6MI0310
Agency Specific Requirements
Federal Protective Service

The Agency Specific Requirements (ASRs) do not reduce the minimum requirements contained within the Lease. These ASRs provides specific agency requirements, which may be complementary, more specific, or more stringent than those of the Lease minimum requirements.

Furniture, Fixtures, and Equipment (FF&E)

DHS/FPS – Grand Rapids Area Command (AC)

Grand Rapids, MI

1.0 Purpose

The purpose of this Statement of Work (SOW) is to procure, deliver, and install all Furniture, Fixtures, and Equipment (FF&E) required that best supports the DHS/Federal Protective Service (FPS) Grand Rapids, MI Area Command (AC) in accordance with the approved Program of Requirements (POR). The Contractor shall provide all labor, materials, equipment, supervision, project management, and quality control necessary to furnish and install FF&E that meets DHS, FPS, and GSA standards.

2.0 Scope

The Contractor shall provide a complete FF&E solution for all administrative, operational, and mission-support spaces identified in the POR. This includes, but is not limited to:

- Personnel workstations (36 SF cubicles)
- Supervisory workstation enhancements
- Evidence, weapons, and secure storage solutions
- Bulk and Tactical equipment storage
- K-9 storage and explosive bunker storage
- Huddle and Conference room furniture capable of technology integration
- Break area furnishings and millwork
- IT LAN/IDF room equipment racks and accessories
- Detainee processing fixtures (handcuffing bench(s)
- General support furnishings and accessories

All FF&E shall be new, commercial-grade, compliant with federal standards, and suitable for a law-enforcement operational environment.

3.0 Applicable Documents

The Contractor shall comply with the following:

- DHS/FPS Program of Requirements (POR) –Grand Rapids, MI AC
- GSA PBS P100 Facilities Standards
- GSA Federal Management Regulation (FMR)
- GSA Schedule 71/72 (if applicable)

- DHS Sustainability and Environmental Requirements
- ADA Accessibility Guidelines
- NFPA and OSHA requirements for applicable equipment

4.0 Requirements

4.1 General Requirements

The Contractor shall:

- Provide FF&E that meets or exceeds DHS/FPS durability, security, and ergonomic standards.
- Coordinate all measurements, field verifications, and installation logistics with GSA and FPS.
- Provide finish selections, product data sheets, and shop drawings for Government approval.
- Deliver, assemble, and install all FF&E in accordance with manufacturer specifications.
- Remove all packing materials and restore the site to clean condition.
- Provide warranties, maintenance instructions, and as-built documentation.

5.0 Room-Specific FF&E Requirements

5.1 Personnel Workstations (36 SF Cubicles)

Provide complete workstation packages for five (5) positions, including:

- Modular cubicle system workstations (36 SF footprint)
- Height-adjustable (electronic)
- Ergonomic task chair (adjustable chairs offering girth 25”+, 300lbs + weight capacity, drop away arms, offer a back support in height of 24”+
- Locking mobile pedestal
- Overhead storage bin
- Dual Monitor arms
- Task lighting
- Integrated power/data raceway
- Cable management

Supervisor workstation shall include two guest chairs and one lateral file cabinet.

5.2 Storage & Mission Support Spaces

5.2.1 Bulk Storage – 120 SF

- Heavy-duty shelving (14-gauge steel)

- Lockable storage cabinets
- Equipment bins/totes
- Pallet-capable floor rack

5.2.2 Ammo/Weapons Storage – 100 SF

- Stackable GSA-approved class 5/6 weapons lockers
- GSA-approved class Ammunition storage cabinets
- Reinforced shelving
- Wall-mounted gear racks
- Class 5 Weapons Container

5.2.3 Secure File/Evidence Combo – 120 SF

- GSA security containers
- Evidence lockers
- Shelving for boxed evidence
- Lockable file cabinets

5.2.4 Tactical Equipment Storage – 160 SF

- 36”-48” TA-50 Tactical Gear Locker
- Lockable cage storage
- PPE storage solution
- Wall-mounted tactical panels

5.2.5 Evidence Room – 120 SF

- Evidence lockers
- High-density
- Refrigerated evidence locker (if required)

Evidence Processing Hutch with Cubbies

- Full-height or counter-height hutch as shown in plan.
- Individual cubbies sized for envelopes, documents, and small evidence packets.
- Lockable doors on lower storage (if required by agency SOP).
- Durable laminate or powder-coated steel construction.
- **Evidence Shelving (if required by program)**

- Heavy-duty steel shelving, adjustable.
- Minimum 200–300 lb. shelf capacity.
- Anti-tip hardware.
- Law Enforcement Task Chair
    - Heavy duty, 24/7 rated chair.
    - Vinyl or cleanable upholstery.
    - Adjustable height and back support.
- (1) Workstation
- Desk / Worktable
    - Standard 30" depth, 60–72" width (or as shown in plan).
    - Durable laminate or steel top.
    - Cable management grommets.
- Task Chair
    - Same spec as Evidence Room or agency approved equivalent.

5.2.6 Secure File Room – 120 SF

- GSA-approved file cabinets
- Lockable shelving
- Document storage racks
- Evidence Room Desk

5.2.7 K-9 Storage – 75 SF

- Ventilated storage cabinets
- K-9 equipment racks
- Odor-resistant bins
- Tiedown points (as/if required)

5.2.8 Explosive Bunker – 25 SF

- Blast-rated storage container
- Fire-resistant cabinet
- Safety signage

5.2.9 Canine Explosive Bunker Storage – 120 SF

- Explosive-rated storage units
- Ventilated cabinets

Included FF&E

- Blast rated storage container
    - Steel, vented, lockable Type-2 or Type-3 explosive storage cabinets (as required by agency SOP).
    - Shelving sized for training aids, inert materials, or operational explosives.
    - Heavy-Duty Shelving
    - Non-sparking, corrosion-resistant shelving for ancillary equipment.
    - Small, non-sparking surface for inspection or packaging tasks.
- PPE Storage Cabinet
    - For gloves, eye protection, and safety equipment.
- Signage & Safety Fixtures
- "Explosives Storage" placards.
- Fire-rated waste receptacle.

Functional Intent

Provide secure, controlled, and compliant storage for explosive materials or training aids, with FF&E that supports safe handling and inventory control.

K9 Room with K9 Storage – 75 SF

Provide and install FF&E to support secure housing, care, and operational readiness of a law-enforcement K9 unit.

- Included FF&E
- K9 Kennel/Crate
- Heavy-duty, law-enforcement grade.
- Chew-resistant, ventilated, and sized for the assigned K9.
- K9 Gear Storage Cabinet
- Lockable cabinet for leashes, harnesses, bite sleeves, training aids, and PPE.
- Adjustable shelving.
- Wall-Mounted Hooks / Racks
- For leads, collars, and frequently accessed gear.
- Durable Work Surface
- Small counter or table for equipment prep, documentation, or medical checks.
- Floor-Mounted Mat or Bedding
- Washable, antimicrobial K9 rest mat.
- Waste & Cleaning Supplies Station
- Covered waste bin.
- Storage for disinfectants, wipes, and cleaning tools.

Functional Intent

Support daily K9 deployment, storage of operational gear, and safe temporary containment of the animal.

5.3 Shared & Common Spaces

5.3.1 Break Area – 72 SF

- Small table and chairs for 2-4 staff
- Refrigerator with a filtered water line for ice and water distribution
- Microwave shelf/cabinet
- Trash and recycling bins
- Casework & Storage
    - Base cabinets for food storage, cleaning supplies, and small appliances
    - Wall cabinets for cups, plates, and dry goods
    - Countertop (solid surface or laminate) with minimum 6 linear feet of workspace
    - Trash and recycling bins (fire-rated if required by facility policy)

5.3. IT LAN Closet (IDF) – 100 SF

- Server racks
- Wall-mounted equipment shelves
- Cable management hardware
- Anti-static mat
- A. IT Workbench / Technician Table
    - 30"–36" deep, 48"–72" wide
    - ESD-safe surface preferred
    - Under-table storage for tools and spare components

  B. IT Task Chair
    - Adjustable, wipe-clean upholstery
    - 24/7-rated if used for monitoring

  C. Storage Cabinets
- Lockable base cabinet for spare cables, peripherals, and tools
- Wall cabinet for consumables and small equipment
- Shelving for boxed equipment, routers, radios, etc.

6.0 Deliverables

The Contractor shall provide:

1. Project Management Plan
2. Product Submittals & Finish Boards
3. Installation Schedule
4. As-Built FF&E Layouts
5. Warranty Documentation
6. O&M Manuals

7.0 Period of Performance

The period of performance shall be established at award and shall include:

- Procurement lead time
- Delivery
- Installation
- Punch-list resolution

8.0 Government Furnished Information (GFI)

The Government will provide:

- POR
- Floor plans
- Access coordination
- Security requirements

9.0 Security Requirements

Contractor personnel shall comply with:

- FPS and GSA access control procedures
- Background check requirements (if applicable)
- Escort requirements for uncleared personnel

10.0 Inspection & Acceptance

The Government will inspect all FF&E for:

- Compliance with specifications
- Proper installation
- Damage or defects
- Operational readiness

Final acceptance occurs after punch list completion.

11.0 Warranty

All FF&E shall include manufacturer warranties. Contractor shall provide warranty service information and points of contact.

SECTION 1 **ROOM SCHEDULE AND DETAILS**
1.01 ROOM SCHEDULE
1.02 SPACE DETAILS

SECTION 2 **DESIGN SCHEMATIC LAYOUT**
2.01 DESIGN SCHEMATIC
2.02 ADJACENCY DIAGRAMS

SECTION 3 **ADDITIONAL SPECIAL REQUIREMENTS AND DETAILS**
3.01 ROOM LAYOUTS
3.02 ADDITIONAL CONSTRUCTION DETAILS

SECTION 4 **GENERAL REQUIREMENTS**
4.01 SECURITY
4.02 INFORMATION TECHNOLOGY
4.03 OTHER

SECTION 1 ROOM SCHEDULE AND DETAILS

1.01 ROOM SCHEDULE

Office Space

Space Type	Quantity	Space Allocation (ABOA SF)	Total
Cubicle	6	36	216
Subtotal			216
Circulation Factor		36%	78
TOTAL			293

Support Space

Space Type	Quantity	Space Allocation (ABOA SF)	Total
Break Room	1	72	72
Office Support Space	1	72	72
Huddle	1	72	72
K9 Bunker	1	72	72
IT LAN Closet	1	100	100
Subtotal			388
Circulation Factor		36%	140
TOTAL			528

Mission Space

Space Type	Quantity	Space Allocation (ABOA SF)	Total
Processing Room	1	72	72
Ammo/Weapons/Evidence Safe	1	120	120
K9 Storage	1	120	120
Tactical	1	100	100
Bulk Storage	1	120	120
Subtotal			532
Circulation Factor		36%	192
TOTAL			724

Office + Support + Mission Space = 1,545 ABOA SF

1.02 SPACE DETAILS

Please refer to the Lease document for the constructions standards applicable to the interior tenant area build-out. These standards provide a general outline of the interior build-out requirements. For a complete list of requirements refer to the Lease document.

Open Office Area

- Flooring – Carpet tile per Lease paragraph FLOOR COVERINGS AND PERIMETERS
- Walls – Per Lease paragraph PARTITIONS: SUBDIVIDING with finishes according to Lease paragraph PAINTING - TI
- Doors – Per Lease paragraph DOORS: INTERIOR with hardware per Lease paragraph DOORS: HARDWARE
- Ceiling – Per Lease paragraph CEILINGS
- Lighting – Per Lease paragraph LIGHTING: INTERIOR AND PARKING – SHELL and LIGHTING: INTERIOR AND PARKING- TI
- Electrical, Data, Voice – One duplex electrical receptacles and one combination data/voice jack per 80 ABOA SF on walls per Lease paragraph ELECTRICAL: DISTRIBUTION and TELECOMMUNICATIONS: DISTRIBUTION AND EQUIPMENT
- Window Coverings – Mini-blinds per Lease paragraph WINDOW COVERINGS for all windows

Enclosed Rooms

- Flooring – Carpet tile per Lease paragraph FLOOR COVERINGS AND PERIMETERS
- Walls – Per Lease paragraph PARTITIONS: SUBDIVIDING with finishes according to Lease paragraph PAINTING - TI
- Door – Per Lease paragraph DOORS: INTERIOR with hardware per Lease paragraph DOORS: HARDWARE
- Ceiling – Per Lease paragraph CEILINGS
- Lighting – Per Lease paragraph LIGHTING: INTERIOR AND PARKING
- Electrical, Data, Voice – Four duplex electrical receptacles and two combination data/voice jack on walls per Lease paragraph ELECTRICAL: DISTRIBUTION and TELECOMMUNICATIONS: DISTRIBUTION AND EQUIPMENT
- Window Coverings – Mini-blinds per Lease paragraph WINDOW COVERINGS for all windows

Break Room and Kitchenette Areas – Only applicable if room schedule calls for a break room or kitchenette area

- Flooring – Per FPS Construction requirements
- Walls – Per Lease paragraph PARTITIONS: SUBDIVIDING with finishes according to Lease paragraph PAINTING - TI
- Door – Per Lease paragraph DOORS: INTERIOR with hardware per Lease paragraph DOORS: HARDWARE
- Ceiling – Per Lease paragraph CEILINGS
- Lighting – Per Lease paragraph LIGHTING: INTERIOR AND PARKING
- Electrical, Data, Voice - Provide three duplex electrical receptacles and one wall combination data/voice jack. Provide two dedicated duplex electrical receptacles for refrigerators and two dedicated duplex electrical receptacles for vending machines. Provide two dedicated electrical receptacles for microwave ovens above the counter. Provide two additional duplex electrical receptacles above the counter (GFI as required by code).
- HVAC (Only if enclosed room) - Independent HVAC zone on thermostat in this room and provide means to ensure negative pressure for this room to avoid odors from escaping this room. Provide filters to remove odors from any air being mixed back into the supply air for the remainder of the building or exhaust directly to the outside.
- Window Coverings – Roller shades for all windows

- Millwork – Per FPS Construction requirements.

SECTION 2 DESIGN SCHEMATIC LAYOUT

2.01 DESIGN SCHEMATIC

General schematics of specific rooms identified in Section 1.01 can be found in Real Property Management Manual, Appendix C, attached hereto. The Lessor is responsible for using the room schedule in section 1.01 and this layout to adapt the Government's requirements to the Space. Specific questions regarding the layout should be directed to the Lease Contracting Officer for resolution. The Government shall not be responsible for errors, omissions, or assumptions made by the Lessor in the adaption of the Government's requirements to the Lessor's Space.

SECTION 3 ADDITIONAL SPECIAL REQUIREMENTS AND DETAILS

3.01 ~~ROOM LAYOUTS~~ INTENTIONALLY DELETED

3.02 ADDITIONAL CONSTRUCTION DETAILS

See the below documents, attached herein. These standards may be more stringent than those listed in the Lease document. Where specified, these standards shall take precedence.

- FPS Real Property Management Manual
- Region 5 Grand Rapids Construction Requirements

SECTION 4 GENERAL REQUIREMENTS

4.01 SECURITY

The following security standards are listed in addition to those listed in the Lease document and the building specific security attachment. See the below document, attached herein

- FPS PACS SOW

4.02 INFORMATION TECHNOLOGY

4.03

The following IT standards are listed in addition to those listed in the Lease document. See the below documents, attached herein

- Grand Rapids Area Command IT SOW
- Gallagher PACS Equipment List

4.04 OTHER – FURNITURE, FIXTURES AND EQUIPMENT

The following FF&E standards are listed in addition to those listed in the Lease document. See the below documents, attached herein

- TA-50 Brochure DASCO
- R5 Grand Rapids FF&E

DASCO
storagesolutions

TA-50 Gear Storage Locker

TA-50 Gear Storage Locker

Store Your Gear with Over 45 ft³ of Storage Space.

The TA-50 Gear Storage Locker is the ultimate gear storage solution. It has plenty of unobstructed room to store whatever you need – uniforms, weapons, gear bags, ammunition, boxes and more.

