) Compliance: (1) Visibility & Analytics, (2) Devices, (3) Network/Infrastructure, (4) Data, (5) Application/Workload, (6) User, and (7) Automation & Orchestration and adheres to Federal Information System Controls Audit Manual (FISCAM), Identity, Credential, and Access Management (ICAM).

C4.4.6 Typical Contractor services activities include:

a. Analyzing DLA physical, electrical, computerized, and mechanical environments the identified FRCS, ICS, or Facilities Internet of Things (IoT) solution will control (e.g., the physical Operational process to be controlled, such as those used in manufacturing, metering, and robotics)
b. Developing a DLA automation solution FRCS, ICS, or Facilities IoT architecture in terms of devices, dataflow, and control loops, outlining interconnectivity with engineering and operator workstations, and Safety Instrumented Systems (SISs) for testing; testing shall be in accordance with DoW Control Systems Security Requirements Guide (SRG), and other identified DLA test processes.
c. Defining how the DLA FRCS, ICS, or Facilities IoT automation solution will connect to external (e.g., plant) and networks, by system description, concept, and dataflow diagram on Purdue Levels. DLA's official model is the Purdue Enterprise Reference Architecture (PERA) Any required deliverables shall map to the DLA PERA attachment provided.
d. Installing, configuring, patching, backing up, and testing the solution. The contractor shall be responsible for installing, configuring, patching, backing up, and testing any application software solution. If the system resides on a DLA approved network, DLA shall be responsible for all installing, configuring, patching, backing up, and testing any Operating System (OS) software solution.
e. Gaining approval of the DLA asset owner for many of the decisions made and outputs generated during the execution of these activities.

C4.4.7 The Contractor shall protect unclassified DoW data from unauthorized access or disclosure in accordance with DoDI 8582.01, "Security of Unclassified Information on Non-DoW Information Systems." Controlled Unclassified Information: All Government controlled unclassified information obtained by the Contractor shall be protected in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations".

C4.4.8 Agencies or Military Services providing external information system services must comply with DLA information security requirements and employ overlayed security controls in accordance with applicable federal laws, Executive Orders, directives, instructions, policies, regulations, standards, and guidance.

C4.5 Tasks and Deliverables

C4.5.1 The Contractor shall provide required implementation and design documentation to the DLA J6 PM and security engineering teams to conduct a cybersecurity risk assessment (RA) of

proposal. Results from accepted RAs will be incorporated into the Systems concepts of operations (CONOPs).

C4.5.2 The Contractor, in collaboration with assigned security manager, DLA J6 PM and system owner, shall identify and document applicable cybersecurity enterprise architectures and deliver system conceptual design drawings.

C4.5.3 The Contractor shall leverage, to the greatest extent possible, DLA Enterprise processes and capabilities.

C4.5.4 The Performance Requirements Summary (PRS) and RMF Documentation Chart and Submission Dates Table, located in Attachment 4, provides a summary of the deliverables required of the Contractor based on identified cybersecurity requirements for Assess and Authorize (A&A), Assess and Incorporate (A&I), and Facility Related Control System Lean Cybersecurity Risk Assessment (FRCS LCRA).

C4.6 System and Network Requirements

C4.6.1 All system/network components and applications shall be compatible with all applicable Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs). Any STIG exceptions must be identified as part of the Contractor's proposal to the Government and approved by J6 Cybersecurity. Exceptions incurring risk found unacceptable to the DLA Authorizing Official are not permitted.

C4.6.2 If cloud technology is in use, it must be FedRAMP+ Authorized at an Impact Level (IL) commensurate with the level of information DLA will be processing. In most cases this is IL Level 4 or 5. The authorization for the technology in use must be listed on FedRAMP Marketplace prior to contract award https://marketplace.fedramp.gov/products .

C4.6.3 All network components and applications shall be IPv4 and IPv6 compatible.

C4.6.4 Network components shall allow configuration of IEEE 802.1x or port security for authentication.

C4.6.5 The Contractor shall provide a complete list of all ports, protocols and services required for any computer system running control system applications or required to interface the control system applications. The Ports, Protocols and Services Management (PPSM) listing shall include all ports and services required for normal operation as well as any other ports and services required for emergency operation. The listing shall also include an explanation or cross reference to justify why each service is necessary for operation.

C4.6.6 The Contractor shall identify any system wireless communication capability, enabled, or disabled. All wireless communications shall meet applicable STIG requirements to include FIPS 140-3 certification. Any requirement to use wireless or cellular must be approved in writing by DLA J6, coordinated with the DLA J6 PM and documented with the DLA Frequency Manager. Wireless or cellular requirements shall be presented as early as possible to possibly incorporate into planning for the effort.

C4.7 Information and Operational Technology Infrastructure Requirements

C4.7.1 In general, the Government expects to furnish and support the IT Infrastructure to host the OT solution(s) and/or system(s) (including VLANs, and Virtual Machines (VMs)) unless there is a hardware, compatibility, or mission issue preventing it. If so, the Contractor must provide justification clearly identifying why and "what" anticipated Government IT Infrastructure is required to host and operate the OT solution(s) and/or system(s) within the design documentation submitted for Government approval at time of award. These anticipated designs will be incorporated into the system CONOPs. In this scenario, DLA is responsible for infrastructure, and the Contractor shall be responsible for all installation, configuration, deployment and support of the OT solution(s) and/or system(s) (including but not limited to) its subsystem(s), application(s), and patch cabling, if required. DLA shall furnish all virtual server and management workstation hardware and DLA will be responsible for supporting hardware and OS throughout the lifecycle. DLA can provide a virtual server with the latest supported OS and Contractor shall provide server specifications along with justification and supporting documentation for approval by DLA J6 (DLA virtualization Team and/or the DLA Storage Team) in advance. In this scenario, DLA is responsible for hardware and OS, and the Contractor shall be responsible for installation, configuration, deployment, and support of the OT application/solution.

C4.7.2 Any requirement for the Vendor to provide their own physical server/appliance or management workstation hardware due to compatibility issues or performance shall be documented in the Vendor proposal and Contractor will get approval from DLA J6 prior to purchasing these items. Vendor supplied systems must meet DoW STIG requirements, with any exceptions noted in the proposal. When approved by DLA J6 in advance, DLA will provide virtual infrastructure to support deployment of contractor supplied management workstations, physical/virtual servers or appliances (OVA files). Vendor supplied systems must meet DoW STIG requirements, with any exceptions noted in the proposal. In this scenario, if server/appliance/workstation is approved by DLA to support in advance, then DLA will provide infrastructure and will support server/appliance or management workstation hardware and OS, and the Contractor shall support the OT application/solution. If contractor furnished server/appliance/workstation is not approved by J6 to support or in cases where standalone is needed or advised by Contractor to support OT solution (like systems for/in secure areas, etc.), the Contractor (not DLA) shall be fully responsible for providing and supporting network infrastructure, servers/appliances, workstations/laptops as well as all the OT devices and applications. The Contractor shall provide justification for standalones for DLA approval in advance.

C4.7.3 Vendor Furnished Physical Server or Appliance

C4.7.3.1 In some instances (such as video surveillance) where there is a requirement for a large amount of storage, the preferred solution recommended by Contractor may be a physical server or an appliance that includes compute/storage in one physical device that meets DoW, NIST and USG regulatory and Cybersecurity policy requirements.

C4.7.3.2 The physical server/appliance shall be sized adequately to store a minimum of 30 days or in accordance with specifications documented in the Task Order PWS if different than the 30 days.

C4.7.3.3 The Contractor shall furnish the physical server/appliance hardware but will get approval from DLA J6 to support prior to purchasing. Depending on make/model of hardware, DLA J6 may be able to support and provide a DLA OS image for the physical server/appliance. If so, DLA J6 will be responsible for the hardware and OS, and the Contractor shall be responsible for the applications related to the OT system. If J6 is not able to provide a DLA image/support for the physical server/appliance, then the Contractor shall be fully responsible for all configuration and deployment of hardware, OS as well as OT application/solution. The Contractor shall be responsible for all physical maintenance activities for any/all appliances including but not limited to, replacement of defective components such as hard drives (to be destroyed onsite per DoW policy, guidance), motherboards, daughterboards etc. and software maintenance activities including but not limited to, firmware updates, OS patching, software patches etc. for the duration of the contract period.

C4.7.4 System(s) shall operate using fully supported OS, software, and firmware throughout the duration of the contract and reviewed and approved by DLA J6 prior to purchase and implementation. All operating systems, software, and firmware shall be upgraded prior to the manufacturer's end of mainstream support for the OS, software, or firmware. The preference is for a virtualized solution. The solution must be upgradeable and remain compliant to cybersecurity specifications during the lifecycle of the solution. The Contractor shall adhere to approved DLA technologies for OS. Available upon request, the DLA Enterprise Architecture Technology Visualization link will be provided.

C4.7.5 The system management workstation requirements shall be able to operate on the latest workstation approved OS.

C4.7.6 For virtualized appliances or virtualized servers, the system shall be capable of running on the latest VMWare.

C4.7.7 Database shall operate using the latest Database Operating System version.

C4.7.8 System must be capable of operating with the latest anti-virus software that's approved for use within DLA.

C4.7.9 Any requirement for the Contractor to provide their own IT Infrastructure, standalone server, or management workstation hardware due to compatibility issues must be documented in the Contractor's proposal and approved by J6 prior to contract award, if applicable. All Contractor provided IT Infrastructure must meet DoW STIG requirements. If the Contractor provides their own IT Infrastructure for the OT solution(s) and/or system(s), upon AO approval of the security authorization package (and prior to final OT solution(s) and/or system(s) acceptance or go-live), all Contractor provided IT Infrastructure will become the property of the Government.
All specialized software provided by the Contractor to the Government must have the applicable license key as well as sales/transaction records, ownership control(s), manuals, technical publications, documentation, and any other information supporting ownership accompanying it. At the time of Contractor hand-off of Contractor owned IT Infrastructure to the Government, all

design information for Enterprise Architecture (EA) for the "as built" OT solution(s) and/or system(s) will be provided. Any Contractor provided OS, software, and firmware throughout the duration of the contract will be upgraded by the Contractor prior to the Contractor's end of mainstream support for the OS, software, or firmware.

C4.7.10 The Contractor will be responsible for the implementation including meeting all required STIG compliance.

C4.7.11 The Contractor shall be responsible for all configuration and deployment which meet DoW, NIST and USG regulatory and cybersecurity policy requirements.

C4.7.12 Any OT solution(s) and/or system(s) with IT Infrastructure provided by the Contractor must be upgradable and remain compliant to cybersecurity specifications during the lifecycle of the solution. Contractor supplied systems must meet DoW STIG requirements, with any exceptions noted in the design documentation.

C4.7.13 Maintenance activities start after handover of the DLA Automation Solution to the DLA asset owner and may continue until the asset owner no longer requires them. Activities are typically short and frequently recurring, and may include one or more of the following:

a. Patching and anti-virus updates
b. Equipment upgrades and maintenance, including small engineering adjustments not directly related to control algorithms
c. Component and system migration
d. Change management
e. Contingency plan management

C4.7.14 All maintenance activities will include completion of identified DoW/DLA Security Awareness training, independent of other training received.

C4.7.15 System(s) shall operate using fully supported OS, software, and firmware throughout the duration of the contract. All operating systems, software, and firmware shall be upgraded prior to the manufacturer's end of mainstream support for the operating system, software, or firmware. The solution must be upgradable and remain compliant with DoW cybersecurity specifications during the lifecycle of the solution.

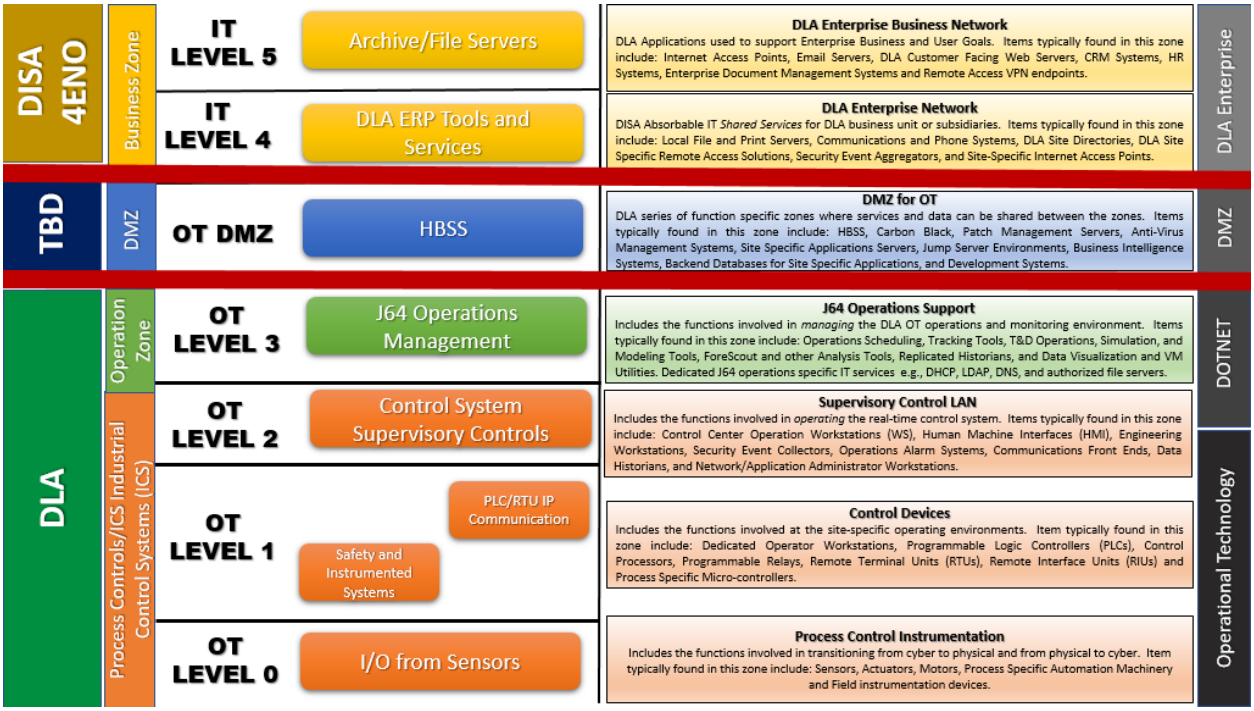
C4.7.16 Government furnished removable flash media shall be requested for system operation and must be reviewed and accepted by the DLA Flash Media Approval Program. Contractor furnished removable flash media shall be provided in advance and will be reviewed for use on a case-by-case basis. Files may be sent via DoD SAFE. All FRCS, ICS, or Facilities IoT solution(s) and/or system(s) must use the PERA Model for Control Hierarchy and must match the included attachment. (Reference ISA Technical Library online https://www.isa.org/) to provide logical and/or physical architecture for networking, security hardware, software, and methods. The PERA Model is an industry standard for manufacturing and/or industrial control systems that segments hardware, devices, and equipment into a hierarchical based design.

DODM 8140.03 WORK ROLE

(451) System Administrator					
		Basic	Intermediate	Advanced	NOTES
Foundational Qualification Options	Education	High school diploma or equivalent, or higher	Associate degree or higher from an accredited college or university	Bachelor degree or higher from an accredited college or university	When Education is listed, recommend an accredited Computer Science, Cyber Security, Information Technology, Software Engineering, Information Systems, or Computer Engineering degree; or a degree in a Mathematics or Engineering field.
		OR	*OR*	*OR*	
	Training	Offerings listed in DoD 8140 Training Repository	Offerings listed in DoD 8140 Training Repository	Offerings listed in DoD 8140 Training Repository	
		OR	*OR*	*OR*	
	Personnel Certification	A+ or CND or Network+ or Security+	Cloud+ or GICSP or GSEC or SSCP	CASP+ or CCNP Security or CCSP	See the Certification Index tab at the end of this document for certification vendor information.
Foundational Qualification Alternative	Experience	Conditional Alternative	Conditional Alternative	Conditional Alternative	Refer to Section 3 of the DoD 8140 Manual for more information.
Residential Qualification	On-the-Job Qualification	Always Required	Always Required	Always Required	Individuals must demonstrate capability to perform their duties in their resident environment.
	Environment-Specific Requirements	Component Discretion	Component Discretion	Component Discretion	
Annual Maintenance	Continuous Professional Development	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	

Reference:
https://www.cyber.mil/dod-workforce-innovation-directorate/8140/qualification-matrices

DLA PURDUE MODEL



C4.8 Installation Security

C4.8.1 Contractor Security Regulations and Conduct

C4.8.1.1 The Contractor or any visitors of the Contractor entering DoD locations to perform contract requirements shall abide by all security regulations and may be subject to security inspections. Contractor personnel and property shall be subject to search and seizure upon entering, while on, and upon leaving the DoD locations pursuant to regulatory guidance.

C4.8.1.2 All Contractor personnel shall always conduct themselves IAW acceptable business decorum. The Contractor shall remove any individual from the site whose continued presence or employment on this contract is deemed by the KO or designee to be contrary to the public interest, adversely affect health, morale, welfare, or good order and discipline on the installation, or is inconsistent with the best interests of national security. IAW USC Title 18, Crimes and Criminal Procedure, Part I, Crimes, Chapter 67, Military and Navy, Section 1382, the Installation Commander has the authority to bar individuals from the host installation.

C4.8.1.3 In the event of a strike by Contractor personnel, the Contractor shall be responsible for the cost of any increased security as determined necessary by the Installation or DLA Site Commander/Director

C4.8.1.4 The Contractor shall report immediately to the KO or designee any suspected, alleged, or actual criminal incidents IAW DLAI 5105 Reporting of Criminal Incidents.

C4.8.2 Contractor Vehicles

C4.8.2.1 The Contractor shall register all Contractor vehicles used in performance of the contract requirements and ensure that Contractor employee vehicles to be driven on the host installation, to include motorcycles, are registered with the host installation security office and are in conformance with State and local regulations in effect at the time of registration and as long as employed by the Contractor. Evidence of a valid driver's license, vehicle registration card, and insurance are required for registration. Contractor employees shall maintain current registration and proof of insurance on all Privately-Owned Vehicles (POV) brought on host installation. The Contractor shall maintain current registration and proof of insurance on all Contractor-owned vehicles brought on the host installation.

C4.8.2.2 The Contractor and its employees shall abide by host installation parking regulations. All vehicles shall be parked in designated parking areas only. The Contractor and its employees shall conform to Federal, State and host installation driving regulations.

C4.9 Information Security

C4.9.1 Upon favorable review and initiation of the PSI to establish the suitability of an employee for the job and the approval for temporary IT access pending final adjudication but not less than fourteen (14) working days prior to the employee's start date, the Contractor shall request Information Technology (IT) eligibility for an employee requiring access and passwords to the government data systems. The employee may start prior to the fourteen working day timeline at the Contractor's discretion provided all other Personnel Clearance requirements are met and there is adequate contractor workload which does not require IT access. All Contractor employees who perform data entry and query functions shall require IT Level III category eligibility (the minimum access level that includes no sensitive or classified information).

C4.9.2 Contractor access to Government IT data systems shall be granted on a "need-to-know" basis, IAW DLAI 6401 IA Management Controls and IA Technical Controls to Contractor personnel who will perform data input and retrieval functions and for "clearance special access," if applicable IAW DoD 5200.2-R, Personnel Security Program. All Contractor personnel provided with access to government computers and systems shall observe IT security policies and procedures as provided by the KO or designee. The Contractor shall notify the KO or designee within 12 hours when, for reasons of personnel resignation, reassignment, termination, or completion of portions of the contract, Contractor personnel no longer require access to government systems.

C4.9.3 The Contractor shall observe all copyright agreements. In the interest of protecting government systems from computer viruses, the Contractor shall not use public domain software nor shall Contractor personnel download software from public bulletin boards or Internet websites. Should the introduction of a computer virus or malicious destruction of computer software, stored information, or hardware result from the use of public domain software or from software taken from a public bulletin board or Internet website, the Contractor shall be required to repair the damage and incur all costs at no expense to the Government and without impact on delivery schedules.

C4.10 Privacy Act Information

Contractor shall comply with the requirements of DoD Directive (DODD) 5400.11 regarding control of privacy act information. Specifically, the Contractor shall ensure that any personally identifiable information (such as but not limited to individual names and associated personal contact information or social security numbers) is restricted to access required for execution of this contract and is not disclosed or stored on any unsecure systems.

C4.11 Sensitive Information

Work on this IDIQ will require Contractor personnel to have access to sensitive, privileged, or Privacy Act information. Personnel shall adhere to the Privacy Act, (5 U.S.C. § 552a) and applicable Agency rules and regulations. Contractor personnel shall not divulge, or release privacy data or information developed or obtained in the performance of this contract award, until made public or specifically authorized by the Government. The Contractor shall not use, disclose, or reproduce a third-party company's proprietary data, other than as authorized and required in the performance of this IDIQ award. The Contractor shall notify the COR within 24 hours, identifying personnel that no longer require access to Government Information Systems (IS).

C.5 DELIVERABLES

C5.1 Monthly Status Report

The Contractor shall provide a monthly status report that analyzes all active/in-process task orders current status and provides task orders accounting information. The Performance Requirements Summary (PRS) and RMF Documentation Chart and Submission Dates Table, located in Attachment 4, provides a summary of the deliverables required of the Contractor.

The Contractor shall also provide the following reports or documentation to the COR on the dates indicated below:

Deliverable	Due Date
(a) Monthly report	Attached to monthly Invoice.
(b) Accident report	Within 24 hours of any accident under contract.
(c) Equipment Inspection Certificates	Within 10 days after inspection.
(d) Equipment/load test report	Within 10 days after testing.
(e) Insurance Certificate	Within 5 days after award.
(f) Quality Deficiency Reports	Response due within 24 hours after issuance.
(g) Contractor's Points of Contact	Within 1 business day of award and 60 days prior to each option year.
(h) Certificate of Operation	Within 1 business day after award.
(i) Strike Contingency Plan	Within Ten (10) days after the award of the contract.
(j) Subcontracting Plan	Within Ten (10) days after the award of the contract
(k) Deficiency Joint Inspection	Scheduled within Ten (10) calendar days after the Contractor receives the notice of award.
(l) Deficiency List Submittal	Submitted to the KO and COR for review within fifteen (15) days after the joint inspection.

C5.2 Cyber Deliverables

The table below provides a summary of the deliverables required of the Contractor based on identified cybersecurity requirements for Assess and Authorize (A&A), Assess and Incorporate (A&I) and Lean Cybersecurity Risk Assessment (LCRA). DLA Artifacts are documents or evidence provided to document the information system and support test results for RMF assessment procedures. Artifacts provided as supporting evidence to test results must be associated with relevant Assessment Procedure(s). Other deliverables may be added or updated at the task order level.

The documents below are required for either an A&A or A&I/LRCA, but will be provided by the Government:

- Configuration Control Working Group Charter
- Supplemental Implementation Guide Contingency Plan
- MOU/MOA/SLA
- Incident Response Plan
- Maintenance SOP
- Privacy Documentation
- System Development Life Cycle (SDLC) Documentation
- DLA Access Control Policy
- Disaster Recovery Plan

#	Deliverable Name	Reference	Submission Due	A&A	A&I/LCRA
1	DoDM 8140.03 Report	C4	Monthly (NLT 5th business day of each month)	Required	Required
2	DoDM 8140.03 Certifications/Information Assurance Certifications	C4	At time of award or when onboarding of replacement personnel	Required	Required
3	CP After Action Report	TO PWS	As listed in the TO PWS	Required	Recommended
RMF Documentation:					

#	Deliverable Name	Reference	Submission Due	A&A	A&I/LCRA
1	System Diagrams (Architecture, Authorization Boundary, Data Flow and Purdue)	C4, C4.4.6	Draft- One (1) month after contract award Final - six (6) months after contract award Update at least annually	Required	Required
2	Comprehensive Hardware/ Software List (DLA provided template)	C4, C4.4.6	Draft- One (1) month after contract award Final - six (6) months after contract award Update at least annually	Required	Required
3	System CONOPs	C4.3.3, C4.5.1, C4.7.1	Six (6) months after contract award Update at least annually	Required	Required
4	Ports, Protocols and Services Management (PPSM)	C4, C4.6.5	Four (4) months after contract award Update at least annually	Required	Required
5	FIPS 199 Categorization	C4, C4.3.2, C4.3.3, C4.3.4	One (1) month after contract award Update at least annually	Required	Required
6	Cybersecurity Scan Results (ACAS, SCAP, WebInspect)	C4	Draft - One (1) month after contract award Final - six (6) months after contract award Update at least annually	Conditionally required for systems with public facing presence	Conditionally required where AB includes components at Purdue 2/3
7	Security Technical Implementation Guides (STIGs) and Security Requirement Guides (SRGs) Checklists	C4, C4.6.1, C4.6.6, C4.7.2, C4.7.9, C4.7.10, C4.7.12	Six (6) months after contract award Update at least annually	Required	Required