The storage applications are endless. Perforated gates and sides are ideal for ventilation and visual inspection. Customize your TA-50 Gear Storage Locker with our standard component offering. Check out the back page for more information.

Features

- Fully welded heavy-gauge steel body and gates
- Integrated Padlock hasp
- 3-point lock mechanism

TA-50 Gear Storage Locker Construction

Our TA-50 Gear Storage Lockers are the strongest, most durable TA-50 Gear Storage Locker available. It's all because of our manufacturing and construction methods:

- All-welded, heavy gauge steel construction
- Perforated gates and side panels
- Four universal back panel columns accommodate Dasco components
- This allows for a fully customizable interior using shelves, storage boxes, hooks, weapon components and more
- Built-in levelling feet
- Black Sandtex powder-coat finish

Two Available Sizes:

78"H x 42"W x 24"D
(1981mm H x 1066mm W x 610mm D)

78"H x 36"W x 24"D
(1981mm H x 914mm W x 610mm D)

Two-Tier TA-50 Gear Storage Locker

The Two-Tier TA-50 Gear Storage Locker has the same great features with two individual locking compartments in the same footprint as the standard TA-50 Gear Storage Locker. They are great for team storage applications, individual lockers or separating items from one another in storage.

Ventilation

Store your damp or wet gear in our full-ventilated TA-50 Gear Storage Lockers. The perforated gates allow for plenty of ventilation which ensures your valuable gear doesn't get musty and moldy. TA-50 Gear Storage Lockers are frequently used for wet suits and scuba gear.

Visual Inspection

The perforated gates also allow for quick and easy visual inspection. You can clearly see the contents of the locker and ensure nothing is being stored that shouldn't be. This is popular for police and military applications.

Versatility

TA-50 Gear Storage Lockers are incredibly versatile. TA-50 Gear Storage Lockers have been used for everything from elite tactical storage to hotel supplies. This is due to the various configurations you can create with your TA-50 Gear Storage Locker. See some of the standard components on the back page.

Two Available Sizes:

78"H x 42"W x 24"D
(1981mm H x 1066mm W x 610mm D)

78"H x 36"W x 24"D
(1981mm H x 914mm W x 610mm D)

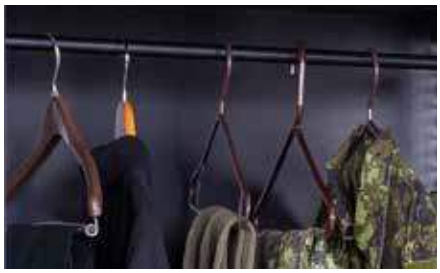
Usable Compartment Space (each):

37.5"H x 42"W x 21.5"D
(953mm H x 1066mm W x 546mm D)

37.5"H x 36"W x 21.5"D
(953mm H x 914mm W x 546mm D)

TA-50 Gear Storage Locker Components

Hanger Bar



The hanger bar is the perfect component for uniform or clothing storage. The durable bar stretches all the way across the rack and is very strong – it won't bend or sag.

Coat Hooks

Coat hooks provide a great hanging option in a versatile cabinet. Not just for coats, properly store your smaller gear like helmets, gloves or facemasks on a designated hook.

Additional Shelving

Compartmentalize your locker with additional shelves. The steel shelves are incredibly strong and have a 200LB capacity - perfect for gear bags, hard cased, boxes and even towels and bedding.

Universal Back Panel Columns

Our universal back panel columns are standard on every TA-50 Gear Storage Locker. You have four columns total to customize with Dasco Storage components. We offer 100's of components to help you store everything from weapons to first aid equipment.

Additional Components

To browse our full range of components, please contact a Dasco Storage Specialist or visit www.dascostorage.com.

DASCO storagesolutions

346 Orenda Rd., Brampton, Ont. Canada L6T 1G1
1-800-387-2468 | www.dascostorage.com
info@dascostorage.com

Ln	Site	Category	Material Manufacturer	Material Part Number	Material Description	QTY
1	BCMC	CABLING	WINDY CITY WIRE	5566040	1000' CAT6 ORANGE, PLENUM	2
2	BCMC	CABLING	TRIPP LITE	N201-001-OR	1' ORANGE CAT6 PATCH CABLES	6
3	BCMC	CABLING	TRIPP LITE	N201-006-OR	6' ORANGE CAT6 PATCH CABLES	2
4	BCMC	CABLING	PANDUIT	F4x4LG6	PANDUCT 4 X 4 FINGER TROUGH	24
5	BCMC	CABLING	PANDUIT	C4LG6	PANDUCT COVER	24
6	BCMC	CABLING	COMMSCOPE	107984015	M101SMB-B-262 SURFACE MTG BOX	4
7	BCMC	CABLING	COMMSCOPE	700206683	MGS400 ORANGE OUTLET	4
8	BCMC	CABLING	WINDY CITY	442342	CABLE FOR REX AND DC 18-04 SHD STR CMP BLU STP 1K FT	4
9	BCMC	CABLING	WINDY CITY	441380	CABLE FOR LOCK - 16-04 UNS STR CMP WHT JKT 1K FT	2
10	BCMC	CABLING	WINDY CITY	4160201	CABLE FOR READER - 18 AWG 3 PAIR BARE COPPER, EACH PAIR SHIELDED PLENUM 1K FT	2
11	BCMC	DOOR HARDWARE	SDC	MSB550	CRASH BAR REX	2
12	BCMC	DOOR HARDWARE	SDC	PT-3V	18" Door Loop, Aluminum	2
13	BCMC	DOOR HARDWARE	BOSCH	DS160	PIR REX	5
14	BCMC	DOOR HARDWARE	BOSCH	TP160	TRIM PLATE FOR DS160 REX	4
15	BCMC	DOOR HARDWARE	HES	1006CLB-630	ELECTRIC STRIKE	5
16	BCMC	DOOR HARDWARE	MAGNASHPERE	MSS-202C	3/4" RECESSED, 12" LEADS TWO CLOSED LOOP ALARM CONTACT WHITE	4
17	BCMC	DOOR HARDWARE	SCHLAGE	M490DEP	DELAYED EGRESS MAGLOCK	2
18	BCMC	DOOR HARDWARE	GALLAGHER	C305505	T21 PIV KEYPAD PROX/INSERT READER	12
19	BCMC	DOOR HARDWARE	GALLAGHER	C305410	T11 PIV PROX READER	4
20	BCMC	PACS PANEL INSTALLATION	ALTRONIX	BT1212	BATTERY, 12V 12 AH (POWER SUPPLIES)	2
21	BCMC	PACS PANEL INSTALLATION	GALLAGHER	FPO250	LSP FPO-250 250W POWER SUPPLY	1
22	BCMC	PACS PANEL INSTALLATION	GALLAGHER	C300680	HBUS 8 IN BOARD	1
23	BCMC	PACS PANEL INSTALLATION	GALLAGHER	C305721	LSP E4 CABINET, 12A PSU (THIRD PARTY PRODUCT)	1
24	BCMC	PACS PANEL INSTALLATION	GALLAGHER	C305740	LSP B100 SECONDARY VOLTAGE MODULE (THIRD PARTY PRODUCT)	1
25	BCMC	PACS PANEL INSTALLATION	GALLAGHER	C305741	LSP C8 LOCK CONTROLLER MODULE, 8 OUTPUT (THIRD PARTY PRODUCT)	2
26	BCMC	PACS PANEL INSTALLATION	GALLAGHER	C305762	LSP FULL BACKPLATE E4 (THIRD PARTY PRODUCT)	1
27	BCMC	PACS PANEL INSTALLATION	GALLAGHER	C305101	HIGH SEC CONTROLLER 6000	2
28	BCMC	PACS PANEL INSTALLATION	GALLAGHER	C300182	8H MODULE PROVIDES 8 HBUS PORTS, 24 BALANCED INPUTS AND 8 RELAY OUTPUTS	2
29	BCMC	PACS PANEL INSTALLATION	GALLAGHER	D8P	LSP D8P CONSTANT VOLTAGE POWER SUPPLY BOARD	3
30	BCMC	PACS SERVER LICENSE	GALLAGHER	C863400	SECUGEN HAMSTER PRO DUO SC/PIV	2
31	BCMC	PACS SERVER LICENSE	GALLAGHER	2A8067	WORKSTATION LICENSE (PER WORKSTATION)	2
32	BCMC	PACS SERVER LICENSE	GALLAGHER	2A8156	WORKSTATION LICENSE (PER WORKSTATION) - SM	2
33	BCMC	PACS DOOR PACKAGE	GALLAGHER	2A8500	HIGH SEC DOOR LICENSE	16
34	BCMC	PACS SERVER LICENSE	GALLAGHER	2A8501	PIV DOOR LICENSE (PER DOOR)-SM	16
35	BCMC	PACS WORKSTATION	DELL	210-BFXG	OPTIPLEX SMALL FORM FACTOR PACS WORKSTATION	2
36	BCMC	PACS WORKSTATION	DELL	210-BBCL	27" MONITOR -P2722H	2
37	BCMC	PACS WORKSTATION	CARLON	SC100RR	1-GANG NON-METALLIC LOW-VOLTAGE OLD WORK BRACKET	2
38	BCMC	PACS WORKSTATION	COMMSCOPE	108168469	FACEPLATE SINGLE GANG 2 PORT (WHITE)	2
39	BCMC	PACS WORKSTATION	COMMSCOPE	107067928	FACEPLATE BLANK INSERTS WHITE	2
40	BCMC	PACS WORKSTATION	COMMSCOPE	107984015	M101SMB-B-262 SURFACE MTG BOX	2
41	BCMC	PACS WORKSTATION	COMMSCOPE	700206683	MGS400 ORANGE OUTLET	2

DHS Management Directorate
IT Statement of Work (IT-SOW)
Federal Protective Service
DRAFT GRAND RAPIDS AREA COMMAND

DESCRIPTION: Renovate current or buildout new space to better align with the increasing mission of FPS in the area.

PROJECT NUMBER:

1. SCOPE:

It is the intent of Federal Protective Service Information Technology Division (FPS ITD) to provide detailed requirements for its Information Technology projects. This will help identify the roles and responsibilities of the vendor completing the work at FPS locations. This location will support 5 personnel in one suite.

2. APPLICABLE DOCUMENTS:

Commercial standards shall be used wherever practicable, and any data cabling will be installed per DHS cable standard.

3. SPECIFIC TASKS:

The contractor shall complete the following tasks as required to comply with this SOW.

- Vendor to install two (2) CAT 6 cable run for data with standard data outlet for each workstation identified in floor plan. (RJ-45 required)
- Vendor to install two (2) CAT 6 cable runs with standard data outlet for each printer location (RJ-45 required).
- Vendor to install one (1) CAT 6 cable run at each fax machine location (RJ-45 required) as identified in the floor plan.
    - Note: if device is a multi-function printer with both fax and printing capability, vendor will install two (2) CAT 6 runs with standard data outlet.
    - Vendor will provide one (1) RJ-11 female to RJ-45 male converter and one (1) RJ-45 female to RJ-11 male converter for each device requiring an RJ-11 connection (e.g., postal meter, fax machine).
- Vendor to install one (1) 18U wall mounted cabinet with a minimum depth of 22”and 19” width EIA in designated LAN area/room.
    - A 12U wall mounted cabinet may be used if inadequate wall space is available for a 18U cabinet. Vendor installation of a 12U wall mounted cabinet must first be approved by FPS ITD or FPS ASD.
    - 12U and 18U wall mounted cabinets will have a weight capacity no less than 150 lbs.

- Provide one (1) 24 Port rack-mounted CAT 6 Patch Panel to include all lines terminated and punched per manufacture standards. Patch panel will be installed in the IT equipment cabinet.
- In addition to workstation data drops, the vendor will provide wiring to the following rooms:
    - As requested by FPS Facilities personnel.
- Furnish and install data pedestals and wall jacks as required. Contractor to terminate and test all drops to LAN cabinet and provide connectivity test results.
- Contractor shall ensure that the alarm panel is connected to the LAN room switch using CAT6 RJ-45 cabling.
- Provide a 6 pair single-mode fiber extension form the building DEMARC to the FPS IT equipment rack.
    - 1.25 inch flexible conduit will be used for the entirety of extension length.
    - Vendor will install 6 port fiber LC single mode type distribution panels and terminate fiber extension at both DMARC and LAN room or rack locations.
    - Vendor will test all fiber pairs installed within of scope this project and provide test results to the COR.
    - Vendor will label all fiber installed within the scope of this project for ease of identification.

4. PROGRAM MANAGEMENT:

The contractor shall exercise technical direction and control of the engineering and test effort required to produce the equipment. This requirement includes the necessary management support tasks related to, configuration control, risk management, testing, quality assurance required to carry out the tasks identified in the SOW.

5. DOCUMENTATION:

Contractor shall provide copies of the documents listed below. One copy of the data shall be delivered in paper form and one copy in electronic form. The electronic form shall be in MS Word format or Portable Document Format (PDF). The documents are deliverables under the contract and shall be delivered to the COR no later than thirty days after contract award:

a. Operations Manual
b. Equipment Specification
c. Standard Warranty
d. Rack Elevation Diagram
e. Test results of all fiber installed
f. Digital Photographs of completed, vendor installed, rack buildouts

6. PLACE OF PERFORMANCE:

Grand Rapids

7. EQUIPMENT:

Equipment Racks:

- Vendor to install one (1) 18U wall mounted cabinet with a minimum depth of 24”and 19” width EIA wide on East common area wall.
- Ensure horizonal and vertical cable management in equipment racks follows industry best practices.
- Securely mount 18U or similar wall mounted cabinet with appropriate mounting board
  - Mounting Board will be painted after installation to match underlaying wall paint.
- Cabinet will be grounded appropriately per ANSI/TIA-942 grounding requirements.
- A 12U wall mounted cabinet may be used if inadequate wall space is available for a 18U Rack. Vendor installation of a 12U wall mounted rack must first be approved by FPS ITD or FPS ASD.
- 12U and 18U wall mounted cabinet will have a weight capacity no less than 150 lbs.

Power Requirements:

Dedicated Power:

- Two (2) dedicated 120-volt, 20-amp termination NEMA 5-20R wall receptacle.

Uninterruptable Power Supply:

- Vendor will procure one (1) 1500VA Rack Mounted UPS 100-127V with a 5-15P input will six (6) 5-15R receptacles.
- Vendor will install any UPS equipment in the wall mounted racks in accordance with UPS vendor recommendations.

Power Distribution Unit (PDU) Requirement:

- One (1) Rack PDU, Basic, 1U, 15A, 120V, with ten (10)5-15R; 5-15P input
- Note: Vendor will procure and install one (1) PDU in the LAN cabinet.

8. VIDEO TELECONFERENCING (VTC):

There is no VTC requirement for this site.

9. FIELD VERIFICATION:

The Government may provide the contractor drawings and specifications. It is the Contractor's responsibilities to field verify all drawings before laying out the work, and the contractor shall be responsible for any errors that might have been avoided by complying with this paragraph.

10. SITE VISITS:

It is the sole responsibility of the Contractor to visit the site, to ensure proper information is available for accurate design and repairs and to field verify any dimensions. Any failure of the Contractor to take the actions described in this paragraph will not relieve the Contractor from the responsibility of estimating properly the difficulty and cost of successfully performing the work. The Government assumes no responsibility for any conclusions or interpretations made by the Contractor based on the information made available by the Government.

Program POC:
Name:
Department of Homeland Security

Alternate POC:
Name:
Department of Homeland Security

11. CABLING:

Cable Color

The Department of Homeland Security has the need for computer equipment to be connected with appropriate color data cables. This will allow proper and quick identification of equipment on the three different Local Area Networks by clearance level and the telecommunication lines.

To meet this requirement, the following color configuration will be used:

Blue data cables for all CAT6 connections:

If necessary, alternate color fiber cables may be substituted for any system, if the cables are clearly marked on both ends designating the level of information traveling across the fiber. Red fiber cabling will not be used as an alternative color.

Horizontal Cables

All cable, equipment, and materials shall meet applicable ANSI/TIA/EIA-568-B, National Electrical Code (NEC) 770, Institute of Electrical and Electronics Engineers (IEEE) 802 and Underwriters Laboratory (UL) Verification Program standards. All cable equipment and materials must be manufactured by facilities that are International Organization for Standardization (ISO) 9001 registered and certified.

- Shall be CAT 6 rating in accordance with ANSI/TIA/EIA-568-B.2
- The cable should have contiguous, 2-foot segment-length markers printed on the cable jacket. The markings must also show the applicable performance CAT 6, as well as the fire rating of the cable being installed.
- The finished cable shall be 100% plenum rated in accordance with the requirements of NEC Article 800, UL 444, NFPA 262, (UL 910), and applicable Canadian Standards Association (CSA) standards.
- Use of Copper Clad Aluminum (CCA) ethernet cables is not permitted.

Patch Cables

Contractor shall supply and install all patch CAT 6 cable required for workstations and patch panels, to include patch panel to switch connections. Use of Copper Clad Aluminum (CCA) ethernet cables is not permitted.

Cables (Workstation)

The workstation patch cable connects the end user devices (personal computer, terminals, etc.) to the IMO (jack). For most installations, these patch cables will be provided and left on-site for the deployment team or local network people to install when setting up workstations and are not included in the overall cable plant certification. The workstation patch cable may be any length if the combined lengths of the workstation patch cable, the horizontal workstation cabling, and the patch-panel cable does not exceed 100 meters (328 feet). If the installation vendor chooses, custom-length, certified station cables can be used.

Patch Cables (Panel)

The patch-panel cable connects the horizontal cable port to the voice and data electronics within a central wire center or closet, typically a RWC or MDF. It is the cable installer's responsibility for patching all active cable locations into active ports, unless otherwise directed by the DHS manager or designated representative. These cables are pre-certified by the manufacturer; therefore, it is unnecessary to include them in the cable plant certification. Wire management and organization is important to facilitate troubleshooting, repair, and documentation and, as such, there are key elements to ensure patch cords are properly installed. The following requirements shall be followed for patching workstation ports to electronics:

- The patch-panel cable may be any length, provided that the combined length of the workstation patch cable, the horizontal workstation cabling, and the patch-panel cable does not exceed 100 meters (328 feet).
- If the installation vendor chooses, custom-length, certified station cables can be used.
- Patch cables must be labeled and matching on both ends, in a standard one-up numeric convention. An example would be a closet that has 100 active workstations, thus 100 patch cables are installed, one for each active node, starting with cable identification (ID) number one and ending with ID number 100. Any support personnel would be able to view the station patch panel and electronics equipment to determine which specific port a particular station is connected.
- Patch cable numbering shall be affixed to both ends of each patch cord approximately one inch from the terminator or mod plug.
- Label IDs must be legible and produced with indelible ink. The preferred method is a printed label. Installers must avoid the use of materials that will distract from the appearance of the installation, or any temporary marking.
- Ensure patch cables are installed in a manner that does not require support personnel to "tug" or "trace" cables in order to determine the active port.
- Cables must be dressed utilizing available horizontal and vertical wire management.
- Patch cables should provide a neat and organized appearance, eliminating large bundles of cables in single locations, preventing tangles and using incorrect or oversized cables that produce excess slack.
- Cables shall never exceed the minimum bend radius or have kinks or nicks in accordance with the ANSI/TIA/EIA specifications.
- Cables should utilize left and right vertical wire management to reduce cable patch congestion and produce even cable distribution within a given cabinet.
- Patch cables shall never create a trip hazard or other risk to equipment, services or personnel.

12. WIRELESS ACCESS POINTS

Vendor will perform a WI-FI site survey to assess optimal Access Point placement within spaces in which FPS personnel reside. High user density areas should, including conference rooms and training rooms, have optimal signal strength (between -55 dBm and -70 dBM) with potential sources of WI-FI interference identified. Vendor will provide FPS a survey report with the following data points for review before performing installation work:

- Floor plan heat map of purposed Access Point placement
- Number of Access Points needed

Access Point Cable Extensions

Once the purposed Access Point placement has been reviewed and approved by FPS, the vendor will extend CAT6e cables:

- Vendor will terminate all CAT6e Access Point Cables to the existing RJ45 patch panels located within the FPS LAN room. Patch panel ports that connect to Access Points will be labeled and patched to LAN room switch(s)
- Access points will be ceiling mounted with appropriate OEM mounting hardware

Hardware

FPS will procure and provide Access Points and mounting hardware to the contractor. The contractor will mount and connect the Access Points to locations identified in the Wi-Fi heat map. Quantities will be based on WI-FI site survey results, as approved by FPS personnel.

13. ACCESSIBILITY REQUIREMENTS (SECTION 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards.

Item that contains Information and Communications Technology (ICT): VOIP Network

Applicable Exception: N/A **Authorization #:** N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for software features and components (including Software infrastructure): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application

Applicable 508 requirements for hardware features and components (including Servers; Peripheral Equipment (ex. keyboards); Video Teleconferencing Equipment; Video Displays and Monitors): All requirements in Chapter 4 apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

Item that contains Information and Communications Technology (ICT): Communication System

Applicable Exception: N/A **Authorization #:** N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for software features and components (including Software infrastructure): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application

Applicable 508 requirements for hardware features and components (including Servers; Peripheral Equipment (ex. keyboards); Video Teleconferencing Equipment; Video Displays and Monitors): All requirements in Chapter 4 apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

Item that contains Information and Communications Technology (ICT): Network equipment configuration

Applicable Exception: N/A **Authorization #:** N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for software features and components (including Web, desktop, server, mobile client applications; Software infrastructure): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria Apply except 2.4.1 Bypass Blocks, 2.4.5 Multiple Ways, 3.2.3 Consistent Navigation, 3.2.4 Consistent Identification, 502 Interoperability with Assistive Technology, 503 Application

Applicable 508 requirements for hardware features and components (including Computers & laptops; Servers; Peripheral Equipment (ex. keyboards); Video Teleconferencing Equipment; Video Displays and Monitors): All requirements in Chapter 4 apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

1. When providing installation, configuration or integration services for ICT, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.

2. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards for each ICT.

3. Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017.

4. Where ICT conforming to one or more requirements in the Revised 508 Standards is not commercially available, the agency shall procure the ICT that best meets the Revised 508 Standards consistent with the agency's business needs, in accordance with 36 CFR E202.7. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017 and 36 CFR E202.6.

DHS Management Directorate
IT Statement of Work (IT-SOW)
Federal Protective Service
DRAFT GRAND RAPIDS AREA COMMAND

DESCRIPTION: Renovate current or buildout new space to better align with the increasing mission of FPS in the area.

PROJECT NUMBER:

1. SCOPE:

It is the intent of Federal Protective Service Information Technology Division (FPS ITD) to provide detailed requirements for its Information Technology projects. This will help identify the roles and responsibilities of the vendor completing the work at FPS locations. This location will support 5 personnel in one suite.

2. APPLICABLE DOCUMENTS:

Commercial standards shall be used wherever practicable, and any data cabling will be installed per DHS cable standard.

3. SPECIFIC TASKS:

The contractor shall complete the following tasks as required to comply with this SOW.

- Vendor to install two (2) CAT 6 cable run for data with standard data outlet for each workstation identified in floor plan. (RJ-45 required)
- Vendor to install two (2) CAT 6 cable runs with standard data outlet for each printer location (RJ-45 required).
- Vendor to install one (1) CAT 6 cable run at each fax machine location (RJ-45 required) as identified in the floor plan.
    - Note: if device is a multi-function printer with both fax and printing capability, vendor will install two (2) CAT 6 runs with standard data outlet.
    - Vendor will provide one (1) RJ-11 female to RJ-45 male converter and one (1) RJ-45 female to RJ-11 male converter for each device requiring an RJ-11 connection (e.g., postal meter, fax machine).
- Vendor to install one (1) 18U wall mounted cabinet with a minimum depth of 22”and 19” width EIA in designated LAN area/room.
    - A 12U wall mounted cabinet may be used if inadequate wall space is available for a 18U cabinet. Vendor installation of a 12U wall mounted cabinet must first be approved by FPS ITD or FPS ASD.
    - 12U and 18U wall mounted cabinets will have a weight capacity no less than 150 lbs.

- Provide one (1) 24 Port rack-mounted CAT 6 Patch Panel to include all lines terminated and punched per manufacture standards. Patch panel will be installed in the IT equipment cabinet.
- In addition to workstation data drops, the vendor will provide wiring to the following rooms:
    - As requested by FPS Facilities personnel.
- Furnish and install data pedestals and wall jacks as required. Contractor to terminate and test all drops to LAN cabinet and provide connectivity test results.
- Contractor shall ensure that the alarm panel is connected to the LAN room switch using CAT6 RJ-45 cabling.
- Provide a 6 pair single-mode fiber extension form the building DEMARC to the FPS IT equipment rack.
    - 1.25 inch flexible conduit will be used for the entirety of extension length.
    - Vendor will install 6 port fiber LC single mode type distribution panels and terminate fiber extension at both DMARC and LAN room or rack locations.
    - Vendor will test all fiber pairs installed within of scope this project and provide test results to the COR.
    - Vendor will label all fiber installed within the scope of this project for ease of identification.

4. PROGRAM MANAGEMENT:

The contractor shall exercise technical direction and control of the engineering and test effort required to produce the equipment. This requirement includes the necessary management support tasks related to, configuration control, risk management, testing, quality assurance required to carry out the tasks identified in the SOW.

5. DOCUMENTATION:

Contractor shall provide copies of the documents listed below. One copy of the data shall be delivered in paper form and one copy in electronic form. The electronic form shall be in MS Word format or Portable Document Format (PDF). The documents are deliverables under the contract and shall be delivered to the COR no later than thirty days after contract award:

a. Operations Manual
b. Equipment Specification
c. Standard Warranty
d. Rack Elevation Diagram
e. Test results of all fiber installed
f. Digital Photographs of completed, vendor installed, rack buildouts

6. PLACE OF PERFORMANCE:

Grand Rapids

7. EQUIPMENT:

Equipment Racks:

- Vendor to install one (1) 18U wall mounted cabinet with a minimum depth of 24”and 19” width EIA wide on East common area wall.
- Ensure horizonal and vertical cable management in equipment racks follows industry best practices.
- Securely mount 18U or similar wall mounted cabinet with appropriate mounting board
  - Mounting Board will be painted after installation to match underlaying wall paint.
- Cabinet will be grounded appropriately per ANSI/TIA-942 grounding requirements.
- A 12U wall mounted cabinet may be used if inadequate wall space is available for a 18U Rack. Vendor installation of a 12U wall mounted rack must first be approved by FPS ITD or FPS ASD.
- 12U and 18U wall mounted cabinet will have a weight capacity no less than 150 lbs.

Power Requirements:

Dedicated Power:

- Two (2) dedicated 120-volt, 20-amp termination NEMA 5-20R wall receptacle.

Uninterruptable Power Supply:

- Vendor will procure one (1) 1500VA Rack Mounted UPS 100-127V with a 5-15P input will six (6) 5-15R receptacles.
- Vendor will install any UPS equipment in the wall mounted racks in accordance with UPS vendor recommendations.

Power Distribution Unit (PDU) Requirement:

- One (1) Rack PDU, Basic, 1U, 15A, 120V, with ten (10)5-15R; 5-15P input
- Note: Vendor will procure and install one (1) PDU in the LAN cabinet.

8. VIDEO TELECONFERENCING (VTC):

There is no VTC requirement for this site.

9. FIELD VERIFICATION:

The Government may provide the contractor drawings and specifications. It is the Contractor's responsibilities to field verify all drawings before laying out the work, and the contractor shall be responsible for any errors that might have been avoided by complying with this paragraph.

10. SITE VISITS:

It is the sole responsibility of the Contractor to visit the site, to ensure proper information is available for accurate design and repairs and to field verify any dimensions. Any failure of the Contractor to take the actions described in this paragraph will not relieve the Contractor from the responsibility of estimating properly the difficulty and cost of successfully performing the work. The Government assumes no responsibility for any conclusions or interpretations made by the Contractor based on the information made available by the Government.

Program POC:
Name:
Department of Homeland Security

Alternate POC:
Name:
Department of Homeland Security

11. CABLING:

Cable Color

The Department of Homeland Security has the need for computer equipment to be connected with appropriate color data cables. This will allow proper and quick identification of equipment on the three different Local Area Networks by clearance level and the telecommunication lines.

To meet this requirement, the following color configuration will be used:

Blue data cables for all CAT6 connections:

If necessary, alternate color fiber cables may be substituted for any system, if the cables are clearly marked on both ends designating the level of information traveling across the fiber. Red fiber cabling will not be used as an alternative color.

Horizontal Cables

All cable, equipment, and materials shall meet applicable ANSI/TIA/EIA-568-B, National Electrical Code (NEC) 770, Institute of Electrical and Electronics Engineers (IEEE) 802 and Underwriters Laboratory (UL) Verification Program standards. All cable equipment and materials must be manufactured by facilities that are International Organization for Standardization (ISO) 9001 registered and certified.

- Shall be CAT 6 rating in accordance with ANSI/TIA/EIA-568-B.2
- The cable should have contiguous, 2-foot segment-length markers printed on the cable jacket. The markings must also show the applicable performance CAT 6, as well as the fire rating of the cable being installed.
- The finished cable shall be 100% plenum rated in accordance with the requirements of NEC Article 800, UL 444, NFPA 262, (UL 910), and applicable Canadian Standards Association (CSA) standards.
- Use of Copper Clad Aluminum (CCA) ethernet cables is not permitted.

Patch Cables

Contractor shall supply and install all patch CAT 6 cable required for workstations and patch panels, to include patch panel to switch connections. Use of Copper Clad Aluminum (CCA) ethernet cables is not permitted.

Cables (Workstation)

The workstation patch cable connects the end user devices (personal computer, terminals, etc.) to the IMO (jack). For most installations, these patch cables will be provided and left on-site for the deployment team or local network people to install when setting up workstations and are not included in the overall cable plant certification. The workstation patch cable may be any length if the combined lengths of the workstation patch cable, the horizontal workstation cabling, and the patch-panel cable does not exceed 100 meters (328 feet). If the installation vendor chooses, custom-length, certified station cables can be used.

Patch Cables (Panel)

The patch-panel cable connects the horizontal cable port to the voice and data electronics within a central wire center or closet, typically a RWC or MDF. It is the cable installer's responsibility for patching all active cable locations into active ports, unless otherwise directed by the DHS manager or designated representative. These cables are pre-certified by the manufacturer; therefore, it is unnecessary to include them in the cable plant certification. Wire management and organization is important to facilitate troubleshooting, repair, and documentation and, as such, there are key elements to ensure patch cords are properly installed. The following requirements shall be followed for patching workstation ports to electronics:

- The patch-panel cable may be any length, provided that the combined length of the workstation patch cable, the horizontal workstation cabling, and the patch-panel cable does not exceed 100 meters (328 feet).
- If the installation vendor chooses, custom-length, certified station cables can be used.
- Patch cables must be labeled and matching on both ends, in a standard one-up numeric convention. An example would be a closet that has 100 active workstations, thus 100 patch cables are installed, one for each active node, starting with cable identification (ID) number one and ending with ID number 100. Any support personnel would be able to view the station patch panel and electronics equipment to determine which specific port a particular station is connected.
- Patch cable numbering shall be affixed to both ends of each patch cord approximately one inch from the terminator or mod plug.
- Label IDs must be legible and produced with indelible ink. The preferred method is a printed label. Installers must avoid the use of materials that will distract from the appearance of the installation, or any temporary marking.
- Ensure patch cables are installed in a manner that does not require support personnel to "tug" or "trace" cables in order to determine the active port.
- Cables must be dressed utilizing available horizontal and vertical wire management.
- Patch cables should provide a neat and organized appearance, eliminating large bundles of cables in single locations, preventing tangles and using incorrect or oversized cables that produce excess slack.
- Cables shall never exceed the minimum bend radius or have kinks or nicks in accordance with the ANSI/TIA/EIA specifications.
- Cables should utilize left and right vertical wire management to reduce cable patch congestion and produce even cable distribution within a given cabinet.
- Patch cables shall never create a trip hazard or other risk to equipment, services or personnel.