8	Documentation supporting RMF security control implementation (as outlined in DLA RMF SOP)	C4, C4.4.4, C4.4.8	Six (6) months after contract award Update at least annually	Required	Required
9	Control assessment procedure test results	C4, C4.4.4, C4.4.8	Six (6) months after contract award Update at least annually	Required	Required
10	Plan of Actions and Milestones (POA&Ms)	C4.4.4	Six (6) months after contract award Update at least annually	Required	Required
11	Privacy Risk Impact Level Analysis (PRiLA) Categorization Worksheet Privacy Impact Assessment	C4.4.4	One (1) month after contract award Update at least annually	Required	Required
12	System Administrator Installation/ Configuration Documentation	C4.7.3.3, C4.7.11	Four (4) months after contract award Updates as required	Required	Required
13	Application Software release/patch Documentation	C4.4.6, C4.7.3.3, C4.7.11	Four (4) months after contract award Updates as required	Required	Required
14	FedRAMP+ Authorization (if cloud technology)	C4.6.2	Prior to contract award Remain current	Required	Required

C.6 TASKS AND DELIVERABLES (BY SITE)

BCS UCS OT Equipment Groupings by Location/Site

	Elevator Systems	Electrical & Lighting Systems (Building)	HVAC + BAS + Utility Metering Systems	Electrical Distribution (Site)	Water Systems (Potable, Sewer/ Waste)	Remarks
DLA Headquarters Complex, Fort Belvoir, VA (HQC)	Contractor	Contractor	Contractor	Contractor	N/A	Confirmed
Defense Supply Center Richmond, VA (DSCR)	Contractor	Government	Government	Government	Government	No Response from site yet
Defense Distribution Center Susquehanna, New Cumberland, PA	Contractor	Government	Government / Contractor*	Government**	Government**	Changes in red
Defense Supply Center Columbus, OH (DSCC)	Contractor	Government	Contractor	Government / Contractor	N/A	Changes in red
DLA Distribution Depot, San Joaquin, CA (DDJC)	Contractor	Contractor	Contractor	Contractor	Contractor	Confirmed

* There is some equipment that is handled by contractor support.

** Non-routine maintenance items are supported by contract (i.e. electrical substation equipment, water tower fire pump system, etc.).

(1) The Contractor needs to provide "Cybersecurity" and "Non-Routine/Ad-Hoc TO" Support for all OT Equipment at all of the above DLA locations/sites.

(2) The Contractor will need to provide the "Routine" maintenance support for the above identified locations/OT Equipment Groupings.

C6.1 DLA Headquarters Complex, Fort Belvoir, VA (HQC)

C6.1.1 Elevator Systems

C6.1.1.1 The primary task is to maintain existing lift equipment, such as elevators and vertical lifts, located throughout the Headquarters, Defense Logistics Agency, Fort Belvoir site in good, operating condition. Lift equipment, as used throughout this document, refers to elevators and vertical lifts installed in the McNamara Complex. The Contractor shall furnish all labor, transportation, equipment, materials, tools, supplies, supervision, and management required to perform the maintenance, repair, and component replacement as required to maintain elevator, stair lift, and chair/cart lift systems in accordance with the manufacturer's original specifications, American National Standards Institute (ANSI), Occupational Safety and Health Administration (OSHA).

C6.1.1.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.1.1.3 This contract will initially service 25 elevators and 1 vertical lift on the Site. With the ongoing effort of building consolidation and expansion, the Government reserves the right to

ADD to or DELETE systems from the contract anytime during the period of the contract as the need arises.

C6.1.2 Electrical & Lighting Systems (Building)

C6.1.2.1 The primary task is to maintain electrical and lighting systems located throughout the Headquarters, Defense Logistics Agency, Fort Belvoir site in good, operating condition. The Contractor shall furnish all labor, transportation, equipment, materials, tools, supplies, supervision, and management required to perform the maintenance, repair, and component replacement as required to maintain electrical and lighting systems in accordance with the manufacturer's original specifications.

C6.1.2.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.1.2.3 The maintenance and repair services are for the general electric systems including all HQC non-security systems, parking lots lights, electrical cables; electronic and communications rooms equipment and all electrical systems. Details for the Electrical and Lighting Systems (Building) Equipment will be included at the TO level.

C6.1.3 HVAC + BAS + Utility Metering Systems

C6.1.3.1 The primary task is to maintain existing mechanical and HVAC/BAS/UMS equipment/structures, located throughout the McNamara Headquarters Complex, Defense Logistics Agency, Fort Belvoir site in good, operating condition. The Contractor shall provide operation, maintenance, repair, and alteration services on a variety of Heating, Ventilation, Air Conditioning and Refrigeration (HVACR) units, BAS, and UMS and their components at the HQC.

C6.1.3.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.1.3.3 This work includes the maintenance, repair, and installation of all components, devices, equipment and associated systems, including but not limited to compressors, Air Handling Units,

blowers, motors, drive assemblies, fans, service valves, dampers, condensers, cooling coils, piping, pumps, purge units, control systems and wiring, duct work, burner assemblies, combustion chambers, thermostats and temperature controls, registers, condensate and drip pans and drains, grills, evaporators, air filters, dual duct VAV units, (approximately 1,100), Fan Powered VAV units (approximately 150), Terminal Reheat VAV units (approximately 100), heat/air conditioning units, government owned refrigerators (quantity approximately 125), Ice Making Machines (Quantity approximately 15), all Commander's kitchen appliances/equipment and all other items of equipment essential to the proper operation of HVACR equipment and systems in accordance with manufacturer's documentation. A list of Heating, Ventilation, and Air Conditioning equipment will be provided after award.

C6.1.3.4 The same requirement shall apply for Building 2462 McNamara POD 10 to include but not limited to Air Handling units, exhaust fans, cabinet and unit heaters, re-circulating fans, compressors, blowers, motors, drive assemblies, fans, service valves, dampers, condensers, cooling coils, piping, pumps, purge units, control systems and wiring, duct work, burner assemblies, combustion chambers, thermostats and temperature controls, registers, condensate and drip pans and drains, grills, evaporators, air filters, fan powered terminal units (approximately 450), Fan coil units, heat/air conditioning units, government owned refrigerators and all other items of equipment essential to the proper operation of HVACR equipment and systems in accordance with manufacturer's documentation, as well as BLDG 2463 Gate 1 Access Control, BLDG 2464 Gate 2 Access Control, BLDG 2465 Gate 3 Access Control, BLDG 2466 Recreational Building, BLDG 2467 Irrigation Well House, BLDG 2468 Child Development Center (CDC) 34,000 SF, BLDG 2469 Three Level Parking Garage building, BLDG 2480 Material Receiving and Screening Facility (MRSF) 15,000 SF, and BLDG 2487 Outfall Control Structure. Details for the HVAC/BAS/UMS Equipment will be provided at the TO level.

C6.1.4 Electrical Distribution (Site)

C6.1.4.1 The primary task is to maintain existing Electrical Distribution (Site) equipment/structure, located throughout DLA HQ, Fort Belvoir, VA in good, operating condition.

C6.1.4.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.1.4.3 The maintenance and repair services are for all Electrical Distribution (site equipment). Details for the Electrical Distribution (Site) Equipment will be provided at the TO level.

C6.1.5 Deliverable(s)

See TO PWS for specific information.

C6.2 Defense Supply Center Richmond, VA (DSCR)

C6.2.1 Elevator Systems

C6.2.1.1 The primary task is to provide elevator maintenance services at the Defense Supply Center Richmond located at 6090 Strathmore Rd. Richmond, Va. The Contractor shall furnish all labor, transportation, equipment, materials, tools, supplies, supervision, and management required to perform the maintenance, repair, and component replacement as required to maintain elevator, stair lift, and chair/cart lift systems in accordance with the manufacturer's original specifications, American National Standards Institute (ANSI), Occupational Safety and Health Administration (OSHA).

C6.2.1.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.2.1.3 The maintenance and repair services are for three (3) 1 car stop elevators, one (1) 4 car stop elevator and two (2) 4 wheelchair lifts, and one (1) stairlift. Details for the elevators included under this requirement will be provided at the TO level.

C6.2.2 Life Cycle Management Cyber Security and Non-Routine/Ad-Hoc Maintenance for the below Government Maintained Equipment:

C6.2.2.1 Electrical & Lighting Systems (Building)

C6.2.2.1.1 The Electrical & Lighting systems at Defense Supply Center Richmond are maintained by Government personnel. The primary contracted tasks for these systems are Cybersecurity and Non-Routine/Ad Hoc support.

C6.2.2.1.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.2.2.2 HVAC + BAS + Utility Metering Systems

C6.2.2.2.1 The HVAC/BAS/UMS lighting systems at Defense Supply Center Richmond are maintained by Government personnel. The primary contracted tasks for these systems are Cybersecurity and Non-Routine/Ad Hoc support.

C6.2.2.2.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.2.2.3 Electrical Distribution (Site)

C6.2.2.3.1 The Electrical Distribution (Site) Equipment at Defense Supply Center Richmond are maintained by Government personnel. The primary contracted tasks for these systems are Cybersecurity and Non-Routine/Ad Hoc support.

C6.2.2.3.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.2.3 Deliverable(s) (Richmond, DSCR)

See TO PWS for specific information.

C6.3 Defense Distribution Center Susquehanna, New Cumberland, PA (DDSP)

C6.3.1 Elevator Systems

C6.3.1.1 The primary task is for the Contractor to perform maintenance, inspection, testing, and repairs as required by the Manufacturers and ASME A17. Monthly maintenance shall be performed during the first fifteen (15) working days of each month. The contractor elevator technician shall report to the Government Representative before starting work. The Contractor shall implement all necessary work control procedures to ensure timely accomplishment of all maintenance and repair work requirements, as well as to permit tracking of all work in progress. The Contractor shall plan and schedule all work to ensure that material, labor, tools and equipment are available to complete maintenance or repair work within the specified time limits and in accordance with the quality standards. The status of any work shall be provided within one (1) hour of the inquiry during regular work hours.

C6.3.1.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.3.1.3 The maintenance and repair services are for 14 different elevator/vertical lifts consisting of 9 passenger elevators, 2 freight elevators, and 3 wheelchair lifts. Details for the Elevator and Vertical Lift Equipment will be provided at the TO level.

C6.3.2 HVAC + BAS + Utility Metering Systems (partial/Johnson Controls)

C6.3.2.1 The primary task is to maintain HVAC/BAS/UMS systems located throughout the Defense Distribution Susquehanna Pennsylvania site in good, operating condition. The Contractor shall furnish all labor, transportation, equipment, materials, tools, supplies, supervision, and management required to perform the maintenance, repair, and component replacement as required to maintain the systems in accordance with the manufacturer's original specifications.

C6.3.2.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.3.2.3 Details for the HVAC/BAS/UMS Equipment will be provided at the TO level.

C6.3.3 Life Cycle Management Cyber Security and Non-Routine/Ad-Hoc Maintenance for the below Gov't Maintained Equipment

C6.3.3.1 Electrical & Lighting Systems (Building)

C6.3.3.1.1 The Electrical & Lighting systems at Defense Distribution Susquehanna Pennsylvania are maintained by Government personnel. The primary contracted tasks for these systems are Cybersecurity and Non-Routine/Ad Hoc support.

C6.3.3.1.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall

be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.3.3.2 HVAC + BAS + Utility Metering Systems

C6.3.3.2.1 The HVAC + BAS + Utility Metering Systems at Defense Distribution Susquehanna Pennsylvania are maintained by Government and Contractor personnel. The primary contracted tasks for these systems are Cybersecurity and Non-Routine/Ad Hoc support.

C6.3.3.2.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.3.3.3 Electrical Distribution (Site)

C6.3.3.3.1 The Electrical Distribution (Site) Systems at Defense Distribution Susquehanna Pennsylvania are maintained by Government personnel. The primary contracted tasks for these systems are Cybersecurity and Non-Routine/Ad Hoc support.

C6.3.3.3.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.3.3.4 Water Systems (Potable, Sewer/Waste)

C6.3.3.4.1 The Water Systems (Potable, Sewer/Waste at Defense Distribution Susquehanna Pennsylvania are maintained by Government personnel. The primary contracted tasks for these systems are Cybersecurity and Non-Routine/Ad Hoc support.

C6.3.3.4.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance

with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C**6**.3.4 Deliverable(s) (Susquehanna, New Cumberland, PA)

See TO PWS for specific information.