12. WIRELESS ACCESS POINTS

Vendor will perform a WI-FI site survey to assess optimal Access Point placement within spaces in which FPS personnel reside. High user density areas should, including conference rooms and training rooms, have optimal signal strength (between -55 dBm and -70 dBM) with potential sources of WI-FI interference identified. Vendor will provide FPS a survey report with the following data points for review before performing installation work:

- Floor plan heat map of purposed Access Point placement
- Number of Access Points needed

Access Point Cable Extensions

Once the purposed Access Point placement has been reviewed and approved by FPS, the vendor will extend CAT6e cables:

- Vendor will terminate all CAT6e Access Point Cables to the existing RJ45 patch panels located within the FPS LAN room. Patch panel ports that connect to Access Points will be labeled and patched to LAN room switch(s)
- Access points will be ceiling mounted with appropriate OEM mounting hardware

Hardware

FPS will procure and provide Access Points and mounting hardware to the contractor. The contractor will mount and connect the Access Points to locations identified in the Wi-Fi heat map. Quantities will be based on WI-FI site survey results, as approved by FPS personnel.

13. ACCESSIBILITY REQUIREMENTS (SECTION 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards.

Item that contains Information and Communications Technology (ICT): VOIP Network

Applicable Exception: N/A **Authorization #:** N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for software features and components (including Software infrastructure): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application

Applicable 508 requirements for hardware features and components (including Servers; Peripheral Equipment (ex. keyboards); Video Teleconferencing Equipment; Video Displays and Monitors): All requirements in Chapter 4 apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

Item that contains Information and Communications Technology (ICT): Communication System

Applicable Exception: N/A **Authorization #:** N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for software features and components (including Software infrastructure): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application

Applicable 508 requirements for hardware features and components (including Servers; Peripheral Equipment (ex. keyboards); Video Teleconferencing Equipment; Video Displays and Monitors): All requirements in Chapter 4 apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

Item that contains Information and Communications Technology (ICT): Network equipment configuration

Applicable Exception: N/A **Authorization #:** N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for software features and components (including Web, desktop, server, mobile client applications; Software infrastructure): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria Apply except 2.4.1 Bypass Blocks, 2.4.5 Multiple Ways, 3.2.3 Consistent Navigation, 3.2.4 Consistent Identification, 502 Interoperability with Assistive Technology, 503 Application

Applicable 508 requirements for hardware features and components (including Computers & laptops; Servers; Peripheral Equipment (ex. keyboards); Video Teleconferencing Equipment; Video Displays and Monitors): All requirements in Chapter 4 apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

1. When providing installation, configuration or integration services for ICT, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.

2. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards for each ICT.

3. Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017.

4. Where ICT conforming to one or more requirements in the Revised 508 Standards is not commercially available, the agency shall procure the ICT that best meets the Revised 508 Standards consistent with the agency's business needs, in accordance with 36 CFR E202.7. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017 and 36 CFR E202.6.

DEPARTMENT OF HOMELAND SECURITY (DHS)
FEDERAL PROTECTIVE SERVICE (FPS)

STATEMENT OF WORK (SOW)
FOR

FPS Space Physical Access Control Solution for XXXXXXXXX

1. INTRODUCTION

The Federal Protective Service/DHS intends to procure and install a stand alone Physical Access Control (PACS) solution with the capability to be enterprised in the future and to comply with directives and mandates, as well as any other applicable standards.

1.1. Background

DHS/FPS is responsible for Homeland Security Presidential Directive (HSPD-12) compliant PACS solution within DHS/FPS occupied space, which establishes a secure and controlled access to FPS perimeter doors and internal restricted areas.

1.2. Guiding Documents

This section lists the references and authoritative documents for guiding this requirement:

1. HSPD-12 dated August 27, 2004, DHS Policy Directive 3, *Homeland Security Advisory System*, March 11, 2002
2. Federal Information Security Management Act of 2002 (FISMA)
3. National Institute of Standards and Technology (NIST):
    a. Federal Information Processing Standards 199 dated February, 2004.
    b. Federal Information Processing Standards 140 dated February 2001.
    c. Federal Information Processing Standards 200 dated March, 2006.
    d. Federal Information Processing Standards 201 dated February 25, 2005 (subsequently amended).
    e. Federal Information Processing Standards 201-2.
    f. NIST Special Publication 800-30 - Risk Management Guide for Information Technology Systems dated July, 2002.
    g. NIST Special Publication 800-37 - Guide for the Security Certification and Accreditation of Federal Information Systems dated February, 2010.
    h. NIST Special Publication 800-53 - Security Controls for Federal Information Systems and Organizations dated May, 2010.
    i. NIST Special Publication 800-57 – Recommendation for Key Management dated March, 2007.

DRAFT

j. NIST Special Publication 800-73 – Interfaces for Personal Identity Verification.

k. NIST Special Publication 800-116 - "A Strategy for the Use of PIV Credentials in Physical Access Control Systems." dated November, 2008. (subsequently amended to 800-116-1)

l. Federal Information Processing Standards publication 140-2 date May 25, 2001.

4. Office of Management and Budget (OMB M-10-15)

   a. E-Authentication Guidance for Federal Agencies (M-04-04) dated December 16, 2003.

   b. Implementation of HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors (M-05-24) dated August 5th 2005.

   c. Protection of Sensitive Agency Information (M-06-16) dated June 23, 2006.

   d. Acquisition of Products and Services for Implementation of HSPD-12 (M-06-18) dated June 30, 2006.

   e. Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials (M-07-06) dated January 11, 2006.

   f. FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (M-10-15) dated April 21, 2010.

   g. Continued Implementation of HSPD-12- Policy for a Common Identification Standard for Federal Employees and Contractors (M-11-11) dated February 3, 2011.

5. Interagency Security Committee (ISC)

   a. Facility Security Level Determinations for Federal Facilities (2008).

   b. Physical Security Criteria for Federal Facilities (April 12, 2010).

   c. Facility Security Committees (February 28, 2011).

   d. Selecting PIV Authentication Mechanisms_DRAFT (2013).

6. Federal Council of CIOs

   a. Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance, dated November 2009.

   b. Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance Version 2, dated December 2, 2011.

   c. DRAFT: Federated Physical Access Control System (PACS) Guidance, V1.

DRAFT

d. Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), DRAFT, Version 2.0.2, May 24, 2012.

e. HSPD-12 Personal Identity Verification and Credentialing Handbook, dated October 20, 2008.

f. *Response to OMB Request on Security and Privacy Needs,* dated January 31, 2007.

g. Identity, Credential and Access Management (ICAM) Roadmap, dated October 2008.

h. LACS/PACS Deployment Plan developed by the HSPD-12 Program Management Office and the Security Division (dated October, 2009) and submitted to the Office of Management and Budget on February 22, 2010.

i. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, May 2012.

DRAFT

2. SCOPE

The DHS FPS intends to acquire a Gallagher PACS solution that includes hardware and software, equipment, installation, maintenance and warranty for the FPS space located at the XXXXX .

3. OBJECTIVES

The scope of this acquisition is to provide a Gallagher PACS solution to reduce risks to personnel and assets by monitoring and controlling physical access to facilities. Work shall include, but is not limited to:

1. Conducting site surveys, special studies, special assessments, and preparing reports.
2. Developing preliminary engineering concepts.
3. Developing equipment installation engineering plans.
4. Providing hardware and software.
5. Installing hardware, software and cabling.
6. Providing system integration for proper subsystem interaction and operation.
7. Testing, inspecting, and reporting all work performed, in writing, on a weekly basis.
8. Preparing reports on achieving significant milestones.
9. Preparing other reports as requested but not identified in this list.
10. Providing as-built installation drawings in Visio, AutoCAD 2010 or BIM, provided DHS/FPS has said programs.
11. Performing facility modification/construction in support of equipment installation.
12. Providing and installing new data transmission systems.

13. Interfacing with existing data transmission systems.
14. Determining compatibility and interfacing of new equipment with existing equipment and documenting this information for submission.
15. Providing operation and maintenance manuals.
16. Providing training.
17. Warranting systems.
18. Maintaining and servicing systems.
19. Monitoring and maintaining operation of systems.

The Contractor shall be certified by the manufacturer and shall hold an HSPD-12 certification as an approved vendor listed on the Approved Products List (APL) of Federal Acquisition Service (FAS) IT Schedule 51, 70, 84 or SIN 132-62. Contractor personnel who will configure the solution must hold the Certified System Engineer ICAM PACS (CSEIP) certification as recognized by the General Services Administration. The current registry of certified individuals can be found here. http://www.smartcardalliance.org/activities-cseip-registry/

DRAFT

4. GENERAL REQUIREMENTS

4.1. General Requirements

This section provides general requirements for the Solution itself.

Table 4.1: General Requirements

Reference	Reference	Requirement
Mandatory	4.1.1	The system shall have the following password rules: Password shall be eight characters with a minimum of one (1) uppercase character and numeric/special character as defined by DHS/FPS OCIO.
Mandatory	4.1.2	Passwords shall not be stored in clear text; they shall be cryptographically hashed.
4.1.3	**4.1.3**	**Security Requirements**
Mandatory	4.1.4	All Administrator actions within any account shall be written into a non-editable journal, identifying the Administrator who performed the action, the time at which it was performed, the action performed, and the resulting data entered into (or removed from) the system. All communication shall be encrypted according to DHS/FPS policy.

Mandatory	4.1.5	Audit logs shall be archived and backed up to the Disaster Recovery site.
4.1.6	**4.1.6**	**Software Upgrade Process**
		The software of the centralized PACS application shall be upgradable by the Contractor with minimal down-time for the application, and no down-time for the on premise equipment. Upgrades shall be performed during non-business hours within an agreed software maintenance window. There shall be no loss of data during a software upgrade process. All major software and firmware updates will require vulnerability scans prior to deployment to Production. The contractor will be required to show evidence of updates and vulnerability scans.
		The firmware in the on premise control equipment (control panels, edge devices, etc.) shall be upgradeable and no user intervention shall be required.

DRAFT

4.2. Application Maintenance and Service Level Requirements

This section provides the application maintenance and service requirements for the Solution itself.

Table 4.2: Application Maintenance and Service Level Requirements

Reference	Reference	Requirement
4.2.1	**4.2.1**	**Application Maintenance and Service-Level Agreement (SLA) Requirements**
Mandatory	4.2.1.1	Contractor shall provide ongoing application maintenance as needed to provide code fixes, routine feature enhancements, and updates required to comply with HSPD-12, FIPS 201 and FISMA requirements.
Mandatory	4.2.1.2	Contractor shall perform all system administration required on servers, storage, and related operating systems and third-party applications used in its product.

Mandatory	4.2.1.3	Contractor shall perform all Database Administration (DBA) required on the Primary and Disaster Recovery database systems used in its product.
Mandatory	4.2.1.4	Contractor shall provide an SLA for responding to service impairments, downtime, or any other compromised performance.
Mandatory	4.2.1.5	Contractor shall upgrade system capacity as required to maintain the established response time performance requirements.
Mandatory	4.2.1.8	Contractor shall provide sufficient storage in both the Primary and Disaster Recovery facilities to ensure that all database records are retained for at least five (5) years.
Mandatory	4.2.1.9	All database records shall be automatically mirrored from the Primary database to the Disaster Recovery database on a continuous real time basis. The Contractor shall describe how this requirement is to be met.

4.3. Scaling Requirements

This section provides the performance and scaling requirements for the COTS PACS application.

Table 4.3: Application Scaling Requirements

Reference	Reference	Requirement
4.3.1	**4.3.1**	**Scaling**
Mandatory	4.3.1.1	The solution shall be capable of supporting at least 500 credentialed users initially, with demonstrable scalability to at least "unlimited but controlled."

DRAFT

Mandatory	4.3.1.2	The solution shall be capable of being configured to support at least 5,000 logins initially, with demonstrable scalability to at least 20,000.
Mandatory	4.3.1.3	The solution shall provide sufficient storage to maintain all system records and event histories for a minimum of five (5) years.

		All system level data related to presence, status, alarm data as well as virtual software points produced in the system shall be auto-exposed to third-party systems. These points shall be automatically exposed in the system meaning system integration or programming to customize the transport of these data points to third-party system shall not be required. Data shall be available down to the edge device such as card reader and door contact, occupancy sensor, etc.
		System shall normalize and cleanse data prior to transport to third-party systems. This includes following a common and approved point naming convention mutually agreed upon by DHS/FPS and PACS vendor.
		PACS system shall be able to store no less than 365 days of continuous system data.

DRAFT

4.4. ENERGY STANDARDS

"All hardware procured directly or in support of this action must meet applicable and appropriate EPEAT and Energy Star standards. The EPEAT standard level met must be entered into the NPPD SAMS inventory system when the property is received."

5. PACS SPECIFICATIONS

The following specifications provide functional, technical and operational requirements for the PACS.

5.1. Summary

1. The Gallagher PACS solution shall provide complete access control capable of being integrated with video surveillance (i.e. CCTV), intrusion detection, and other perimeter security countermeasures and systems.
2. The PACS solution shall consist of an application, Access Control Panels (ACPs), FIPS 201 readers (including PIV, see Reader section), and related sensor and door control devices. As described below, the ACP may be either a traditional multi-door control panel, or a single-door "edge" device.
3. All relevant systems shall be integrated for detecting, delaying, and deterring unauthorized individuals from entering protected facilities while providing access to authorized personnel.
4. The PACS solution shall:

   - Support the use of PIV III-IV, and common access card (CAC) credentials. The solution must be technical interoperable with all PIV card stock in current use by the Federal Protective Service.

   - Support the four (4) electronic identification and authentication mechanisms (PKI-Auth, Biometric, CHUID, CAK).

   - Support registration of PIV/PIV-I/CAC credentials by performing credential & user verification (BIO, CAK, PKI-Auth).

   - Provide routine status checks for all registered credentials (eg: Caching Status Proxy).

   - Have the ability to process the 1st five (5) elements of the FACSN (64 Bits) plus the 128 Bit UUID.

   - Support or be upgradable to support challenge/response at the door.

5.2. PACS Requirements

The PACS requirement shall be a hardware and software solution meeting the following criteria:

1. COTS Solution: The solution shall be a Gallagher product found on the GSA APL. DHS/FPS does not intend to issue a development contract for a system, and therefore will rely on existing COTS solutions.

2. The contractor shall provide a computer complete with hardware/software capable of fully operating the PACS. The laptop will be screened by the FPS IT division before being placed into operation. Coordination for the screening shall be made by the COR. The laptop will become government property.

DRAFT

3. The solution shall remain fully functional while being upgraded or backed up.

4. Disaster Recovery: The architecture shall also support a geographically remote Disaster Recovery facility with a full copy of all applications, synchronized databases, and the immediate ability to take over data processing operations in the event of a catastrophic failure at the primary facility. Failover and synchronization with a disaster recovery server shall occur immediately and seamlessly in the event of a manmade or natural disaster. Should the events be precipitated by technical issues, a decision to failover and commence synchronization shall be made and implemented within 90 minutes from the time of the occurrence.

The E-PACS shall be capable of evaluating the validity of a PIVcredential and the binding of the credential to the bearer at time of registration and at time of access in accordance with the following requirements:

5. The E-PACS shall confirm the validity of the PIV credential presented by performing the following functions:
    a. Active Authentication
        i. A challenge/response protocol using PKI certificates on the PIV card.
        ii. Note: at time of access, the E-PACS shall confirm the public key used in item 1.a.i is identical to the public key that was initially registered and authorized for access.
    b. Validation of Trusted Origin
        i. Certificate status checking (i.e. confirming expiration, revocation, signature validation).
        ii. Path discovery and validation (i.e. evaluating the full trust chain to a trust anchor for policies, constraints, expiration, revocation status and signature verification).
        iii. The certificate policy presented by the credential shall chain back to [Common] for PIV, or to [FBCA] for PIV-I.
    c. Bearer Confirmation
        i. Use PKI-CAK if no bearer confirmation is required.
        ii. Use PKI-AUTH for challenge/response, and confirmation of the bearer's presented PIN.
        iii. Use PKI-AUTH + BIO(-A) for challenge/response and confirmation of the bearer's presented PIN and fingerprint.

    Only when the results of these three operations (1.a, 1.b and 1.c) are confirmed as positive should a credential either be registered to the E-PACS for authorization, or granted access based on the authorization profile for that credential.
6. The E-PACS shall use an [APL] approved Validation System to perform item 1.b "Validation of Trusted Origin". Validation Systems may use one or a combination of:
    a. Certificate Revocation Lists (CRLs),
    b. Online Certificate Status Protocol (OCSP), or

DRAFT

    c. Server-based Certificate Validation Protocol (SCVP).
7. The E-PACS may use cached information for item 1.b "Validation of Trusted Origin" using the technologies identified in 2. In all cases, credentials must be valid at time of registration or access such that:
    a. The PIV credential's certificates have not been placed on CRL by the issuing certificate authority within the previous six (6) hours.
    b. Full path discovery and validation information is not more than 18 hours old.
8. At time of in-person registration, the E-PACS shall:
    a. Capture the Content-Signer certificate, the PKI-AUTH certificate, and the PKICAK certificate for purposes of periodic Validation of Trusted Origin (items 1.b, 2 and 3).
    b. At a minimum, use PKI-AUTH for challenge/response, and confirmation of the bearer's presented PIN.
    c. Check the expiration date of all data objects and signers on the credential and perform a private key challenge/response for each certificate being registered.
    d. Perform Validation of Trusted Origin (items 1.b, 2 and 3) of the user's credential and its signers.
9. An organization may have an Enterprise Identity Management (E-IdM) system in place. In this environment, the E-PACS may have direct provisioning and deprovisioning of access records from the E-IdM that are tightly bound to Human Resources processes. This method shall be in addition to "Validation of Trusted Origin" as described in items 1.b, 2 and 3.
    a. At a minimum, the E-IdM shall provide the CHUID, the Content-Signer certificate, the PKI-AUTH certificate, and the PKI-CAK certificate for purposes of:
        i. Periodic "Validation of Trusted Origin" (items 1.b, 2 and 3)
        ii. Verification of the public key as registered to the E-PACS (item 1.a.ii)
10. Performance Criteria at time of access
    a. PKI-CAK
        i. Performance Time is measured from detection of the card by the PIV reader (contact or contactless) to the access grant or access denied response at the door. Included as a part of this process is the PKI challenge and response to include certificate validation (items 1.b, 2 and 3).
        ii. Performance Time shall be 2.5 seconds or less.
    b. PKI-AUTH
        i. Performance Time is measured from completion of entering the PIN to the access grant or access denied response at the door. Included as a part of this process is the PKI challenge and response to include certificate validation (items 1.b, 2 and 3).
        ii. Performance Time shall be 2.5 seconds or less.
    c. PKI-AUTH + BIO(-A)

DRAFT

i. Performance Time is measured from completion of entering the PIN and successful presentation of a fingerprint to the access grant or access denied response at the door. Included as a part of this process is match-to-card fingerprint validation, and the PKI challenge and response to include certificate validation (items 1.b, 2 and 3).

ii. No Performance Criteria are established at this time.

11. Severity Notification

a. Background: The FIPS 201 Evaluation Program / Approved Product List (APL) updates the technical criteria for approved product / service listings on a periodic, and as needed, basis. When these updates are made, listed/approved products are re-assessed according to the updated criteria (this generally occurs due to identification of new threats, updated standards / policies, etc.). Noncompliant products / services will be assessed a "Severity" finding. When this is the case, the Severity classification may be either a 1 (most severe), 2 (moderate), or 3 (low severity). Each severity finding has an allowable period of time for the vendor to correct and update their product / service.

b. Requirements: Severity 1 findings require the most urgent attention by the vendor to correct the noted product / service issue.

i. It is the responsibility of the product/service vendor to promptly notify the Integrator / Installer of any Severity 1 findings, and provide a brief action plan to address timely resolution of the noted issue. Resolution of noted issue shall include provision of a "patch", approved by the FIPS 201 Evaluation Program, free of charge to the Integrator / Installer. Additionally, the product / service vendor shall notify the Integrator / Installer when the issue has been resolved and confirm acknowledgement.

ii. It is the responsibility of the Integrator / Installer to promptly notify the Contracting Officer (CO) and / or Contracting Officer Technical Representative (COTR) of any Severity 1 findings, and provide a brief action plan to address timely resolution of the noted issue. Resolution of noted issue shall include provision of a "patch", approved by the FIPS 201 Evaluation Program, free of charge to the government. Additionally, the Integrator / Installer shall notify the CO/COTR when the issue has been resolved and confirm acknowledgement.

12. Products / Services Transitioned to the Removed Products List (RPL)

a. Background: The FIPS 201 Evaluation Program / Approved Product List (APL) updates the technical criteria for listing on a periodic, and as needed, basis. When these updates are made, listed/approved products are re-assessed according to the updated criteria (typically due to identification of new threats, updated standards / policies, etc.). When this occurs, products or services may be transitioned to the Removed Products

DRAFT

List. In general, this is done when technology becomes obsolete or is no

Area	Card Reader Dual Factor	Card Reader Single Factor	Electric Lock	Video Intercom Door Station	Door Sensor	Video Intercom Master Station	Request to Exit (REX)	**Enrollment Station
Floor								
Total								

longer suitable for government use (due to vulnerability, etc.).

b. Requirements: The Integrator / Installer of APL approved Products / Services vendor must stipulate that their product / service, when provided to the government, shall, from time of procurement, remain active on the APL (not transitioned to the RPL) for a minimum period of one year.

DRAFT

5.3. PACS Components Requirements

** The enrollment stations shall consist of one (1) stand alone laptop or desktop computer with 20" monitor fully loaded with all necessary software to enroll personnel and facility access cards and PIV credentials, track, revoke, and monitor access. Conduct reports of access activity. The station shall be equipped with the necessary card reader to perfom enrollment activities.

5.4. PACS Operational and Functional Requirements

The following sections define the operational and functional requirements for the PACS solution:

a. Shall control, monitor, and record all valid and invalid entry attempts by personnel using access cards at card reader terminals.

b. Shall authenticate the person based on the credential value read from the card by the reader.

c. Shall automatically control door access by comparing credential value(s) stored within the access card with similar information previously programmed into the PACS.

d. Shall display to the guard station, the image associated with each credential/user requesting access as a secondary authentication factor.

e. Shall be compliant with authentication and authorization procedures required under HSPD-12 and FIPS 201-1, including but not limited to facility code,

agency code, and credential value, as contained in the Federal Agency Smart Credential Number (FASCN) and/or Cardholder Unique Identifier (CHUID), as well as the Universal Unique Identifier (UUID).

f. Shall maintain a database describing authorized access card I.D. numbers with their authorized points and times of entry, access level, and other associated privileges based on the programming entered by the system administrator, but initially established by the contractor.

g. Shall be a central PACS application to provide credential verification/certificate monitoring.

h. Shall perform authentication and authorization as follows:

- If the information on the card is authenticated against the data stored in the PACS, a signal is sent to the card reader terminal location to operate the release device, allowing the person to open the door/gate/turnstile.
- If the information on the card is not authenticated within the PACS, the PACS does not release the activating device but sounds a brief alarm, either audible, visual or both at the reader and logs the access card number, access point, time of day, and an indication of why access was denied.
- Each door shall be monitored and logged for real time status (open/close).
- A programmable alarm shunt timer (two (2) to 120 seconds) allows door to be opened for authorized card access entry, allowing adequate time to enter without alarming the system. An alarm shall occur if the door remains open beyond the preset alarm period.
- The system shall not alarm when an exit device (pushbutton or request to exit sensor) is used to leave a secure area.

i. Shall report power loss, tampering, door ajar, and forced alarms.

j. Shall be restricted through at least two (2) security access levels in order to prevent unauthorized program modifications or use by unauthorized personnel. The system shall require two (2) factor authentications using the PIV card for system login/administration and for authorization to change programming parameters.

k. Shall maintain a calendar clock for controlling and indicating all time related functions, such as schedule door lock open and close command.

l. Shall allow the system administrator, using appropriate keyboard commands, to program the ACP to automatically suppress alarms and unlock doors to enable door access for extended time intervals when monitoring is not required. This event information shall be recorded and capable of being documented.

DRAFT

m. Shall allow the system administrator to display on monitor, interface, and print summary reports, including:

- Alarms.
- Access activity at specified card reader.
- Denied access attempts.
- Doors in override mode (card access).
- Doors with alarms suppressed (monitored).
- All transactions stored in disks (printout to be sorted by date, time, transaction type, card ID number, card reader, or alarm monitor transactions).
- No data shall be stored on removable media (archiving shall be to systems which comply with the CIO Server Policy).
- All user programmable data.

n. Shall allow for the separation of PII information from non-PII information.

DRAFT

5.4.1. PACS System Architecture Requirements

1. The PACS solution shall use either multi- or single-door ACPs or edge devices, which shall make and manage local access control decisions when access cards are presented to readers.

2. In addition to the PIV card, the ACPs shall be capable of accommodating multiple card formats all up to 200 bits and accept one or more reader types.

3. In the case of multi-door ACPs, the ACP shall accept expansion modules that provide additional capacity or functionality to the system. Each of these expansion devices shall connect to and manage a set of inputs, outputs, or reader

5.4.2. Networking and Data Security Requirements

1. Administrative access to the security management application and the personnel security data shall be protected by dual-factor FIPS 201 credentials.

5.4.3. Access Control Functional Requirement

The PACS (application and ACP) shall support the following features:

1. Access control features shall include:

    a. Multiple group privileges per person.

2. Reader/credential support for the following:

a. Federal standards: PIV, PIV-I, CAC, TWIC, Facility Access Cards used by the Federal Protective Service.

b. Biometric.

c. Digital keypad.

d. Contact and contactless smart cards.

3. Detailed time specifications.

4. Multiple card formats for mixed card populations (minimum of 12).

5. Activation/expiration date/time by person with one minute resolution.

6. Access level disable for immediate lockdown.

7. Multiple holiday schedules.

8. Timed unlock schedules.

9. Scheduled actions for arming inputs, activating outputs, locking and unlocking portals.

10. Card enrollment reader support.

11. Visitor Management:

    a. The vendor will provide the government with an HSPD-12 compliant visitor managememnt system.

    b. FPS requires that the system is capable of producing accurate and comprehensive data regarding each incidence of access attempted or granted. The system shall be capable of presenting the cardholder's image on screen in order to verify the credential holder with his or her stored photograph.

12. Timed anti-pass back.

13. Muster/Roll Call Reporting.

14. Dual reader portal support.

15. Wiegand keypad PIN support.

16. RS 485 (bi-directional communication).

17. First-in/Supervisor unlock rule.

18. At least 20 user-defined and searchable database fields.

DRAFT

19. System user permissions to grant whole or partial access to system resources, commands, and personal data.

20. Ability to arm/disarm groups of inputs based on other system inputs or alarm events.

21. Tiered administrative access to system functions and data such that some administrators' access may be restricted.

5.4.4. Reporting Requirements

1. The system shall be capable of producing a variety of predefined reports regarding software and security hardware configuration, event history, and the administration of people within the system.

2. The system shall be capable of producing for the Administrator ad hoc reports through a graphical user interface. When creating custom reports, the end user shall be able to select the database fields, including user defined fields, for inclusion in reports. For filtering time and date, the custom report writer shall allow entry of relative time and dates such as, "last week, last day, last 60 days," up through one (1) year.

3. The system shall produce reports based on:

    a. Event data.

    b. Personnel data.

    c. System configuration data.

    d. Hardware failure events.

4. The system custom report writer shall allow for selection of devices to be reported on. The report shall include specific events and have filters for selection of personnel.

5. The system shall save custom reports for later reuse, and be printable, to a .pdf file, or exported to MS Excel in a grid (columns) format.

5.4.5. Video Integration Requirements

The system shall be able to integrate video as outlined:

1. Network level Integration with one or more Network Video Recorder (NVR), Digital Video Recorder (DVR), and/or Video Monitoring System (VMS) products.

2. Ability to view live video from internet protocol (IP) Cameras through the web based Graphical User Interface (GUI).

DRAFT

3. Integrate real time IP, DVR, and NVR cameras with stored video replay for events.
4. Real time video monitoring displays, including multiple cameras simultaneously.
5. Images and video be downloadable to a DVD, CD, or other portable/transferable media.
6. Integration with NVR/DVR/VMS products supporting motion detection and video loss to generate system alarm events.
7. Maintain data in the system for at least 30 days.
8. Recall of photo ID and real time image for comparison.
9. View video through a web browser interface.
10. System user permissions to grant whole or partial access to system cameras and video resources.
11. Integrate alarm inputs form the video system.

5.4.6. Access Control Panel (ACP) Requirements

1. The ACP shall be a microprocessor based access control and monitoring panel that serves as the data collection and communications interface between the PACS application and the various field devices, such as card readers, alarm inputs, and control outputs. The ACP shall also be implemented as a single door edge device.
2. The ACP shall have battery backup for uninterrupted, on-line operation for a minimum of four operational hours, in case of ac power loss. The battery shall meet all applicable safety standards.
3. The ACP shall support at least 32 access codes.
4. The ACP shall comply with Underwriters Laboratories (UL) 294 - Standard for Safety Access Control System Units.
5. Shall provide diagnostic status lights for:
    a. Operational status of the ACP.
    b. Relay output status.
    c. Communication will be operational Ethernet interface.
    d. Internal diagnostic/system configuration.
6. The ACP shall make authorization decisions and allow or deny access within 250 milliseconds of receiving a credential from a reader.

DRAFT

7. The ACP components shall be housed in a tamper-proof case enhanced with alarm monitoring features.

8. Provide for protection of Personal Identifiable Information (PII) contained in a PACS. See NIST SP 800-57, Parts 1 and 2.

6. READER REQUIREMENTS

Readers shall support the following protocols: Wiegand (DO/D1), magnetic stripe (CLK/Data), RS232, and RS-485 communications with future TCP-IP support.

6.1. Card Reader Requirements

Readers shall be interoperable with other required components including, CAK Authentication, Certificate Validation, CHUID Authentication, PIV Authentication, and Caching Status Proxy from a variety of sources. Card readers shall support or be field upgradable to support industry standard protocols (eg: OSDP) that will allow for future interoperability.

Readers shall minimally have the following characteristics:

1. Compatibility with the existing FPS inventory of PIV cards (III, IV and V).

2. Ability to perform challenge response (CAK/PKI) or the ability to add this capability in the future.

3. Ability to perform PKI Authorization, Bio functions (fingerprint or iris scan), or the ability to add in the future (e.g. sidecar) without full reader replacement.

4. Ability to pass the entire FACN or GUID without truncation.

Readers/writers shall be provided where shown on the drawings.

Credential reader/writers may be "single-Package" type, combining controller, electronics, and antenna in one Package, in the following configurations:

1. All/any network cabling shall be orange with all fully meeting manufacturer requirements.

2. Mullion mount Reader/Writer, Mullion mount Reader/Writer + PIN, and Mullion mount Reader/Writer + Biometric fingerprint scanner. All models shall be able to mount to “single-gang” electrical boxes using an optional Single-Gang Mounting Kit.

3. All exterior readers shall be PKI-CAK +PIN to PACS on any DHS/FPS-designated secure areas, Maturity Level 2, as outlined indicated in the Selecting PIV Authentication Mechanisms for Physical Access Control, The installation will be consistent with NIST SP-800-116.

DRAFT

4. All interior readers shall be proximity 13.56 khz (contactless) only, unless space/equipment requires higher level access and then a two (2)-factor contact reader will be required.

5. Unless otherwise indicated for ADA or other special requirement the reader shall be mounted at 42 inch AFF (bottom of reader) with protective/insulated plate between reader and wall/junction box.

6. Multi-technology capable of reading all technologies and compatible with new system design as certified by the manufacturer and listed as a FIPS 201 certified product (unless included within "end-to-end" package solution on revised APL 2.0) on the GSA Approved Products List.

7. The reader/writer shall be of potted, ABS material, sealed to a rating of (IP67).

8. The reader/writer shall comply fully with ISO 14443 parts 1, 2, 3 and 4 open card standards to fully enable interoperability among suppliers of similar products

9. The reader/writer shall conform fully to ISO 14443 Part 3 - Anti-collision and Transmission Protocol and shall be capable of identifying multiple credentials in a single field.