C6.4 Defense Supply Center Columbus, OH (DSCC)

C6.4.1 Elevator Systems

C6.4.1.1 The primary task is to provide elevator maintenance services at the Defense Supply Center, Columbus, OH located at 3990 E. Broad St. Whitehall, OH. The Contractor shall furnish all labor, transportation, equipment, materials, tools, supplies, supervision, and management required to perform the maintenance, repair, and component replacement as required to maintain elevator, stair lift, and chair/cart lift systems in accordance with the manufacturer's original specifications, American National Standards Institute (ANSI), Occupational Safety and Health Administration (OSHA).

C6.4.1.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.4.1.3 The maintenance and repair services are for 19 elevators and 2 wheelchair lifts on the DSCC that will require these services. The elevators consist of both hydraulic and rope (mechanical) type elevators. The equipment varies in age and has multiple manufacturers. The wheelchair lifts and elevators require monthly inspections and periodic maintenance/ repairs as needed. Details for the elevators included under this requirement will be provided at the TO level.

C6.4.2 HVAC + BAS + Utility Metering Systems

C6.4.2.1 The primary task is to maintain existing mechanical and HVAC/BAS/UMC equipment/structure, located throughout Defense Supply Center, Columbus, OH (DSCC) in good, operating condition. The Contractor shall provide operation, maintenance, repair, and alteration services on a variety of Heating, Ventilation, Air Conditioning and Refrigeration (HVACR) units, BAS, and UMS and their components.

C6.4.2.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall

be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.4.2.3 The maintenance and repair services are to support HVAC systems throughout multiple buildings at DSCC. Examples of systems covered at DSCC are Trane Tracer, Tridium Vykon, Honeywell Comfort Point, etc. Details for the HVAC/BAS/UMS Equipment will be provided at the TO level.

C6.4.3 Electrical Distribution (Site)

C6.4.3.1 The primary task is to maintain electrical distribution equipment/structure, located throughout the Defense Supply Center, Columbus, OH in good, operating condition. The Contractor shall provide operation, maintenance, repair, and alteration services on a variety of electrical distribution components.

C6.4.3.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.4.3.3 Details for the Electrical Distribution (Site) Equipment will be provided at the TO level.

C6.4.4 Electrical & Lighting Systems (Building)

C6.4.4.1 The Electrical and Lighting Systems at Defense Supply Center, Columbus, OH are partially maintained by Government personnel. The Contractor shall provide operation, maintenance, repair, and alteration services as defined in the specific TO to maintain electrical and lighting systems in accordance with the manufacturer's original specifications.

C6.4.4.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.4.5 Deliverable(s) (Columbus, DSCC)

See TO PWS for specific information.

C6.5 DLA Distribution Depot, San Joaquin, CA (DDJC)

C6.5.1 Elevator Systems

C6.5.1.1 The primary task is to provide elevator maintenance services at DLA Distribution San Joaquin, California (DDJC), 25600 South Chrisman Road, Tracy, California. The Contractor shall furnish all labor, transportation, equipment, materials, tools, supplies, supervision, and management required to perform the maintenance, repair, and component replacement as required to maintain elevator, stair lift, and chair/cart lift systems in accordance with the manufacturer's original specifications, American National Standards Institute (ANSI), Occupational Safety and Health Administration (OSHA).

C6.5.1.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.5.1.3 The maintenance and repair services are for 2 passenger elevators and one freight elevator. Details for the elevators included under this requirement will be provided at the TO level.

C6.5.2 Electrical & Lighting Systems (Building)

C6.5.2.1 The primary task is to maintain Electrical and Lighting systems located throughout the DLA Distribution San Joaquin, CA site in good, operating condition. The Contractor shall furnish all labor, transportation, equipment, materials, tools, supplies, supervision, and management required to perform the maintenance, repair, and component replacement as required to maintain electrical and lighting systems in accordance with the manufacturer's original specifications.

C6.5.2.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.5.2.3 Details for the Electrical and Lighting Systems (Building) Equipment included under this requirement and will be provided at the TO level.

C6.5.3 HVAC + BAS + Utility Metering Systems

C6.5.3.1 The primary task is to maintain existing mechanical and HVAC/BAS/UMS equipment/structure, located throughout DLA Distribution San Joaquin, CA in good, operating condition. The Contractor shall provide operation, maintenance, repair, and alteration services on a variety of Heating, Ventilation, Air Conditioning and Refrigeration (HVACR) units, BAS, and UMS and their components.

C6.5.3.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.5.3.3 Details for the HVAC/BAS/UMS Equipment included under this requirement will be provided at the TO level.

C6.5.4 Electrical Distribution (Site)

C6.5.4.1 The primary task is to maintain existing Electrical Distribution (Site) equipment/structure, located throughout Defense Supply Center, San Joaquin, CA in good, operating condition.

C6.5.4.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.5.4.3 Details for the Electrical Distribution (Site) Equipment included under this requirement will be provided at the TO level.

C6.5.5 Water Systems (Potable, Sewer/Waste)

C6.5.5.1 The primary task is to maintain existing Water Systems (Potable and Wastewater) equipment/structure, located throughout DLA Distribution San Joaquin, CA in good, operating condition. The Contractor is required to be directly responsible for the water and wastewater treatment systems. As such the Contractor is required to maintain on site staffing to meet the

requirements below within 30 days of notice to proceed. This staff shall be employed on-site, on a full-time basis and shall not be time shared with another project without Contracting Officer written approval.

Potable water requirements for San Joaquin, CA:

California certification in accordance with Section 63770, Title 22, CCR.
Plant is designated as a T1 treatment & D2 distribution system.
The Chief operators need to be certified at the minimum T1 & D2 level.
The shift operator must be certified at the minimum T1 & D1 level.

Wastewater certification requirements for San Joaquin, CA:

California certification in accordance with Title 23, California Code of Regulations, Divisions 3, Chapter 26, Section 3670-3719.16
Plant is designated as a Grade II system.
The Chief operators need to be certified at the minimum Grade II.
The shift operator must be certified at the minimum Grade I.

C6.5.5.2 The contractor is responsible for ensuring this system remains in compliance with current Government cybersecurity standards throughout the lifecycle of the system. Software Maintenance (SM) includes patching of the firmware upgrades to the building level controllers and software patches if applicable. Contractor personnel supporting cybersecurity functions shall be appropriately certified according to DoD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification & Management Program. The contractor shall provide Cybersecurity in accordance with all current policies, procedures, and statutes in accordance with the requirements in Section 4 Security/Cybersecurity.

C6.5.5.3 The maintenance and repair services are for the Potable Water plant, a designated T1 treatment & D2 distribution system and the Wastewater plant, a designated Grade II system. Details for the Water Systems Equipment will be provided at the TO level.

C6.5.6 Deliverable(s) (San Joaquin, DDJC)

See TO PWS for specific information.

ATTACHMENT 1 DEFINITIONS & ACRONYMS

A1.1 Definitions

AFTER ACTION REVIEW/LESSONS LEARNED. An assessment conducted after a project or major activity that allows the Government and contractor to discover (learn) what happened and why.

ALTERATIONS. Alterations are new work that is not related to the maintenance and repair of the building. Alterations may include installation of equipment and related items, fabrication of items, relocation of equipment, materials, and devices, minor construction work requirements and related services. Alterations with a total cost including non-direct labor and materials below the discipline threshold shall be classified as minor work, and alterations with a total cost above the discipline threshold shall be classified as Non-Routine/Ad Hoc work requiring issuance of a Task Order (TO).

ASSESSMENT AND AUTHORIZATION (A&A), ASSESSMENT AND INCORPORATE (A&I), AND FRCS ASSESS ONLY RISK ASSESSMENT (FRCS AORA). A comprehensive evaluation of an organization's information system policies, security controls, policies around safeguards, and documented vulnerabilities.

AUTHORIZING OFFICIAL (AO). A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including missions, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

BEYOND ECONOMICAL REPAIR: An item is considered beyond economical repair where the repair would exceed 50% replacement cost of the item. If the equipment repair exceeds 50% of the replacement cost and the value of the equipment exceeds the discipline threshold, the equipment or item shall be replaced under a new Ad-Hoc IDIQ task order or means other than this contract as determined by the KO or COR. If the replacement value of the equipment is equal to or less than the discipline threshold, replacement shall be covered by the contractor under the firm fixed price portion of this contract. Extraordinary Repair Work, and End of Life Repair / Replacement are not included in this definition.

BUILDING AUTOMATION SYSTEM: The use of automation and control systems to monitor and control building wide systems.

CONCEPT OF OPERATIONS (CONOPS). A security focused description of an information system, its operational policies, classes of users, interactions between its system and its users, and the system's contributions to the operational mission. Specific CONOPS requirements are defined by the system ISSM.

CONTRACT ADMINISTRATOR. The official Government representative delegated authority by the Contracting Officer to administer a contract. This individual is normally a member of the appropriate Contracting/Procurement career field and advises on all technical contractual matters.

CONTRACTOR. A supplier or vendor awarded a contract to provide specific supplies or services to the Government. The term used in this contract refers to the prime.

CONTRACTING OFFICER (KO). A person with authority to enter into, administer, and/or terminate contracts, and make related determinations and findings on behalf of the Government. Note: The only individual who can legally bind the Government.

CONTRACTING OFFICER'S REPRESENTATIVE (COR). An employee of the U.S.

Government appointed by the KO to administer the contract. Such appointments shall be in writing and shall state the scope of authority and limitations. This individual has the authority to provide technical direction to the Contractor if that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have the authority to change the terms and conditions of the contract. This individual has responsibility for surveillance of the Contractor's performance against the contract requirements at the IDIQ level.

CYBERSECURITY. The collected set of technologies, processes, and procedures organizations use to protect their computing environments from damage and unauthorized data access perpetrated by cybercriminals or malicious insiders.

DELIVERABLE. Anything that can be physically delivered but may include non- manufactured things such as meeting minutes or reports.

DISCIPLINE THRESHOLD: The discipline threshold is the dollar value of a specific discipline, or BCS/UCS system, beyond which further repairs or replacements would not be included in the Firm Fixed Price portion of the contract. The threshold values of each discipline will be defined in the specific TOs.

DIRECT LABOR. Labor personnel performing the work identified in CLIN 0001, 0002, 0003, 0004, and 0005 Routine/Preventive Maintenance, Repair, Alterations, and Equipment Replacement, Firm Fixed Price (FFP) of the contract.

EFFLUENT: Liquid waste or sewage discharged into a river or the sea.

ELECTRICAL DISTRIBUTION SYSTEM: The part of the electric system after the transmission system that is dedicated to delivering electric energy to an end-user.

ELECTRICAL METER: A device the measures the total power consumer over a time interval.

ELEVATOR MONITORING SYSTEM. Monitoring system for Elevators and Vertical Lifts specifically at Defense Supply Center Columbus, OH (DSCC), Defense Supply Center Richmond, VA (DSCR), DLA Distribution Depot, San Joaquin, CA (DDJC), DLA Distribution Center Susquehanna, PA (DDSP), and DLA Headquarters Complex, Fort Belvoir, VA (HQC).

END OF LIFE REPAIR/REPLACEMENT: Covers equipment with a value in excess of the discipline threshold and the manufacture no longer provides support. Once the manufacture provides a statement to the contractor in writing that they no longer support the equipment, and the contractor submits notification to the KO and COR, the government will start the replacement process through an IDIQ Ad-Hoc task order or other means other than this contract as determined by the COR or KO. During the replacement process, the contractor shall continue to maintain and repair the equipment until replaced or through the point of Beyond Economical Repair. Equipment that is End of Life Repair and/or Replacement with a value equal to or less than the discipline threshold shall be covered under the Fixed Firm Price Portion of this contract. Beyond Economical Repair, and Extraordinary Repair Work, are not included in this definition**.**

EXTRAORDINARY REPAIR WORK: Includes repair and replacement work required due to accidents, acts of God, unlawful acts, or faulty or negligent operations by personnel other than the Contractor and its agents maintaining the system. Extraordinary repair work falling within the minor work threshold shall be covered by the contractor under the firm fixed price portion of this contract. Extraordinary repair work exceeding the scope of minor work may be accomplished by issuing a separate IDIQ Ad-Hoc task order or means other than this contract as determined by the KO or COR

FEDERAL ACQUISITION REGULATION. The principal set of rules established to govern the acquisition process of the Government purchasing goods and services.

FULLY BURDENED LABOR RATE: This rate encompasses all labor costs, including direct labor (wages/salaries), indirect labor, fringe benefits (payroll taxes, insurance, retirement, paid time off, etc.), and other applicable labor-related expenses (profit, etc.). Proposed fully burdened labor rates will be competitively evaluated against other offerors' rates during the government's price analysis.