10. The contactless reader/writer shall have an approximate read range of one(1) inch to two (2) inch when used with ISO 14443 access control badges.

11. The reader/writer and card shall use challenge response mutual authentication.

12. The reader/writer shall be capable of reading access control data from any ISO 14443 compliant contactless credential, and transmitting that data in Wiegand format and RS485.

13. The reader/writer shall be capable of reading the card serial number (CSN) and/or, a permanent, unique identification number from any 15693 credential, and transmitting that data in Wiegand format.

14. The reader/writer shall be capable of reading and is dependent upon security of the data, Privacy Officer approval and acceptance of engineering costs, from the card a profile unique to the card owner which can then be transmitted to third-party building and business systems. Profile information shall be securely separated from all user PII data but may contain information related to a user's work space, assigned work area, etc. which can then be used by third-party business and building systems to alter the building space based on the profile of the user. An example application would be a user's work space location preference, lighting set point preference and temperature preference that can then be stored on the card and then shared with hoteling space management software as well as building automation systems.

15. The reader/writer shall be capable of writing to any ISO 14443 compliant credential.

DRAFT

16. The reader/writer shall have separate terminal control points for the light emitting diode (LED) and for the audible indicator.

17. The reader/writer shall have multiple LEDs for increased visibility.

18. In addition to being listed on the DHS/FPS Approved Products List, all readers shall be FIPS 201 compliant.

19. DHS/FPS is standardized on reverse 64-bit encryption.

20. The reader naming convention shall be as follows:

    Example: R08 CO0514 A0102-XXXXXXXXXXXXXXX

    R08 = Regional Designation (RXX)

    CO0514 = State and Building Number

    A01 = A-panel (to be sequenced (AXX)

    02 = Second Reader on the Panel (XX)

The following sections establish requirements for peripheral hardware connected to the PACS.

DRAFT

7. DOOR STRIKES

1. Construction: Stainless steel, tamper resistant, internal solenoid.

2. Opening Force: 1,900 pounds.

3. Operation: Field reversible, plug-in connectors.

4. Solenoid: Internally mounted to facilitate electric strike installation in hollow metal, concrete filled, and aluminum and wood jambs.

5. Solenoid: Operated by direct current to provide silent operation.

6. Electric Strike: Capable of operation with less than 30 pounds of force against keeper.

7.1. Magnetic Door Contact

The contact shall be designed specifically for use in steel and wooden doors. The unit shall offer a sealed unibody construction, with flexible ribbed sides for quick secure installation without gluing. The electronic strike and magnetic lock shall provide remote release of a locked door or gate. All interior card reader doors (except stairwell doors) shall be fitted with fail safe hardware complying with all applicable safety standards. Configuration:

1. Contain hermetically sealed magnetic reed switch.

2. Unobtrusive, flush with surface of doorframe and door.

3. Contact and Magnet Housing: Snap-lock into 3/4 inch or one (1) inch diameter hole.

4. Color of Housings: Choose to match color of door frame.

5. Snap-lock insulation bushing for tight fit.

6. Overhead door contact shall be designed with a low profile heavy cast aluminum housing with a wide operating gap of up to three inches.

7.2 Door Hardware, Locksets, Etc (if required).

1. Locksets shall be able to withstand 3,000 inch pounds of torque applied to the locked lever without gaining access.

2. Locksets required for fire doors, shall be listed by Underwriters Laboratories for ratings of A (3-hours) label.

3. Lockset levers shall be made of solid material with no plastic fillers

4. Latchbold head shall be one piece stainless steel

5. Latchbold assemblies shall be encased within the lockbody

6. Lockset shall be a storeroom/closet or asylum function as specified by the government.

DRAFT

7.3 Emergency/Panic Bar (if required)

The emergency/panic bars shall meet the following criteria:

1. The push pad on a panic bar must be at least half the width of the door itself.
2. The center of the push pad shall be 41 inches above the floor.
3. The finish on this and all door hardware shall match the existing architectural finishes.
4. The vendor is responsible to test the push pad to ensure it is functional.
5. The hardware to operate the emergency/panic bar shall require no more than of 15 pounds of force and no less than 5 pounds of force to operate.
6. Fail secure electric strikes shall be used on fire doors unless otherwise requested by the government.
7. Electromagnetic locks shall release by a sensor or by a switch in the panic hardware.
8. Shall be designed to withstand high impact application and high level of useage without causing any mechanical or asthetic decline in performance or appearance.
9. Shall work flawlessly with the installed physical access control system (PACS) hardware.

10. Shall be capable of accomodating a fail safe or fail secure status in the event of a fire emergency. The settings for fail safe or fail secure shall be determined by the government.
11. Shall be Builders Hardware Manufacturers Association (BHMA) certified to ANSI A156.3 (American National Standard for Exit Devices) for Grade one (1) exit devices and comply with NFPA life safety code.

8. REQUEST TO EXIT SENSOR

Description: The sensor shall detect motion in its established coverage area and signal the ACP to either unlock a door or shunt door contact associated with coverage door.
Configuration:

1. For single or double door use.
2. Wall and ceiling mountable.
3. Operate on 12 or 24 VAC or DC.
4. Up to 60-second adjustable latch time.
5. Include selectable relay trigger mode.
6. Selectable fail safe/fail secure mode of operation.

DRAFT

8.1. Video Intercom with Door Release

1. The PACS solution shall be designed to incorporate video intercom door and master stations to unlock a secure door/barrier/turnstile or gate.

2. Video intercom door stations and master/submaster shall be installed in areas specified by the customer and allow the remote release of select doors.

3. The release shall be connected to the door in a manner that works flawlessly with the physical access control system (PACS) to ensure persons operating the switch can remotely allow access to persons as needed.

8.2. Egress –Reading card on exit

In all facilities, in which optical turnstiles exist or are installed, it will be required that personnel exiting the facility, except during a fire (or other life safety event), validate and read their credential at the turnstile for egress. This allows for accurate population count within the facility and constitutes as an electronic “sign in/out” log after normal business hours (Federal Management Regulation; 41 CFR 102-74.375).

9. Key Personnel

The Government has identified the Contractor's Program Manager as Key Personnel.

9.1. Project Manager

The Program Manager shall have a minimum of six (6) years of experience with supervising and managing technical teams and projects of similar nature to that described within this statement of work. Education shall be at the Bachelor degree level or higher. **The contractor shall not remove or replace key personnel until the contracting officer approves the change.**

10. REPAIR AND MAINTENANCE

The Contractor shall provide all labor, services, parts, supplies, packaging, and shipment of items necessary to check the overall functional operation of the PACS system and to accomplish the scheduled maintenance tasks required.

Annual Maintenance (AM) scheduled visits shall include one (1) annual inspection and a corrective maintenance session. Preventive Maintenance (PM) scheduled visits shall include semi-annual visits per site and warranty repairs as well as any and all calls for service. The Contractor shall coordinate with the MegaCenter's point of contact.

10.1. Annual Maintenance

Each annual visit shall include:

- Check whether staff has experienced any problems with the system.
- Check mains and stand-by power supplies including charging rates.
- Check operation of all door contacts.
- Check operation of "door ajar" sounders.
- Check operation of locks/strikes.
- Check operation of door closures.
- Check operation of emergency break glass/mechanical exit.
- Check operation of readers.
- Apply any firmware updates available for and approved by DHS/FPS to readers
- Check operation of keypads and LEDs.
- Check communications with all controllers and reset error log.
- Check operation of Input / Output controller.

DRAFT

- Check access control software.
- Check door open times.
- Back-up historic data and database. Ensure the MegaCenter keeps this in a secure location.
- Verify correct operation of doors in a fire condition.
- Carry out minor adjustments.
- Provide answers to any questions or queries the MegaCenter may have.
- Check installation against records, record and report any discrepancy.
- Check inbuilt diagnostics and history file for any error and fault messages.
- Check and test the operation of all peripheral devices to ensure alarms are registered at the operator station.
- Check operation of all control equipment.
- Check and test the operation of every audible, visual alarm and warning device.
- Check the operation of all activating outputs which respond to an alarm condition.
- Check, in cooperation with the monitoring station, the operation of any communication equipment.
- Check system voltage under full load conditions with the mains supply OFF for not less than 10 minutes.
- Ensure that the output under such conditions of all standby batteries and power supplies is not less than 95 percent of rated voltage.
- Check and record charger output voltage to battery.
- Check back-up power supply:
    - terminals for tightness, cleanliness and corrosion.
    - enclosure for cleanliness and corrosion.
- For microprocessor based systems check:-
    - on board battery, replace if passed use by date.
    - clock setting.

Check the condition of all equipment for damaged, stressed or heated components.

DRAFT

10.2. Preventative Maintenance:

Each semi-annual visit shall include:

1. The Preventative Maintenance visits shall be scheduled at a mutually agreed time, or combined with an unscheduled service visit performed within 15 calendar days of that scheduled PM.

2. Requests for services will be dispatched by the Contracting Officer's Representative (COR).

3. Preventative maintenance shall be conducted during normal business hours, from 8:00 a.m. to 4:30 p.m. local time (excluding Federal holidays). The COR or authorized FPS Technical Representative will ensure that the system is available for inspection/maintenance.

4. The Contractor shall provide a five (5) year preventive maintenance plan and an extended optional maintenance plan for each system provided under this procurement

5. "Wear & Tear" items that appears to be wearing and needs replacing will proactively be replaced during a Preventive Maintenance (PM) or Corrective Maintenance (CM) service call. All "Wear & Tear" services performed in accordance with the contract guidelines shall be done at no additional cost to the Government. The Government will provide approval for all wear and tear repairs/replacements outside of the scope of this Statement of Work (SOW).

6. The correction of System damage due to unauthorized maintenance performed on the PACS system may result in additional time and material costs.

7. The Contractor's preventive maintenance plan shall incorporate examining, calibrating, cleaning, lubricating, testing, and adjusting the equipment, and as conditions warrant, repairing or replacing equipment included under the contract in accordance with Original Equipment Manufacturer standards.

10.3. Work Not Covered by Warranty:

1. The maintenance service will not cover force majeure events, including but not limited to:
   - Acts of God.
   - Acts of War.
   - Acts of Invasion.
   - Acts of Foreign enemy.
   - Acts of a Public enemy.

DRAFT

- Acts of the government in either its sovereign or contractual capacity.
- Acts of hostility.
- Terrorist acts.
- Civil war.
- Rebellion.
- Fires.
- Floods.
- Epidemics.
- Quarantine restrictions.
- Strikes.
- Freight embargoes.
- Unusually severe weather.

2. The Contractor shall be paid separately for, labor services and costs to perform repair/replacement of failed materials, when the aforementioned is due to:

- Malfunctions caused by negligence, transportation between sites.
- Malfunctions caused by improper manipulation by FPS users.
- Properly dispose of waste and any materials replaced during maintenance of the system.
- Failure of electrical power.
- Any possible additions to the system(s) required by the user, not approved by the Contractor.
- Improper manipulation by the user or by the user's assigned personnel or by third-parties not assigned or authorized by the Contractor.
- Tampering or deliberate or involuntary attempts at manipulation.
- Repairs or attempted repairs by user or by third-parties not designated or authorized by the Contractor.

Due to the critical nature of the Security Management System (SMS) protecting FPS's information, facilities and personnel the continued operation of these systems is required. The Contractor shall propose a maintenance plan for the SMS providing routine and emergency support. The Contractor's maintenance plan shall include a

DRAFT

full time SMS administrator. The Contractor proposed maintenance plan shall be broken down into one base period and four option periods, totaling a coverage period of five (5) years.

In the performance of SMS maintenance the Contractor will be required to restore SMS operations within two (2) hours for level one issues, six (6) hours for level two issues, and 24 hours for level three issues. FPS will identify the level of the issue at the time of notifying the Contractor of the problem. The Contractor is required to identify in their proposal a primary and alternate point of contact that will receive SMS issue notifications 24 hours a day, seven (7) days a week, every day of the year.

The Contractor's Maintenance Plan shall include SMS equipment replacement costs and hourly labor costs for installation for non-warranty items. In performance of the Contractor's Maintenance Plan the Contractor shall be required to perform operating system patches and updates as prescribed by FPS. In performance of the Maintenance Plan the Contractor shall provide and install all SMS software and firmware updates from the manufacturer. In performance of the Maintenance Plan the Contractor shall provide and install SMS operating system software and hardware updates prescribed by FPS. For this requirement the Contractor is responsible for seeking the SMS manufacture's concurrence that the SMS operating system software and hardware updates prescribed by FPS will not negatively impact SMS operations.

Maintenance and repairs must be performed during the hours of 8:00 a.m. to 4:30 p.m. (local time), Monday through Friday (excluding Federal holidays with COR concurrence).

The Contractor must respond to verbal or written service requests from the authorized ordering official at the FPS location responsible for the MegaCenter where the PACS is located.

"Response" to a service call is considered to be verbal instructions provided over the telephone by a qualified technician system administrator which details the procedure for restoring full operational status of the PACS, or the arrival of a qualified technician at the site where service is being requested, to evaluate and affect the repair. Any actions taken by the PACS Administrator at the request of the Contractor must be at the Contractor's risk.

The Contractor must maintain a maintenance log to catalog all service requests, the action taken, time expended, date completed and the name of the technician who completed the service call. The maintenance log must be made available to the CO and COR upon request.

The Contractor must provide a toll free customer support telephone services to receive routine and emergency service requests, and coordinate service technician response. The Customer Service representatives must be available during the hours of 8:00 a.m. to 4:30 p.m. locally, and fluent in English as spoken in the United States, including common terms and idioms used in the access control business.

DRAFT

10.4. EXTENDED WARRANTY

The Contractor must provide an extended warranty.

Scope: This option would be executed to meet operational requirements.

1. The Contractor shall provide all services, parts, supplies, packaging, and shipment of items necessary to diagnose and correct malfunctions or failures of the PACS system, upon request.

2. Corrective maintenance services shall provide diagnosis within one hour of FPS reporting an issue. "Wear & Tear" items shall be addressed and corrected during the scheduled maintenance visits after Government approval.

3. Parts replaced during corrective maintenance will become the property of FPS.

10.5. PROGRAMMING AND ACCOUNTABILITY

DHS/FPS requires that a single person(s) provide all naming conventions, DHS/FPS network configuration (in collaboration with DHS/FPS OCIO) and PACS specific programming (access categories, door programming, etc.) for every facility. The person(s) responsible for the programming/configuration shall have experience in 30 or more DHS/FPS facilities (single facility of 200,000 square feet (sf) or larger), 50 or more doors, be in possession of a DHS/FPS PIV card and have DHS/FPS network access.

DRAFT

11. PERIOD OF PERFORMANCE

The period of performance is for 90 days after award but no later than 120 days for installation and acceptance. The manufacturers warranty shall start the dtate of acceptance and there will be four additional one-year maintenance option periods.

12. EMPLOYEE IDENTIFICATION

12.1. On-Site Contractor Employees

Contractor employees visiting Government facilities shall wear an identification badge that at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

12.2. Employee Conduct

Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when

visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security.

13. MATERIALS

Materials are to be provided by the Contractor when essential to the performance of the SOW and specifically approved by the COR. All materials purchased by the Contractor for the use or ownership of the Federal Government become the property of the Federal Government. The Contractor shall document the transfer of materials in the monthly progress report as a result of meetings or work being completed.

14. SUBMITTALS

All submittals shall be accurate and delivered in a timely manner.

Additionally, a file of system documentation at the project site shall be maintained throughout the course of the work. Such file shall be updated with new information as equipment is received and installed. System documentation shall be available for inspection by Contracting Officers Representative (COR) as required.