GOVERNMENT-FURNISHED PROPERTY OR GOVERNMENT PROPERTY.

Property in the possession of, or directly acquired by, the Government and subsequently made available to the Contractor.

HEATING, VENTILATION, AIR CONDITIONING, AND REFRIGERATION (HVACR) SYSTEMS: The use of various technologies to control the temperature, humidity, and purify of air in an enclosed space.

INFORMATION SYSTEMS SECURITY MANAGER (ISSM). Individual responsible for the information assurance of a program, organization, system, or enclave.

IT INFRASTRUCTURE. The system of hardware, software, facilities, and service components that support the delivery of business systems and IT enabled processes.

KEY PERSONNEL. Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract by the Key Personnel listed in the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

MATERIAL OVERHEAD RATE: This rate covers indirect costs associated with acquiring, storing, and handling materials used in production, excluding the direct material purchase price. Profit is NOT allowed on Material. Offerors should propose a reasonable and efficient material overhead rate as the proposed material overhead rate will be competitively evaluated against other offerors' rates during the government's price analysis. Offerors will be required to submit 3 bids for all material purchases to ensure that the Government is receiving a competitive material price. The government seeks to ensure cost control and efficient material acquisition.

MINIMUM GUARANTEED: The Government guarantees to issue and the Contractor agrees to accept a minimum of $10,000.00 in task orders under this Indefinite Delivery Indefinite Quantity (IDIQ) contract during the ordering period, commencing [Start Date] and ending [End Date]. This minimum guarantee represents the Government's good faith commitment to utilize

this contract and does not obligate the Government to order items or services beyond its actual needs.

MINOR WORK. Minor work is defined as alterations and extraordinary repair work when the total cost of the required work, including non-direct labor, equipment, and materials, is less than the discipline threshold. Minor work is considered Routine/Preventive work covered under the firm-fixed price portion of the contract.

MONTHLY STATUS REPORT. To keep project status visible to senior management in the customer and delivery organization by providing an appropriate summary of project status on a regular monthly basis.

NETWORK. Information system(s) implemented with a collection of interconnected components.

NON-DIRECT LABOR. Subcontracted labor or contractor labor not already included under the Direct Labor category.

NON-ROUTINE / AD HOC REPAIRS. Maintenance, repair, alteration, and equipment replacement work requirements beyond the scope of the services performed under the Routine/Preventive Maintenance CLIN(s). This work is over the discipline threshold and requires a Task Order to be issues by the Contracting office for work to commence.

OTHER DIRECT COSTS. Non-labor and non-travel expenses incurred for the Government (i.e. facilities, shipments).

OPERATIONAL TECHNOLOGY (OT). A broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).

PHYSICAL SECURITY. Actions that prevent the loss or damage of Government property.

POTABLE WATER SYSTEM: A system for the provision of water to for human consumption.

PROJECT MANAGEMENT PLAN. A plan for executing a project and to meet specific objectives for the project. It should be used as a foundation for information and resource management planning and guidance.

PERFORMANCE WORK STATEMENT. Explains concisely what is to be accomplished in terms of results so that the Government can monitor and evaluate the progress and final result of the project effectively.

QUALITY ASSURANCE. The Government procedures to verify that services being performed by the Contractor are acceptable IAW with established standards and requirements of this contract.

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP). An organized written document specifying the Government surveillance methodology to be used for surveillance of Contractor performance.

QUALITY CONTROL. All necessary measures taken by the Contractor to assure that the quality of an end product or service shall meet contract requirements.

QUALITY CONTROL PLAN. The Contractor's standardized procedure/methodology for self-monitoring and documenting contract performance to ensure all contract requirements are met.

QUARTERLY MANAGEMENT REPORT. To keep project status visible to senior management in the customer and delivery organization by providing an appropriate summary of project status/management on a quarterly basis

RECOVERY TOOLS. Repairing, restoring, or diagnosing computer problems and systems.

REPAIR. Repair is the restoration of a piece of equipment, a system, or a facility to such condition that it may be effectively and reliably utilized for its designated purposes, and is a result of ordinary use, operation, normal wear and tear and the passage of time. Repairs may be overhaul, reprocessing, or replacement of constituent parts or materials that have deteriorated by action of the elements or usage and have not been corrected through maintenance, or replacement of the entire unit or system if beyond economical repair. All repair work less than the discipline threshold is considered routine work covered under the firm-fixed price portion of the contract. Beyond Economical Repair, Extraordinary Repair Work, End of Life Equipment Replacement and Non-Routine Repair are not included in this definition.

RISK ASSESSMENT (RA). The process of identifying risks to organizational operations, organizing assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.

ROUTINE/PREVENTIVE MAINTENANCE. The regularly scheduled and Routine/Preventive maintenance of equipment to keep Elevators and Vertical Lifts running in exceptional operating condition and prevent any costly unplanned downtime from unexpected equipment failure. This work is performed in accordance with the Routine/Preventive Maintenance Plan that outlines the contractor's approach testing, maintenance, repair, and schedule.

SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG). Implementation guide based on Department of Defense (DoD) policy and security controls that is geared to a specific product and version. Contains all requirements that have been flagged applicable for the product which have been selected on a DoD baseline.

SERVICE ORDER/CALL. Maintenance work which involves the repair or replacement of components which have failed or broken down and were discovered and requested by the Government.

SUBCONTRACTOR. One that enters into a contract with a prime Contractor. The Government does not have privity of contract with the Subcontractors.

SUBSTATION: A set of equipment reducing the high voltage of electrical power transmission to that suitable for supply to consumers.

SYSTEM. A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

TRANSFORMER: A device the transfers electric energy from one alternating-current circuit to one or more other circuits.

VERTICAL LIFT. A vertical platform lift (VPL) gives vertical access to people using scooters or wheelchairs. A residential VPL is commonly used to provide access between the ground level and a porch or deck and are considered a space-efficient solution in comparison to a ramp.

VIRTUAL LOCAL AREA NETWORK (VLAN). A broadcast domain that is partitioned and isolated within a network at the data link layer.

VIRTUAL MACHINE (VM). Software that allows a single host to run one or more guest operating systems.

WASTEWATER SYTEM: The structures, equipment, systems, and processes required to collect, carry away, and treat wastewater.

WIDE AREA WORKFLOW. A web-based application that allows Contractors to electronically submit invoices and receiving reports and the Government to inspect, accept, receive, and pay electronically.

WORKDAY. A day on which the government is routinely present, usually Monday through Friday, excluding federal holidays. A workday is distinguished from a calendar day, as within ten calendar days there may be a range of five to eight workdays. This will be defined in this PWS and at the T.O. level.

WORK WEEK. Monday through Friday, except for Federal holidays unless specified otherwise.

A1.2 Acronyms

AAR	After Action Review
A&A	Assessment and Authorization
A&I	Assessment and Incorporate
ACD	Accelerated Capabilities Division
ALP	Acceptable Level of Performance
ANSI	American National Standards Institute
AO	Authorizing Official
BAS	Building Automation System
BBP	Best Business Practice
BCS	Building Control Systems
CAC	Common Access Card
CCR	California Code of Regulations
CFR	Code of Federal Regulations
CLIN	Contract Line-Item Number

CNA	Capability Needs Analysis
CNSSI	Committee on National Security Systems Instruction
CoE	Center of Excellence
CONOPS	Concept of Operations
CONUS	Continental United States (excludes Alaska and Hawaii)
COR	Contracting Officer's Representative
DD254	Department of Defense Contract Security Classification Specification
DFARS	Defense Federal Acquisition Regulation Supplement
DoD	Department of Defense
DODD	DoD Directive
DSSR	Department of State Standardized Regulations
FAR	Federal Acquisition Regulation
FFP	Firm Fixed Price
FIPS	Federal Information Processing Standard
FTR	Federal Travel Regulations
FRCS	Facility Related Control System
FRCS AORA	FRCS Assess Only Risk Assessment
GFE	Government-Furnished Equipment
GFP	Government-Furnished Property
GFI	Government-Furnished Information
IA	Information Assurance
IAW	In Accordance With
ID	Identification
IDIQ	Indefinite Delivery/Indefinite Quantity
IEEE	Institute of Electrical and Electronics Engineers
IS	Information Systems
ISSM	Information System Security Manager
IT	Information Technology
JIIM	Joint, Interagency, Intergovernmental and Multi-national
JPAS	Joint Personnel Adjudication System
JTR	Joint Travel Regulations
KO	Contracting Officer
MSR	Monthly Status Report

NIE	Network Integration Evaluations
NIST	National Institute of Standard and Technology
NOSC	Network Operations Support Center
OCI	Organizational Conflict of Interest
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Costs
OT	Operational Technology
OPSEC	Operations Security
PIPO	Phase In/Phase Out
PM	Project Manager
PMP	Project Management Plan
POC	Point of Contact
POP	Period of Performance
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Program
QMR	Quarterly Management Report
RA	Risk Assessment
SOP	Standard Operating Procedures
STIG	Security Technical Implementation Guide
TOR	Task Order Request
TO	Task Order
VAL	Visit Authorization Letter
VLAN	Virtual Local Area Network
VM	Virtual Machine
WAWF	Wide Area Workflow
WBS	Work Breakdown Structure

ATTACHMENT 2 EQUIPMENT/INVENTORY IDIQ LIST

A sample TO and Equipment list will be provided for bidding purposes with the IDIQ. Detailed equipment lists will be provided with TO as available. Equipment lists will be verified by the contractor as part of the maintenance plan development.

ATTACHMENT 3 REFERENCE/CODES

References and Codes

In general, all maintenance shall be done in accordance with the manufacturer's recommendations, industry standards, and the Systems Operations and Maintenance Manuals (SOMMs). The Contractor shall follow applicable specifications listed below. The specifications listed below apply if those systems are being maintained, in other words a mechanical UFC does not apply for electrical equipment being maintained unless it is part of a mechanical system. All Federal, State, and Local jurisdictional laws and codes (including environmental, EPA) also apply even if not listed below. All contracts will use the current versions of these references (at time of contract award) unless otherwise approved. Additional references may be provided at the TO level. References include, but are not limited to:

Elevator Specific:

ASME A17.1, Safety Code for Elevators and Escalators

ASME A17.1, Handbook for Elevators, Escalators, and Moving Walks

ASME A17.2, Inspector's Manual for Elevators and Escalators

ASME A17.3, Existing Elevators and Escalators, Safety Code

ASME A17.4, Emergency Evacuation of Passengers from Elevators

ASME QEI-1, Standard for the Qualification of Elevator Inspectors

GSA, 501030S

ABA, Architectural Barriers Act

ITG 2013-01 (All references to the Navy shall be interpreted to mean the Pentagon. The approving authority for all areas within this document is the Pentagon Building Management Office)

OSHA 29 CFR (Code of Federal Regulations) 1926.552, Material Hoists, Personnel Hoists, and Elevators

UFC 3-490-06 Elevators, With Change 1

UFGS-14 21 23, Electric Traction Passenger Elevator

UFGS-14 24 23, Hydraulic Passenger Elevator

Electrical and Lighting Specific:

ASHRAE Standard 90.1, current version as of award of contract

ASHRAE Standard 55 Thermal Environment

Army Regulation AR 420-1, Rapid Action Revision 24 August 2012

DLAI 4170.11 Energy and Water Resource Management

EM 385-1 Safety and Health Requirements, U.S. Army Corps of Engineers

E.O. 14008 - Tackling the Climate Crisis at Home and Abroad

E.O. 14057 - Catalyzing Clean Energy Industries and Jobs Through Federal Sustainability

NFPA 31, Standard for the installation of Oil-Burning Equipment

NFPA 54, National Fuel Gas Code

NFPA 58, Liquefied Petroleum Gas Code

NFPA 70 National Electric Code

NFPA 70B, Standard for Electrical Equipment Maintenance

NFPA 70E, Standard for Electrical Safety in the Workplace

NFPA 90A, Standard for Installation of Air Conditioning and Ventilation Systems

NFPA 90B, Standard for the Installation of Warm Air Heating and Air-Conditioning Systems

NFPA 92, Standard for Smoke Control Systems

NFPA 96, Standard for Ventilation Control and Fire Protection of Commercial Cooking Operations

NFPA 101, Life Safety Code

NFPA 204, Standard for Smoke and Heat Venting

UFC 1-200-01 DoD Building Code with change 1

UFC 1-200-02 High Performance and Sustainable Building Requirements

UFC 1-201-01, Non-Permanent DoD Facilities in Support of Military Operations, with Change 3

UFC 1-201-02, Assessment of Existing Facilities for Use in Military Operations

UFC 3-301-01 Structural Engineering with change 4

UFC 3-401-01 Mechanical Engineering, With Change 1

UFC 3-410-01 Heating, Ventilating, and Air Conditioning Systems, With Change 8

UFC 3-430-07 Operations and Maintenance: Inspection and Certification of Boilers and Unfired Pressure Vessels, With Change 5

UFC 3-440-01 Renewable Energy

UFC 3-501-1 Electrical Engineering

UFC 3-520-01 Interior Electrical Systems with change 1

UFC 3-530-01 Interior and Exterior Lighting Systems and Controls with change 4

UFC 3-540-01 Emergency Generators 2014

UFC 3-560-01 Electrical Safety

UFC 3-575-01 Lightning and Static Electricity Protection Systems

UFC 3-600-01 Fire Protection Engineering with change 6

UFC 4-010-01, Minimum Antiterrorism Standards for Buildings, with Change 1

UFC 4-010-05 SCIF 2023

UFC 4-010-06, Cybersecurity of Facility Related Control Systems, with Change 1

UFC 4-440-01 Warehouses with change 1

UFC 4-610-01 Administrative Facilities with change 1

UFGS 01 91 00.15 Building Commissioning

UFGS 01 91 00.15 20 Total Building Commissioning Feb 2021

UFGS 25 08 11.00 20 facility related control systems

UFGS 25 10 10 Utility Monitoring and Control Systems

UFGS 48 14 00 Solar Photovoltaic Systems

TRANSFORMERS:

Specific instructions for work on transformers under this contract shall be defined in the Task Orders.

Transformers shall be maintained per manufacturer's specifications.

UFGS 26 12 19.10 Three Phase Liquid Filled Pad Mounted Transformers

UFGS 26 12 19.20 Single Phase Pad Mounted Transformers

UFGS 26 12 21 Single Phase Pad Mounted Transformers

UFGS 26 12 00.00 40 Medium Voltage Transformers

transformer sections of NFPA 70 National Electric Code which include Article 450

NFPA 70B, Standard for Electrical Equipment Maintenance

IEEE C57.12.80 terminology standard for power / distribution transformers

In addition to the specifications listed above, the Contractor shall follow current Industry Standards where applicable. All contracts will use the current versions of below references unless otherwise approved. References include, but are not limited to:

Manufacturer's Equipment Specific Maintenance Guidance

Manufacturer's Installation Guidance

International Property Maintenance Code (IPMC)

ASCE/SEI 7, Minimum Design Loads and Associated Criteria for Buildings and Other Structures.

1. Attachments in the TO may include, but are not limited to: existing infrastructure details
2. Approved Design drawings
3. Extracts of Design drawings
4. Letters (approvals, warranty, waivers)
5. Manufacturer guides or manuals
6. Cost Estimate(s)
7. System details
8. Security and network details
9. Diagrams, other pictures, or specifications

HVAC Specific:

ANSI/ASHRAE/ACCA Standard 180

ASHRAE Standard 62.1 Ventilation

ASHRAE Standard 180 HVAC inspection

Standard Practice for Inspection and Maintenance of Commercial Building HVAC Systems

UFC 3-410-02 Direct Digital Control for HVAC and Other Building Control Systems, With Change 2

UFGS 23 09 13 Instrumentation and Control Devices for HVAC

Electrical Lighting Distribution Specific:

ASHRAE Standard 90.1

UFC-3-501 Interior Electrical Systems with change 1

Wastewater/Potable Water Specific:

Wastewater Treatment Plant operations guidelines and standards for the state of Pennsylvania

EPA as of the date hereof, as contained in the Disinfectants and Disinfection Byproducts Rule (as promulgated in the Federal Register on December 16, 1998)

U.S. EPA for Public Water Systems and National Primary Water Treatment Regulations

The Federal Safe Potable Water Act of 1974, as amended last in 1996

Title 22, California Code of Regulations, Section 64400 et esq

UFC 3-230-01 Water Storage, Distribution, and Transmission

UFC 3-240-03, 03 October 2019, Operations & Maintenance Wastewater Treatment

AMERICAN WATER WORKSASSOCIATION, http://www.awwa.org

AWWA Manual M 27, \2\External Corrosion Control for Infrastructure Sustainability/2/

AWWA Manual M58, \2\Internal Corrosion Control of Water Distribution Systems/2/

AWWA Standard C651, Disinfecting Water Mains

AWWA Standard D100, Welded Carbon Steel Tanks for Water Storage

AWWA Standard D102, Coating Steel Water Storage Tanks

UFC 3-230-03, Water Treatment\1\

UFC 3-570-02A, Cathodic Protection 21

NSF Standard 61, Drinking Water System Components, latest edition 23

The Contractor and its personnel shall comply with all DoD and DLA regulatory guidance, including but not limited to:

System Identification Reference Documents:

A. Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems, December 15, 2022
B. Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
C. Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
D. Federal Information Security Modernization Act December 18, 2014, Department of War Instruction 5000.02, Operation of the Defense Acquisition System, January 23, 2020
E. Department of War Instruction 5200.39, Critical Program Information (CPI) Identification and Protection within the Research, Development, Test, and Evaluation (RDT&E) Incorporating Change 3, Effective October 1, 2020

System Compliance, Instructions and Guidelines Reference Documents:

a. 44 U.S.C. § 3542, December 2014

b. Department of War Instruction 8510.01, Risk Management Framework (RMF) for DoW Information Technology, December 2022
c. Department of War Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems & Networks, February 16, 2024
d. DoW Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle
e. Defense Acquisition Guidebook (DAG)
f. Department of War Directive DoDM 8140.03, Cyberspace Workforce Management, February 15, 2023
g. Department of War Instruction 8330.01, Interoperability of Information Technology (IT), Including National Security Systems (NSS), September 27, 2022

Personnel Requirements Reference Documents:

a. DoW Manual (DoDM) DoDM 8140.03 Cyberspace Workforce Qualification & Management Program, dated 15 Feb 2023

System Cybersecurity Implementation Reference Documents:

A. Department of War Instruction 8580.1, Cybersecurity in the Defense Acquisition System, July 9, 2004
B. National Institute of Standards and Technology Special Publication 800-82 Revision 3, Guide to Industrial Control Systems (ICS) Security, September 2023
C. Unified Facilities Guide Specifications (UFGS)-25 50 00.00 20 Cybersecurity of Facility-Related Control Systems
D. United Facilities Criteria (UFC) 4-010-06, Cybersecurity of Facilities-Related Control Systems
E. 44 U.S.C. § 3554, Executive Order (E.O.) 14028, Improving the Nation's Cybersecurity
F. OMB Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices.

FRCS, ICS, Facilities IOT Guidelines Reference Documents:

a. Defense Logistics Agency Risk Management Framework Standard Operating Procedures, December 2024
b. Office of the Assistant Secretary of Defense Facility Related Control Systems (FRCS) Master List Memo, October 2020

Physical Security Reference Documents:

a. DLAI 5200.01, Information Security Program
b. DLAI 5205.02, Operations Security (OPSEC) Program
c. DoDM 5200.01, Information Security Program
d. DoDI 5200.02, DoD Personnel Security Program
e. DoDM 5200.02, Procedures for the DoD Personnel Security Program

f. DoD 5200.8-R, Physical Security Program
g. DoD 5205.02-M, DoD Operations Security (OPSEC) Program Manual
h. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM)
i. DoD 5220.22-R, Industrial Security Regulation
j. DoD 2000.12, DoD Antiterrorism Program
k. DoDI O-2000.16, V. 1-2) DoD Antiterrorism (AT) Program Implementation
l. DoD O-2000.12-H, DoD Antiterrorism Handbook
m. DoD 5220.22-S, COMSEC Supplemental to Industrial Security Manual for Safeguarding Classified Information
n. DoDI 5240.6, Counterintelligence (CI) Awareness and Briefing Program
o. DoD 5100.76-M, Physical Security of Sensitive Conventional Arms, Ammunition and Explosives (AA&E)
p. DLAM 5200.08 (V. 1-2) DLA Physical Security Manual
q. DLA Crime and Loss Prevention SOP

ATTACHMENT 4 PERFORMANCE REQUIREMENT SUMMARY (PRS)

Performance Objective(s):

Performance Objective(s)	Task(s)	PWS Section(s)	Acceptable Quality Level (AQL)	Method of Surveillance	Deliver To:
Service Order/ Call Repairs	Repairs are made in a timely manner; Customers are informed of expected repair time. Response and repair is made within the specified time.	C2.5	Response to and repairs of service orders/calls are timely 98% of the time.	Periodic (Monthly)	COR
Perform Routine/Preventive Maintenance	All BCS/UCS systems are fully operational 99% of the time. Failed equipment is responded to within the proper response time 100% of the time, and no failed equipment or component down longer than permitted.	C2.6.1	Reports all of BCS/UCS systems fully operational 99% of the time.	Periodic (Monthly)	COR
Routine/Preventive Maintenance Plan	Accurate plan is delivered within 2 business days of initial submission and when significant changes occur	C3.4.3	98% of reports are timely and accurate	100% Inspection	COR
Submit Maintenance and Repair Reports	Accurate reports are delivered within two business days	C5.1	98% of all reports are timely and accurate	Periodic (Monthly)	COR

Submit 8140 Report	Accurate reports are delivered by 5th of each month	C3.1.1	98% of reports are timely and accurate	Periodic (Monthly)	COR
Staffing Plan	Accurate reports are delivered within two business days of significant changes	C3.2	98% of reports are timely and accurate	100% Inspection	COR
Required RMF Documentation	Accurate artifacts are delivered within 2 business days of Submission Dates in Table A4-2	C3.5.3	98% of artifacts are timely and accurate	100% Inspection	COR
Monthly Report	Accurate reports are delivered within two business days	C4.20, C4.9	98% of reports are timely and accurate	Periodic (Monthly)	COR
Quality Control Plan	Accurate reports are delivered within two business days	C5.1	98% of all reports are timely and accurate	Periodic (Monthly)	COR
Program Management Plan	Accurate reports are delivered within two business days	C7.2	98% of all reports are timely and accurate	Periodic (Monthly)	COR
Meeting Management	Meeting minutes provided within 2 business days	C2.42.4	98% of all meeting minutes submissions are timely and accurate	Periodic (Monthly)	COR

ATTACHMENT 5 COMMON ACCESS CARD LANGUAGE

Common Access Card (CAC) Procedures

Performance under this contract will require the contractor to obtain a CAC. When CACs are issued under this contract, the contractor shall complete and comply with the following steps to obtain, control, and turn-in Government-issued CACs, as well as establish procedures to control and account for contractor CACs at all times. This process is only for the issuance and accountability of CACs. Contractors may be required to provide additional forms and follow additional procedures for other forms of access and/or background/security checks depending on local site/installation requirements.

The Contractor has each contractor employee requiring a CAC complete and sign Sections I and II of the DD Form 1172-2. The instructions for completing the DD Form 1172-2 are located at http://www.cac.mil/docs/1172-2-Instructions.pdf.

For Section II, Block 22, the contractor employee signs and the DD Form 1172-2 is then forwarded by the contractor. This provides verification for the employee information. If the contractor is submitting a DD Form 1172-2 for him/herself (e.g., the owner) with no higher authority above them for verification, then the signature in Block 22 must be notarized to verify identity.

The Contractor forwards the DD Form(s) 1172-2 via hand-carry, secure mail, or encrypted email to (NOTE: The Contractor may forward these forms individually or as a group):

(1) The COR for the contract, if a COR was designated.
(2) The KO for the contract, if no COR was designated.

Each Contractor employee must verify his/her account information upon receipt of a username and password for the Identity, Credential, and Access Management (ICAM). A Government employee will directly provide this information to the Contractor, as well as the web link for ICAM.

Each Contractor employee will receive an email via ICAM when his/her account has been approved. The email will notify the employee to obtain a government-issued CAC from the nearest Real-Time Automated Personnel Identification System (RAPIDS) office. The email will also provide a link that identifies the locations of RAPIDS offices.

Each Contractor employee shall obtain his/her issued CAC from the RAPIDS office.

The Contractor, within one (1) business day of issuance, provides written notice via email to the COR (or the KO, if no COR was designated) for each Contractor CAC issued identifying the Contractor employee's name, the date of issuance, and the date of expiration of the CAC. This notification may be made individually for each Contractor employee or together for a group of Contractor employees.

The Contractor establishes procedures to control and account for Government-issued contractor CACs at all times, to include the following:

1. Ensure Contractor CACs issued for this contract are only used for the purpose of performing under this contract.
2. Ensure Contractor CACs are secured in a manner that precludes unauthorized use and that recognizes the CAC is the property of the U.S. Government.
3. Ensure Contractor employees do not abuse or place holes in their CACs.
4. Ensure Contractor employees do not display their CACs in public.