The following submittals are required:

1. Project Schedule and Log.
2. List of all proposed products and product data sheets.
3. Shop Drawings, including data on custom-fabricated components. Drawings shall include elevations and section details of all installed devices and features.
4. Test Reports.
5. Certification that all relevant equipment is FIPS-201-1 compliant and is listed on the DHS/FPS APL.
6. Operation and maintenance manuals for all equipment and software.
7. Project Record Documents in AutoCAD 2010 (uploaded into PACS).
8. Notations reflecting as-built conditions of any additions to or variation from original drawings.
9. Accurately show the physical placement of the following:
    a. Location and identification of distribution cabinets and of equipment located inside cabinets and equipment rooms.
    b. Junction and pull box locations.
    c. Schematic drawings of installed devices.
    d. Routing of cable and termination information.
    e. End-of-line resistor locations.
    f. Interfaces to external equipment.
    g. Connections to power and telephone circuits.
    h. Location of servers.
    i. Conduit runs.
    j. Conduit (minimum 3/4 inch).

DRAFT

10. Complete listing of pair assignment records for copper wiring, optical fiber cabling and coaxial cabling.
11. Optical Fiber Cable Records: Include strand allocation, test results, and identification of media and protocol used.
12. Project record drawings showing wire and cable runs, zone numbers, tamper circuit configuration, panel/circuit breaker numbers from which equipment is powered, and splice points.
13. Project Record Drawings submitted on CD utilizing AutoCAD 2010.
14. Upon completion of work, and prior to final acceptance, contractor shall prepare and submit to (Client) Project Manager three (3) sets of system documentation.
15. Incorporate "as built" complete diagrams as part of the final system (product loaded into administrative area of the system).
16. Documentation of data points made available in the system.
17. Documentation of communications and methods for integration with third-party building and business systems.
18. Documentation on PACS dependent sequence of operations to achieve an Integrated Systems Sequence of Operations (ISSO) for the facility.

DRAFT

15. EXECUTION

The Contractor is to provide a turnkey solution including all labor and material necessary to complete the PACS system.

The contractor is required to have the system fully installed and accepted no later than 120 days from award.

The contractor is responsible to deinstall and dispose of all existing PACS components as required by the government.

The contractor shall repair/patch all holes,scrapes,mars and other damage to walls, doors etc. resulting form the removal and installation of PACS components and wiring.

The contractor is responsible to ensure all door handles and door hardware match the existing design.

The contractor is responsible to ensure all doors open an dclose smoothly and security upon completion of the installation of new PACS equipment.

Wiring for all PACS devices shall be tamper resistant. Wiring for all PACS field devices shall not be exposed (i.e. shall be internal to a secure space wall, ceilings, doorframes, etc.) upon installation. Wiring for all PACS components should remain within FPS space to the fullest extent possible. When it is not feasible for wiring to remain internal to FPS space the contactor shall provide a tamper resistant or conduit solution. Approval by the COR is required for any wiring to be placed external of FPS controlled spaces. The Contractor shall securely fasten all PACS wiring above drop ceilings to provide adequate support in an approved method and per prevailing electrical code(s). No wiring may be directly in contact with acoustical ceiling tiles. The Contractor may not abandon any

wiring in the ceiling per the applicable fire code. When replacing existing security system wiring the Contractor shall remove abandoned PACS wiring in the ceiling per the applicable code. Line security to end devices shall be implemented through End-of-Line resistors installed at the device. Line security from the PACS head end to the access control panels shall be by encryption.

High security screws shall be used for all PACS components that are exposed (i.e. can be viewed externally or are not secured behind a face plate).

The contractor shall not leave any wiring exposed either inside or outside the FPS space.

All wiring shall consist of a single, unbroken run that is free of splices and T-Taps. All wiring shall be labeled at both ends using a numerical system to allow for identification. The wire labeling configuration shall be called out on the as-built PACS drawings to be provided. The Contractor will patch and paint any holes and make any repairs to any surface (i.e. walls, doors, ceiling, etc.) that is the result of the Contractor's work. Repair work shall match existing construction in grade and likeness.

The Contractor is to provide and install all equipment associated power for PACS operation.

DRAFT

16. QUALITY ASSURANCE

16.1. Manufacturer Qualifications

All personnel shall be fully trained, factory authorized, and certified for installation and service of equipment provided.

16.2. Installer/Integrator Qualifications:

1. Certified as an HSPD-12 service provider in accordance with the APL managed by DHS/FPS (Schedule 70 or 84), trained and certified by electronic security equipment manufacturer, and strictly adheres to the engineering, installation and testing procedures in accordance with the requirements of DHS/FPS, and equipment manufacturer(s).

2. The Installer/Integrator shall utilize authorized manufacturer components and distribution channels in provisioning this project.

3. The Installer/Integrator shall be experienced in electronic security work and the ability to demonstrate direct experience on recent systems of similar type and size.

4. The Installer/Integrator shall own and maintain tools and equipment necessary for successful installation and testing of PACS.

5. The Installer/Integrator shall employ a full-time Project Manager. The Project Manager shall:

    a. Be Installer/Integrator's representative and speak for Installer/Integrator.

    b. Make any necessary visits to construction site to determine progress of construction and be available to resolve contract issues with the DHS/FPS COR.

Per the IDManagement.gov site, that there are three primary components *required* by GSA to maintain compliance for the installation and integration of an approved FICAM PACS solution:

1. "Qualified HSPD-12 Service Provider" Approved Company (GSA IT Schedule 70 with SIN 132.62. (Reference to *IT Schedule 70 - SIN 132 62*),
2. Qualified Personnel (CSEIP), and
3. Products must be listed on the GSA Approved Products List (APL). https://www.idmanagement.gov/IDM/s/article_detail?link=list-of-certified-services

6. Project Meetings:

    a. Pre-Construction Meeting: Attend meeting when requested by CO or COR. Come prepared with questions and proposed resolution to questions about the PACS.

    b. Progress Meetings: Attend weekly progress meetings as requested by the CO or COR. Come prepared with questions and proposed resolution to questions about PACS in question.

Note: Any contractor or sub-contractor working on any DHS/FPS installation shall at a minimum, meet the following requirements:

a. Any person(s) working in or around a DHS/FPS facility shall be in adjudicated and have received a final favorable determination from the Department of Homeland Security/Federal Protective Service.
b. Any person(s) working in or around a DHS/FPS facility shall be in possession of or have been sponsored for a DHS/FPS Access Card (GAC)/PIV.
c. Any person(s) installing the PACS equipment shall be certified by the manufacturer for installation, service, maintenance/repair (documentation to be supplied).
d. Vendor/contractor shall have previous experience installing selected system in more than 30 Government facilities that are at least 200,000 sf, 75+ readers, multiple door and hardware/locking mechanism types and the facility has to have a Facility Security Level of 3 or greater.

DRAFT

16.3. Use of Design Intent Documents

1. Diagrammatic Drawings:

    a. Due to small scale of drawings, it is not possible to indicate offsets, fittings, changes in elevation, etc. Prior to rough-in, verify exact locations for installation with field measurements and with equipment being connected.

    b. If field conditions or equipment require significant change to original documents, contact CO or COR before proceeding.

    c. Exact locations of equipment and fixtures subject to approval of COR.

2. Omissions from diagrammatic drawings or specifications, or incorrect description of details of work which are necessary to carry out intent of drawings and specifications, or which are customarily performed, shall not relieve contractor from performing such omitted or incorrect described detail of work.

3. Review of Contract Documents: All dimensions on contract documents shall be verified. This includes the location of work and its relation to existing work and current conditions.

4. Coordination: All work is to be coordinated with the individuals responsible for maintaining fire alarms and other life/safety equipment, the Local Area Network (LAN) Manager, and local Property Manager.

    a. This coordination may include additional meetings with representatives of DHS/FPS, as specified above, including the COR.

    b. The contractor will record agreements reached between DHS/FPS representatives and/or COR, CO, and forward this record to the COR for concurrence prior to distribution to other participants.

    c. Where there are updated adjustments/modifications, all drawings will be updated specifically detailing proposed modifications to architectural, mechanical or electrical facilities.

5. Methods of construction not specifically described or indicated in contract documents will be subject approval of COR or authorized Technical representative.

16.4. Delivery, Storage, Handling and Work Schedules

1. Cable Storage: Do not roll or store cable reels without appropriate underlay.

DRAFT

2. Pre-installation Inspection: Visually inspect all PACS equipment, and shipping cartons to detect possible damage incurred during shipping and transport.

3. Visibly damaged goods will be replaced at no additional cost to DHS/FPS.

4. For areas with other ongoing projects, installation will be coordinated with the COR or authorized FPS representative. All drawings will be updated detailing proposed modifications to architectural, mechanical or electrical facilities.

5. In an effort to make portions for the project available to DHS/FPS as soon as possible, work schedules may be adjusted with the agreement of the COR.

16.5. Field Quality Control

16.5.1. Site Tests & Inspections

Inspections and tests will be conducted by the COR or authorized FPS technical representative.

a. The Contractor will be responsible to assist the COR or authorized FPS technical representative with these functionality and performance tests.
b. Failure of the PACS or any subsystem to perform as specified will be construed as a failure to comply with requirements of contract.

16.5.2. Demonstration and Instruction: Include, but not be limited to:

- Physical review of installed cable plant.
- Review of cable plant documentation and test results.

ONLINE WEB-BASED SERVICE AND MAINTENACE PORTAL

1.0 SUMMARY

Provider shall supply a web based user portal to provide real time information on service work orders, reporting and access to an information repository. Portal shall not require use of a prescribed web browser or downloading of a proprietary application.

2.0 FUNCTIONALITY

2.0.1 WORK ORDERS

1. System shall enable the user to create preventive or demand service work orders from one location for all facilities
   - Ability to select work order priority and required response time.
   - Display site requirements specific to each individual site/location

2. System shall provide for real time update of work order information and status

DRAFT

3. Work order history shall include real time stamps of work order activity (including date and time), description of work performed, parts ordered and invoicing and billing summaries

2.0.2 REPORTING

1. The System must have the capability to enable the user to request reports by building, campus or all locations

2. There shall be three (3) types of reporting – Metric, Service Spend and Status Reports
   - Metric reporting – quantitative measurement of response to user defined SLA (service level agreement). Reporting period shall be monthly and include 12 months from current month. Metrics shall reflect results for all priorities of work orders and include:
     a. Measurements of % time specialist arrived on site within SLA
     b. Average hours to on site from time work order was created
     c. Average days to finish work order
   - Service Spend - Reporting period shall be monthly and include prior 12 months from current month. Information shall include total value of invoices, number of invoices and average spend/invoice
   - Status Reporting - shall be updated real time to reflect changes to the work order status. From all status reports shall have the ability to link to view work order information. Report information shall include the following:
     a. Time service request is received
     b. Time of service dispatch to technician
     c. Time technician departs for customer site
     d. Time of arrival on site
     e. Technician notes identifying action taken and resolution, and any outstanding issues
     f. Time of completion
     g. Time Technician departs site
     h. Work order status – open/dispatched/en route/on site/parts on order/awaiting customer action/finished

   Multiple status reports shall be available including:
   - Work Order Summary – historical listing of all created work orders, status time stamps and problem resolution.
   - Open Work Order- listing of all open work orders, current status, problem definition and resolution.
   - Work Order History by Site – All work orders for selected building(s) and timeframe. Ability to link to work order from report
   - Work Order History by Equipment – All work orders for selected piece of equipment for defined building(s) for specified time period. Ability to link to work order from report

DRAFT

2.0.3 INFORMATION REPOSITORY

1. Without exiting the user portal, provide web access to a file sharing application providing the ability to:
   - Without limitation to file type, upload and edit all files
   - Read files posted by others
   - Provide viewing and collaboration by multiple simultaneous users

3.0 SECURITY

1. All customer data must be protected through a documented security structure that includes the following elements:

   - Data transmission protection through 256 bit encrypted SSL certificate
   - Unique user combination email/password to access portal
     - Each user is assigned:

       a. Access –buildings user can be assigned permissions. Ability to set access from one building to any combination of buildings including all buildings

       b. Permissions – topics within iCare user has the ability to perform functions for defined access

     - Hardware and software based intrusion detection, network monitoring and policy based procedures.

DRAFT

17. BACKGROUND INVESTIGATION/CONTRACTOR FITNESS REQUIREMENTS

The Contractor shall submit to FPS the following documentation for all initial non-cleared employees involved on this contract (including owners, management, supervisors, reserve workforce personnel, etc.) within five (5) days but no later than 10 business days after the date of award. Documentation on all replacement employees shall be submitted to FPS no later than 14 calendar days prior to their start work date. FPS shall provide all forms upon request after contract award. All forms shall be filled in using a typewriter, completed on a computer, or by means of ballpoint pen. Forms shall be legible and completed using black ink. All security requirements shall be provided by and coordinated with the FPS CO and/or COR. FPS shall inform the contractor when all security are met.

The Contractor shall submit two (2) fully completed FD-258 Fingerprint Cards. Forms shall be legible, completed using black ink, and signed by both the applicant and the person who took the prints. Fingerprints are required for all applicants.

All application packages require a Contractor Information Worksheet (CIW).

FPS will process a National Agency Check with inquiries (NACI) or a six (6) month Temporary Law Enforcement Check (LEC) depending on the job requirement.

For an LEC, the contractor will provide the CIW, and OF-306 and the Addendum form filled out as required.

For a NACI, FPS will process an Electronic Questionnaire for Investigations Processing (e-Qip) case, and "invite" the applicant via e-Mail notification to complete an SF-85 application online. Instructions on where and how to access the website will be provided. The OF-306 shall also be completed. After the applicant has completed the SF-85 online application, the contract company shall hand carry or mail FPS a CIW, or OF-306, signature pages from the electronic SF-85, and fingerprints for each applicant.

Forms shall have original signature date, copies will not be accepted. If there is not enough room on the form, an additional sheet can be attached indicating what section is being addressed.

All forms can be submitted in person or mailed to:

This will be the COR and the COR will be responsible to send the documents to DHS HQ for processing.

DRAFT

18. PHASING REQUIREMENTS

Within 10 days of award, the Contractor shall provide a phasing plan for the project, which will address accessibility and timing of demolition and construction. This phasing plan shall be submitted in writing and approved by the contracting officer and Project Manager or COR.

Disruption to traffic flow and accessibility shall be minimized at all times. Any disruption to traffic flow shall be coordinated with the COR 48 hours in advance.

19. TRANSITION TO NEW PACS

All work is to be conducted in a seamless and non-disruptive manner.

Contractor shall provide advance notice in writing to the Project Manager and COR. The COR will establish a date and time for system cutover. The selected date and time will be after normal business hours to ensure the least disruption to building occupants.

Contractor will provide the necessary technical personnel onsite to assist with legacy system deactivation, PACSS activation, and any other issues.

The existing PACSS may only be phased out provided the Project Manager receives an approved phasing schedule. 72 hours advanced notice is required for any transition.

The existing PACS will be shut down only when the contractor communicates, in writing, that the new PACS is ready to be deployed and has certified HSPD-12 compliance. For existing reader locations, down time will not exceed three (3) hours during normal business hours or may require overtime. Overtime costs shall be at the expense of the Contractor and at no additional expense to the Government.

20. ACCEPTANCE

1. The Contractor should begin the installation no later than 60 days After Receipt of Order (ARO), and shall have the work complete and system ready for testing and acceptance as identified in the individual site delivery orders. The Contractor shall coordinate daily work hours with the DHS/FPS Project Manager. The Contractor shall coordinate daily work hours with the DHS/FPS Project Manager and the FPS Technical Representative. Any technical questions regarding the installation of the system or its technical operation should be directed to the DHS/FPS Project Manager and/or the FPS Technical Representative.

2. After all work is completed, contractor and COR or authorized FPS Technical Representative shall conduct a final inspection and pre-test all equipment and system features. Written notice of the pre-test shall be provided to the DHS/FPS Project Manager and COR or authorized FPS Technical Representative and approved prior to testing. Contractor shall correct all identified deficiencies discovered as a result of the inspection and pre-test.

3. Contractor shall submit a request for an acceptance test, in writing, to the DHS/FPS Project Manager and COR or authorized FPS Technical Representative upon determining equipment is operational. The request for acceptance test shall be accompanied by certification from contractor that all deficiencies identified in the pre-test have been corrected, if any.

4. During the acceptance test, contractor shall demonstrate all equipment and system features to DHS/FPS.

5. If, at the conclusion of the acceptance test, all work is found to be acceptable and in compliance with the requirements, the DHS/FPS project manager will issue a letter of acceptance.