If a Contractor CAC is lost or stolen:

1. The Contractor employee shall immediately notify the Contractor that the Contractor CAC has been lost or stolen.
2. The Contractor shall immediately notify the COR (or the KO, if no COR was designated), detailing the circumstances regarding the lost or stolen contractor CAC, as follows:
    a. In person, followed within one (1) business day by a written notice via email, or
    b. In writing, via email, or
    c. By telephone, followed within one (1) business day by a written notice via email
3. The Contractor shall report the lost or stolen CAC card to the local DLA Police/host installation police, who will provide the Contractor a police report. If there is no local DLA Police/host installation police, or no police report is provided, the Contractor shall provide information to the COR/KO, as applicable, detailing the circumstances of how the CAC was lost or stolen. The COR/KO will provide a memorandum for the contractor employee to support issuance of new CAC.
4. The Contractor has the Contractor employee bring the report/memorandum to the nearest RAPIDS office. If the CAC can be reissued within 24 hours, bring the report/memorandum to the nearest CAC office for reissue. If the CAC cannot be reissued in 24 hours, follow the steps for a new CAC, beginning at Step 1.

If the expiration date for a Contractor CAC is prior to completion of the contract and the Contractor employee is to continue working under the contract and still requires a CAC, the Contractor:

1. Notifies the COR as follows:
    (a) In person, followed within one (1) business day by a written notice via email, or
    (b) In writing, via email, or
    (c) By telephone, followed within one (1) business day by a written notice via email
2. No less than two (2) weeks prior to the current CAC's expiration date, completes and complies with the steps above beginning with Step 2 for issuance of a new contractor CAC for the employee.
3. Brings the expiring CAC to the RAPIDS office for turn-in and receives new CAC.
4. Notifies the COR once a new CAC has been issued.

The Contractor/Contractor employee turns in any found CACs immediately, via hand carry, to the nearest Federal law enforcement office.

The Contractor immediately collects all Contractor CAC(s) from the Contractor employee(s) at:

Contract completion or termination

Termination/reassignment of an employee (this includes any reason the employee is no longer working for the contractor under the contract or otherwise no longer requires a CAC)

The Contractor:

For contract completion or termination – within one (1) business day after collecting the contractor CAC(s), arranges for turn-in via one of the below methods:

If the COR/KO is co-located or near enough that in-person transfer of CACs can be arranged, the contractor:

Arranges to meet the COR (or the KO, if no COR was designated) to turn-in the collected contractor CAC(s).

Hand-carries all collected contractor CACs for turn-in to meet the COR (or the KO, if no COR was designated).

Completes and signs the Government-Issued Contractor CAC Turn-In Receipt with the COR (or the KO, if no COR was designated). The Contractor is provided a copy of the receipt.

If in-person transfer of CAC cannot be arranged, the contractor:

Sends, via certified mail, the CACs to the COR/KO. The Contractor includes in the package the Government-Issued Contractor CAC Turn-In Receipt, with signed acknowledgement of contractor turn-in.

Notifies COR/KO that CACs have been sent via certified mail.

Receives a completed copy of the receipt from the COR/KO once the COR/KO has received the CACs.

For termination/reassignment of an employee:

Immediately notifies the COR (or the KO, if no COR was designated) that the employee is no longer working for the contractor under the contract or otherwise no longer requires a CAC, as follows:

In person, followed within one (1) business day by a written notice via email,

In writing, via email, or

By telephone, followed within one (1) business day by a written notice via email

Follows the turn-in procedures above for contract completion or termination, as applicable.

Contractor Reporting Requirements:

The Contractor is required to submit, on a monthly basis, to the COR (or the KO, if no COR was designated) a report of all employees working on the contract who have been issued CAC cards and a verification of whether each listed employee still requires a CAC. The report must note where changes have occurred (additions or deletions) since the previous month. Contractor employees who already have a CAC related to another DLA or DoD contract must be included in the Monthly Report. Contractor shall note the issuing organization and the CAC expiration date. Contractor is still responsible for notifying the COR/KO when the individual is no longer working under the subject contract.

The above procedures have been established as a DLA security measure. Contractors are advised that failure to comply with any of the above requirements will be considered a violation of the terms and conditions of the contract and the KO may take action to remedy such violations. Specifically, failure to safeguard, follow these procedures, including reporting requirements, or turn-in CACs within the established timeframes, may result in the following actions, which are in addition to other actions the KO may take under governing law and regulation and the terms and conditions of the contract:

Immediate work stoppage (issuance of a stop service order), not to be lifted until resolution of CAC issue.

Disapproval of invoices and delay of payment.

Withholding of final payment (in accordance with FAR 52.204-9).

Documentation of CAC Non-Compliance in the Contractor Performance Assessment Reporting System (CPARS).

ATTACHMENT 6 INSPECTION SHEET

DLA Contract Number	Task order	Receive date
SP4705-F-xxxxx		

DLA

HQC Installation Management
Final Inspection Form

This quality assurance surveillance plan (QASP) is pursuant to the requirements listed in the performance work statement (PWS). This plan sets forth the procedures and guidelines that will be used in ensuring the required **performance standards or services levels are achieved by the contractor.**

Location: (Building or Pod, Floor, Room #) _____

Task/Job:

☐ Satisfactory (date required)

☐ Unsatisfactory (Reason and date required)

Inspection date: _____

Comments: (required with "Unsatisfactory" inspection):
Use back of this sheet if necessary.

☐ **Re-inspection**

☐ Satisfactory (Date required)

☐ Unsatisfactory (Date required)

Inspection date: _____

Comments: (Required with "Unsatisfactory" re-inspection)
Use back of this sheet if necessary.

COR/Inspector Name: _____ Contractor Name: _____

COR/Inspector Signature: _____ Contractor Signature: _____

COR/Inspector signature (ALT) : _____

ATTACHMENT 7 INVOICING AND PAYMENT SCHEDULE

Payment of invoices will be accomplished by payment through the Defense Finance and Accounting Service (DFAS). Invoices will be submitted to the Wide Area Workflow (WAWF) system in accordance with DFARS 252.232-7003 Electronic Submission of Payment Requests and Receiving Reports and DFARS 252.232-7006 Wide Area Workflow Payment Instructions no later than 7 workdays at the end of each month.

1. The invoice shall be submitted no more than once a month. The invoice should include the specific performance standards performed and accepted and associated performance payments being invoiced for the month. Invoices are to be sent directly to the COR electronically at the address included in this PWS. Within seven days of the receipt of the invoice, the COR/ will review for accuracy and payment will be certified in the WAWF system by the COR. The requirements of a proper invoice are subject to FAR 52.232-25 - Prompt Payment. The vendor may check on the status of their invoice(s) by registering for My Invoice at https://wawf.eb.mil or contacting DLA at (800) 756-4571.

2. The following correct information constitutes a proper invoice per the Prompt Payment Act standards, and/or is required documentation for payment requests submitted electronically into the Wide Area Work Flow (WAWF) System - Hard copy invoices cannot be accepted.

3. Name and Address of Contractor/Vendor

4. Invoice date

5. Contract number (including the order/call number where applicable), or other authorization for delivery of goods or services. Note: DO NOT USE THE BID OR SOLICITATION NUMBER.

6. Invoice number, account number, and/or any other identifying number agreed to by contract.

7. Shipment Number, including the date (where applicable). Same as Block 2 of the DD Form 250. (See "Shipment Number Construction and Usage", page 13 for format).

8. Description: line-item number, National Stock Number, Manufacture's Part Number, unit of measure, quantity shipped, unit price, and extended amount, where applicable.

9. Shipping and payment terms (unless mutually agreed that this information is only required in the contract); including terms of any discount for prompt payment offered.

10. Electronic Funds Transfer (EFT) banking information, unless agency procedures provide otherwise, or except in situations where the EFT requirement is waived under 31 CFR 208.4.

11. Point of Contact (POC) name (where practicable), title and telephone number of person to notify in the event that the invoice is defective.

12. Other substantiating documentation or information required.

13. The contractor's failure to include the necessary information will result in invoices being rejected.

14. Back up documentation (such as timesheets, receiving reports etc.) can be included and attached to the invoice in WAWF. Attachments created in any Microsoft Office product are attachable to the invoice in WAWF. Maximum size limit of each attachment is 2 Megabytes (MB). Total size limit for all files is 5MB.

15. After clicking the "submit" button, a Notice of Successful/Unsuccessful Submission will appear. This screen contains a "Send More E-Mail Notifications" button. Click on this button and add the email addresses for the Program Office and others as desired. Notification shall be provided for each invoice submitted.

16. WAWF Tools and Help

17. The vendor may have their CAGE code activated (required only first time) in WAWF by calling 866-618-5988. Once activated, the vendor should self-register at the web site https://wawf.eb.mil.

18. Vendor training is available at: http://www.wawftraining.com. Additional support can be obtained by calling the DISA Ogden Help Desk at 1-866-618-5988 or e-mailing to cscassig@ogden.disa.mil.

19.WAWF Vendor "Quick Reference" Guides are located at https://acquisition.navy.mil/rda/home/acquisition_one_source/ebusiness/don_ebusiness_solutions/wawf_overviewvendor_information.

ATTACHMENT 8 CONTRACTOR PERSONNEL SECURITY

Work to be performed under this contract or task order may, in full or in part, be performed at the Defense Logistics Agency (DLA) field activity office(s), or other Federally-controlled facilities. At the time of contract T.O. award, clearances may be required at the T.O. site specific level.

Tiered Investigation Standards

Tiered Investigation Standards					
Position	Low-Risk	Moderate Risk		High Risk	
		Confidential	Secret	Top Secret	SCI
Position Sensitivity	Non-Sensitive	Non-Critical Sensitive		Critical Sensitive	Special Sensitive
Investigation	Tier 1/NACI	Tier 3/NACLC/ANACI		Tier 5/SSBI	
Formerly Known As	IT-III or IT-3	IT-II or IT-2		IT-I or IT-1	

As outlined in DoDM5200.02, the Investigative Requirements and Civilian Positions are as follows:

Special-sensitive and Critical-sensitive. Civilian personnel in special-sensitive and critical-sensitive positions require a favorably adjudicated SSBI or its equivalent.

INVESTIGATIVE REQUIREMENTS. DoDM 5200.02, April 3, 2017, Change 1, October 29, 2020, a. A non-U.S. citizen, including immigrant alien, may be issued an LAA (Limited Access Authorization) to systems and information under direct government supervision) investigative requirements of that country. b. A favorably completed and adjudicated SSBI (within the immediately preceding 5 years) is required before granting an LAA. If the SSBI cannot provide full investigative coverage, a polygraph examination (if there are no applicable host country prohibitions) to resolve the remaining personnel security issues will be favorably completed in accordance with DoDD 5210.48 before granting access.
If geographical, political, or medical situations prevent the full completion of the SSBI or prevent the polygraph examination to supplement a less than full SSBI, an LAA may be granted only with approval of the DDI(I&S).

If an LAA is withdrawn and the person subsequently is again considered for a new LAA, an SSBI and polygraph examination may be required. The scope of the SSBI will cover the period from the previous investigation or 10 years, whichever is shorter.

A PR will be conducted on every person with an LAA 5 years from the closing date of the previous SSBI or SSBI-PR, as appropriate.
For both OT and IT system support and roles must Identify the role with the required IT 1,2,3 designation and the system/mission sensitivity Activities or roles are Identified in DoDM 5200.02 4.1.

Not all systems have the same criticality, moderate risk duties on a critical system are not the same as moderate duties on a non-critical system. The Impact to information and availability are different.

OCONUS Investigation Standards

The following OCONUS countries require the investigation standards below for contractors:

Germany:
Local National Screening Program (LNSP) database, instructions for processing and access are all on the home page https://lnsp.ext.eur.army.mil/. Access must be requested via the Garrison. This is a generalized breakdown of the process for Germany.

* AR 604-1B
* Führungszeugnis (German Police Good Conduct Certificate (PGCC))
* Ausweis (Photo ID) front & back
* Individual must have lived in Germany for a minimum of 12 months leading up to the check.
* For non-German citizens from the EU, registration from the local German Rauthaus is required as proof of residents.

Italy:
Italian Air Force checks which include Interpol/Caribinieri and arrest checks. (Initial and 3 year (childcare) or 5 years (non-childcare). Additionally, prior to employment the local national provides a "Certificato Penale" which is like a local police check.

Italy/Spain/Greece/Poland/Romania do NOT issue CACs for LN's CACs are authorized for LN/HN in AFRICOM theater (CLDJ/Bahrain/Isa) after completion of the base vetting requirements.

Sensitive Information Access

Sensitive information access positions are designated based on access to government networks and IT systems and may exceed classified access requirements for this contract. Note that sensitive information access does not imply or convey access to classified information or DOW systems access where sensitive information is stored.

For sensitive information access positions, the required investigation shall be completed, or interim access granted for individuals assigned to sensitive duties. The provisions outlined above apply to the prime contractor and any subcontractors the prime contractor may employ during the course of the contract. In lieu of the correct investigations being completed when contract employees start, a waiver interim clearance may be submitted if no issues exist within the National Background Investigation Services (NBIS) Questionnaire (SF 85) for Non-Sensitive Positions or Questionnaire (SF 86) for National Security Positions. The contractor shall have the NBIS form completed, with any other requirements (fingerprints taken and, if required, an OF306), and reviewed by DLA Intelligence before officially hiring any contractor employee into

sensitive information access positions Declarations for investigation to non-sensitive, sensitive CUI and system access, critical information and related systems access need to be properly Identified. All foreign nationals must be cleared by the correct type of investigation depending on information access and system access. Reference DLAI 5210.01 Effective: February 4, 2021, DoDM 5200.02.

Please note that physical access to DoW installations is not the same as access to sensitive information or DoW sensitive systems access and is covered under DOD M 5200.08 Volume 3.

Access to Classified Information

Most work to be performed under this requirement is unclassified; however, a security clearance will be required for some TOs up to Secret. Contractor must have available staff with a favorably adjudicated Tier 5 investigation prior to the contract award. Contractors shall not be required to store, handle, or process classified information at their facility. Contractors with a safeguarding requirement will need to be approved for safeguarding at the same or higher level of classification listed in Block 1b of DD Form 254.

Contractors are required to comply with 32 CFR Part 117 National Industrial Security Program Operating Manual (NISPOM) in the handling, protection, and safeguarding of classified information in their possession. Security requirements outside the scope of the NISPOM if required, will be defined in the accompanying DD Form 254.

The personnel security investigations conducted for access to classified information will be started by the contractor company Facility Security Officer (FSO).

Citizenship

Each Contractor employee shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence, or who presents evidence from the Immigration and Naturalization Service that employment will not affect his immigration status.

Identification Badges

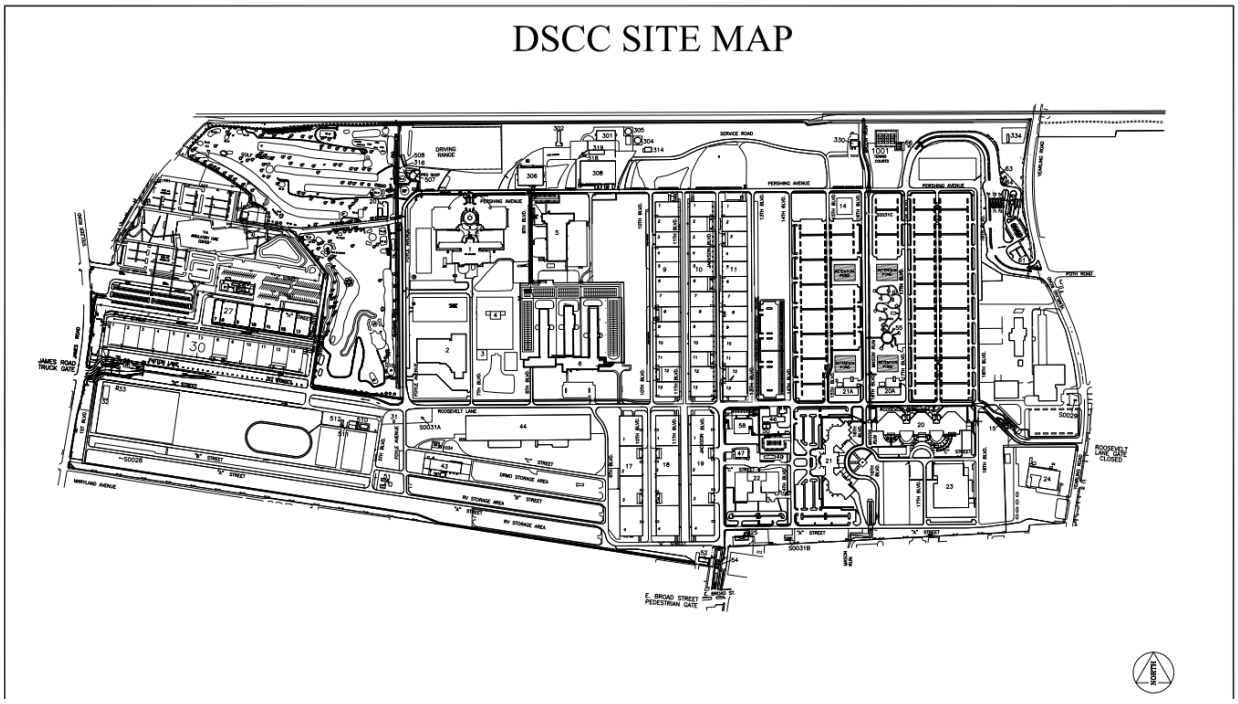
Contractor employees (including those of subcontracts) requiring physical access to the contractual place of performance and/or access to the DLA network/system for successful contract performance will be required to obtain a Common Access Card (CAC) prior to starting work. Lost or stolen CACs must be promptly reported by the Contractor to the KO or their authorized representative and to the appropriate Government security personnel. The Government will retain sole decisional authority on issuance of a replacement CAC.

ATTACHMENT 9 MAPS

Richmond, VA

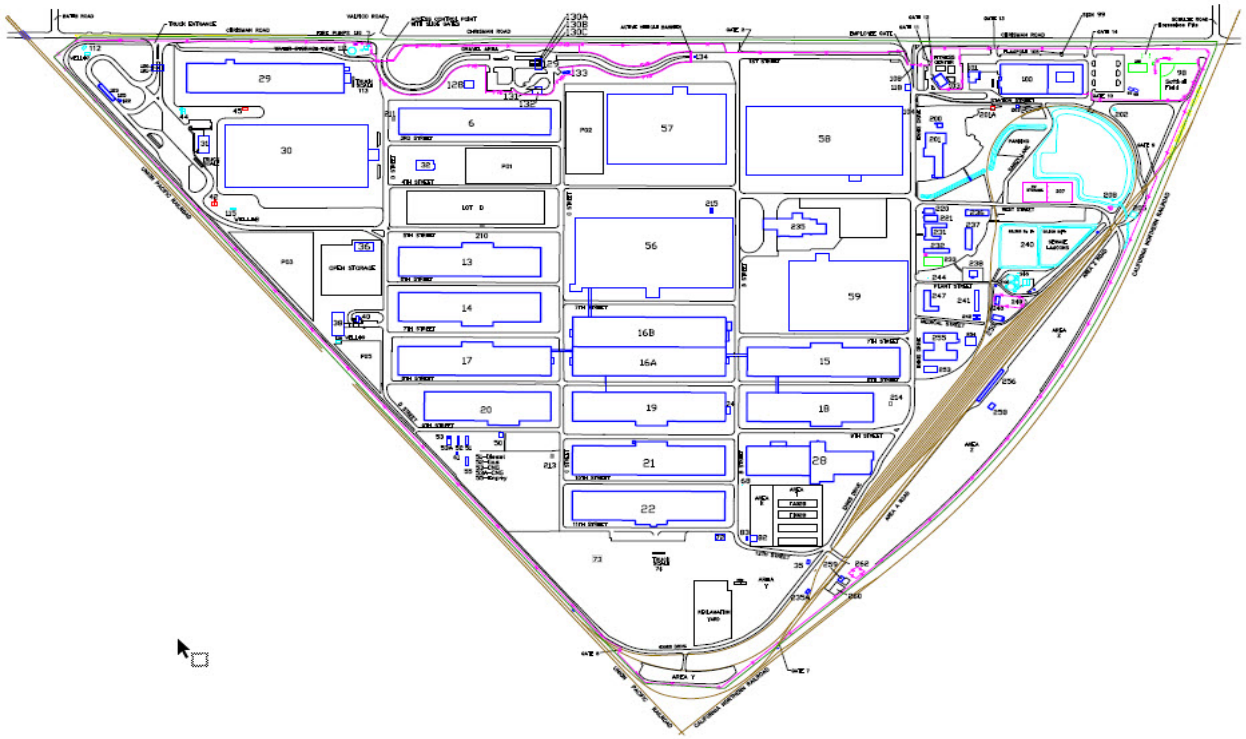
Return to Table of Contents

Columbus, OH



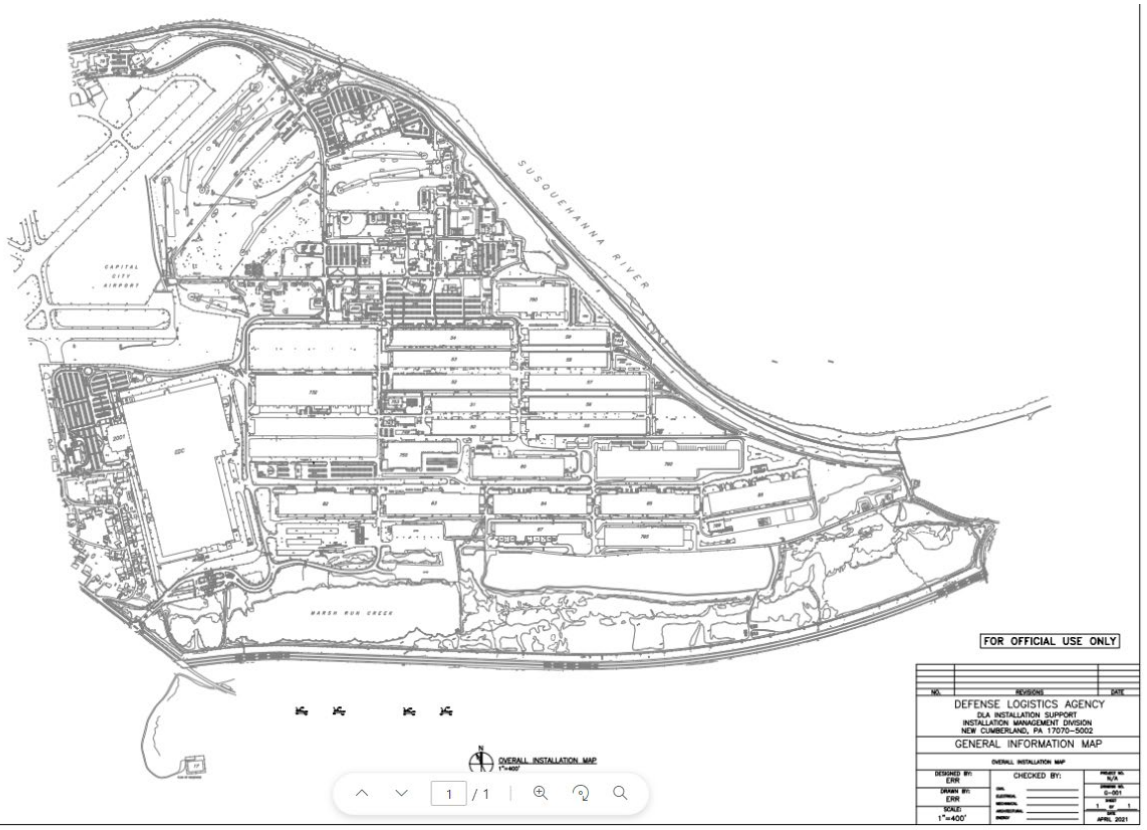
Return to Table of Contents

San Joaquin, CA



Fort Belvoir, VA:

New Cumberland, PA Map:


SUSQUEHANNA RIVER
CAPITAL CITY AIRPORT
MARSH RUN CREEK
OVERALL INSTALLATION MAP
1"=400'
1 / 1
FOR OFFICIAL USE ONLY
NO. REVISIONS DATE
DEFENSE LOGISTICS AGENCY
DLA INSTALLATION SUPPORT
INSTALLATION MANAGEMENT DIVISION
NEW CUMBERLAND, PA 17070-5002
GENERAL INFORMATION MAP
OVERALL INSTALLATION MAP
DESIGNED BY: ERR
DRAWN BY: ERR
SCALE: 1"=400'
CHECKED BY:
PROJECT NO. N/A
DRAWING NO. G-001
SHEET 1 OF 1
APRIL 2021