DRAFT

21. POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than five (5) business days after the date of award. The purpose of the Post Award Conference (PACS), which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract and review the Contractor's Submittals Draft Plan.

22. PROGRESS MEETINGS

The Contractor's Project Manager shall meet with the COR and other agency personnel on a weekly basis to discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall be held at the MegaCenter. The Contractor shall provide meeting minutes within two (2) business days of the progress meeting that will include:
1) Description of work planned during the past week.

2) Description of work accomplished.
3) Analysis of the difference between planned and accomplished work.
4) Work planned for the following week.

23. PACS EQUIPMENT AND PROCEDURE FAMILIARIZATION

The Contractor shall provide the coordination, creation, and facilitation of one (1) training session for FPS personnel in accordance with the equipment operational capacity based on manufacture recommendations. Equipment and procedure familiarization content and format shall be FPS-specific based upon workflow, number of trainees, and accreditation requirements.

Specific task activities include but are not limited to:

- Development of a equipment and procedure familiarization curriculum and plan for familiarizing staff to operate the PACS
- Development of a equipment and procedure familiarization curriculum and plan for training staff to do System administrations for the PACS.
- Development of equipment and procedure familiarization schedule for designated sites in conjunction with FPS workflow.
- The execution of equipment and procedure familiarization following equipment installation at each location.
- The creation of appropriate equipment and procedure familiarization leave-behind materials including but not limited to user manuals, reference guides, operating instructions, support procedures, and DVDs.

24. GENERAL REPORT REQUIREMENTS

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with Windows XP and Microsoft Office Applications.

25. POINTS OF CONTACT

Contracting Officer's Representative (COR)
NAME-TBD
DUTY STATION
FULL ADDRESS
Phone: XXX-XXX-XXXX
E-mail: _____@fps.dhs.gov

Contracting Officer
NAME-TBD
DUTY STATION
FULL ADDRESS
Phone: XXX-XXX-XXXX
E-mail: _____@fps.dhs.gov

DRAFT

26. GOVERNMENT FURNISHED EQUIPMENT (GFE)

The existing employee PIV credentials are the only GFE on this SOW.

27. SECURITY SENSITIVE INFORMATION (SSI)

The information in this SOW (including any attachments) may contain confidential and/or law enforcement sensitive (LES) information intended for a specific individual and purpose, shall be considered For Official Use Only. (FOUO) DHS 11042.1 (03/05). You are hereby notified that any dissemination, distribution, or copying is strictly prohibited. At a minimum, the information herein shall be disseminated on a "need to know" basis and when unattended, shall be stored in a locked container or area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure. The Contractor shall not retain sensitive documents such as schematics, blueprints, diagrams, photos, videos etc. All documents supplied to the Contractor, by the government for planning and bidding purposes, shall be returned in their entirety. At the completion of the installation all documents developed and/or acquired, such as photos, videos, schematics or diagrams, redlined or final, shall be submitted to the government as part of the final project completion and government acceptance.

Oversight and work coordination shall be performed throughout the duration of the project by the CO, COR and other FPS representatives, and/or authorized personnel as designated.

Signing a Non-Disclosure Agreement (NDA) found in Attachment [Insert Information] shall be required prior to receipt of sensitive/classified information herein.

28. ACCESSIBILITY REQUIREMENTS (SECTION 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

DRAFT

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.23 Telecommunications Products, applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches, circuits, etc. that are procured, developed or used by the Federal Government.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the

DRAFT

agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

29. PRIVACY REQUIREMENTS

29.1. Safeguarding of Sensitive Information (MAR 2015)

(a) *Applicability*. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions*. As used in this clause –

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security Number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national

DRAFT

defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security Numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)

DRAFT

(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal history
(7) Medical information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities*. The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

DRAFT

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by stature or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA)*, as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate.* The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

DRAFT

(1) *Complete the Security Authorization process*. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 12.01, February 12, 2016), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 12.0, November 15, 2015), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third-party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third-party validate the security and privacy controls in place for the system(s). The independent third-party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlines in *NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete the PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be

DRAFT

renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of

DRAFT

computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC,

DRAFT

the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any email. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

DRAFT

(h) *Additional PII and/or SPII Notification Requirements*

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after bring directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit

DRAFT

monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization.*

29.2. Information Technology Security and Privacy Training (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements.*

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security

DRAFT

Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via email notification not later than October 31st of each year. The email notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall email copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the

DRAFT

contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via email notification not later than October 31st of each year. The email notification shall state the required training has been completed for all Contractor and subcontractor employees.

30 Information Security

- The PACS Application will be on a server provided by the vendor
- The server will be behind/inside the "DHS FPS" firewall
    - The government will provide the connection of the server to the FPS network
- The FISMA System and ID is: Will be disclosed after award

DHS 4300 Policy 1.5.1.a This Policy Directive and the DHS 4300A Sensitive Systems Handbook apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS information unless an approved waiver has been granted. This includes prototypes, telecommunications systems, and all systems in all phases of the Systems Engineering Life Cycle (SELC).

DHS 4300 Policy 3.3.a All Statements of Work (SOW) and contract vehicles shall identify and document the specific security requirements for information system services and operations required of the contractor.

DHS 4300 Policy 3.3.b Contractor information system services and operations shall adhere to all applicable DHS information security policies.

DHS 4300 Policy 3.3.e Components shall conduct reviews to ensure that information security requirements and provisions to address supply chain risk are included in contract language and that the requirements and provisions are met throughout the life of the contract.

DHS 4300 Policy 3.3.f Security deficiencies in any outsourced operation shall require creation of a program-level POA&M.

DHS 4300 Policy 3.6.a Components shall ensure that system security is integrated into all phases of SELC.

DHS 4300 Policy 3.6.b Components shall ensure that security requirements for sensitive information systems are incorporated into life-cycle documentation.

DRAFT

DHS 4300 Policy 4.1.3.a System Owners shall ensure that users of the information systems supporting their programs have a valid requirement to access these systems.

DHS 4300 Policy 4.2.1.g Components shall control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

DHS 4300 Policy 4.2.1.j Components shall authorize, monitor, control and maintain records of the delivery and removal of hardware and software that enters and exits a facility.

DHS 4300 Policy 4.3.1.c DHS personnel, contractors, and others working on behalf of DHS are prohibited from using any non-Government-issued removable media (such as USB drives) and from connecting them to DHS equipment or networks or using them to store DHS sensitive information.

DHS 4300 Policy 4.3.1.d All USB drives shall use encryption in compliance with Section 5.5.1 of this Policy Directive.

DHS 4300 Policy 4.3.1.e DHS-owned removable media shall not be connected to any non-DHS information system unless the AO has determined that the risk is acceptable based on compensating controls and published acceptable use guidance that has been approved by the respective CISO or Information Systems Security Manager (ISSM). (The respective CISO is the CISO with that system in his or her inventory.)

DHS 4300 Policy 4.3.3.a Components shall ensure that any information systems storage medium containing sensitive information is sanitized using approved sanitization methods before it is disposed of, reused, recycled, or returned to the owner or manufacturer.

DHS 4300 Policy 4.3.3.b Components shall maintain records of the sanitization and disposition of information systems storage media.

5. **DHS Enterprise Architecture Compliance Terms and Conditions**

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.

DRAFT

- Applicability of Internet Protocol Version 6 (Ipv6) to DRS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be Ipv6 compliant as defined in the US. Government Version 6 (USGv6) Profile National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

32. DHS Geospatial Information System Terms and Conditions

All implementations including geospatial data, information, and services shall comply with the policies and requirements set forth in the DHS Geospatial Information Infrastructure (GII), including (but not limited to) the following:

- All data built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Data Reference Model.
- All software built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Technical Reference Model.

33. GOVERNMENT TERMS & DEFINITIONS

33.1. COR – Contracting Officer's Representative.
33.2. DHS – Department of Homeland Security.
33.3. MD – Management Directive.
33.4. SCI – Sensitive Compartmented Information.
33.5. U.S.C – United States Code.
33.6. CFR – Code of Federal Regulations.
33.7. P.L. – Public Law.
33.8. MST – Mountain Standard Time.

34. DELIVERABLES AND DELIVERY SCHEDULE

The Contractor shall consider items in BOLD as having mandatory due dates. Items in *italics* are deliverables or events that shall be reviewed and/or approved by the COR prior to proceeding to next deliverable or event in this SOW.

DRAFT

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	SOW Section 14	***Submittals Draft Plan***	10 business days after award	COR, Contracting Officer
2	SOW Section 18	***Phasing Requirements***	Within 10 days after award	COR, Contracting Officer
3	SOW Section 21	**Post Award Conference**	5 business days after award	COR, Contracting Officer
4	SOW Section 22	***Progress Meetings***	Weekly basis	COR, Contracting Officer
5	SOW Section 23	***PACS Solution Familiarization***	5 business days after acceptance of the fully installed system	COR, Contracting Officer
6	SOW Section 15	***Execution***	Acceptance of the PACS shall be within 120 days of award	COR, Contracting Officer

DRAFT

FPS Instruction Manual 15.2.6.1-01

Real Property Management

Department of Homeland Security

Federal Protective Service

Office of the Deputy Director for Technology and Innovation

Thomas J. Doran

Deputy Director, Technology and Innovation

Table of Contents

FOREWORD **1**

OVERVIEW **2**

CHAPTER 1 - PROJECT REQUIREMENTS **2**

1.1 INTENT 2

1.2 INDUSTRY CODES AND STANDARDS 2

1.3 DESIGN AND CONSTRUCTION GUIDANCE 2
- 1.3.1 Approving Authority 2
- 1.3.2 Design Intent Documents 3
- 1.3.3 Design Review 3
- 1.3.4 GSA Responsibility 4
- 1.3.5 Material Change(s) 4
- 1.3.6 FPS Review 4

1.4 FPS FACILITY STANDARDS 4
- 1.4.1 FPS Specific Requirements 4
- 1.4.2 FPS Facility Construction Design 4
- 1.4.3 Utility Requirements 4
- 1.4.4 FPS LAN / Radio Rooms 4
- 1.4.5 Radio/Tech/ITFO Lab 4
- 1.4.6 Additional HVAC Requirements 5
- 1.4.7 Cooling Requirements 5

1.5 SECURITY REQUIREMENTS 5
- 1.5.1 Physical Security Criteria 5
- 1.5.2 Site Assessment 5
- 1.5.3 Adjacency Requirements 5
- 1.5.4 Clearance Requirements 5
- 1.5.5 COOP Requirement 5
- 1.5.6 Mechanical Electrical Plumbing (MEP) Services 5

1.6 PARKING 6

1.7 INTERIOR LAYOUTS 6

1.8 SUSTAINABLE DESIGN 7

1.9 ENVIROMENTAL IMPACT ANALYSIS PROCEDURES 7

1.10 ENVIROMENTAL REVIEW PROCEDURES 7

1.11 PROJECT SECHEDULE 8

CHAPTER 2 - REAL PROPERTY **9**

2.1 OVERVIEW 9

2.2 LEASE ACQUISITION 9
- 2.2.1 Leasing Evaluation Process 9
- 2.2.2 Occupancy Agreement (OA) 10

2.2.3 Memorandum of Agreement (MOA)/Memorandum of Understanding (MOU) 10
2.2.4 Inner Agency Agreement (IAA) Funding 11
2.3 ACCEPTANCE 11
2.4 POST OCCUPANCY 11
2.5 TERMINATION 11
2.5.1 Tenant Responsibilities 11
2.5.2 Additional Requirements for IT and Specialized Equipment 13
CHAPTER 3. FURNITURE 16
3.1 OVERVIEW 16
3.2 FURINTURE AND APPLIANCES 16
3.3 VENDORS 17
3.4 REPLACEMENT FURNITURE 17
3.5 TELEVISIONS 17
3.6 EXCESS FURNITURE 18
CHAPTER 4. ANTENNAS 19
4.1 OVERVIEW 19
4.2 ANTENNA ACQUISITION 19
CHAPTER 5. EXPLOSIVE SAFES 20
5.1. OVERVIEW 20
5.2 REQUIREMENTS FOR EXPOLSIVE SAFES 20
5.3 ASD FACILITIES RESPONSIBILITIES 20
5.4 FPS CANINE OPERATIONS BRANCH RESPONSIBILITIES 21
5.5 REGIONAL RESPONSIBILITIES 21
CHAPTER 6. SPACE REQUIREMENTS 22
6.1 OVERVIEW 22
6.2 FACILITIES ROLE 22
6.3 IDENTIFYING NEED FOR SPACE 22
6.4 BUDGET DEVELOPMENT 23
6.5 SEATING 25
6.5.1 Seating Priorities for FPS Personnel 25
6.6 DEVELOPING WORKPLACE STANDARDS 25
6.6.1 Circulation – Defining and Planning 25
6.7 SPACE ALLOCATION 26
CHAPTER 7. CONSTRUCTION DESIGN GUIDELINES 30

7.1 OVERVIEW 30
7.2 ADMINISTRATIVE SPACES 30
7.3 MISSION SPACES 30
7.4 STORAGE SPACES 30
7.5 SCIFS 30

CHAPTER 8. PARKING POLICY 31

8.1 OVERVIEW 31
8.2 SPARED PARKING SPACES AND PARKING NOTATIONS 31
8.3 PARKING AGREEMENTS 31
8.3.1 Occupancy Agreement (OA) 31

CHAPTER 9. CONSTRUCTION REQUIREMENTS 32

9.1 OVERVIEW 32
9.2 PHYSICAL/SECURITY REQUIREMENTS 32
9.2.1 Contractor Security Requirements 32
9.2.2 Perimeter, Demising and Secure Wall Requirements 32
9.2.3 Perimeter Wall 32
9.2.4 Demising Wall 32
9.2.5 General Construction of New Demising Walls 32
9.2.6 Secure Wall (New or Existing) 33
9.2.7 General Construction of Secure Walls 33
9.3 PERIMETER, DEMISING AND SECURE AREA DOOR REQUIREMENTS 33
9.3.1 Construction Requirements for High Security Doors 33
9.3.2 High Security Locks (Perimeter Doors and where applicable) 34
9.3.3 Duct Work Openings 34
9.3.4 Exterior Windows 34
9.4 OFFICE AND CUBICLE IDENTITY SIGNAGE 34
9.5 INFORMATION TECHNOLOGY BUILD-OUT STANDARDS 34
9.6 NETWORK CONNECTIVITY AND COMMUNICATIONS 35
9.7 VIDEO TELECONFERENCE (VTC) 35

CHAPTER 10. OPERATIONS AND MAINTENANCE 36

10.1 OVERVIEW 36
10.2 OPERATIONS AND MAINTENANCE WORK (O&M) 36
10.3 BUILDING SERVICES 36
10.4 GSA MANAGEMENT SERVICES 36
10.5 REIMBURSABLE WORK AUTHORIZATION (RWA'S) FOR MAINTENANCE 37
10.6 FUNDING AND FINANCIAL 37
10.7 PREVENTIVE MAINTENANCE PROGRAM GUIDELINES 38
10.7.1 Preventive Maintenance 38

10.7.2 Breakdown Maintenance 38
10.8 RENT 38
10.9 OPERATIONS AND MAINTENCE BUDGETING 38
10.9.1 Maintenance Budgeting 38
10.9.2 Monitoring Maintenance for Leases 39
10.10 EXPECTED USEFUL LIFE (EUL) MATRIX 39
10.11 MAINTENANCE MANUALS 39
CHAPTER 11. MOVES AND TERMINATIONS (HQ) 41
11.1 OVERVIEW 41
11.2 OFFICE MOVE REQUESTS 41
11.3 RELOCATION 41
11.4 FORCED MOVE 41
11.5 MOVE REQUIREMENTS 41
APPENDIX A1
A: DEFINITIONS A1
B: REFERENCES B1
C: FACILITY CONSTRUCTION DESIGN GUIDELINES C1
Wall Construction C1
Administrative Spaces C4
Mission Spaces C21
Storage Spaces C33
SCIF C37
D: FPS HQ SEAT ASSIGNMENT REQUEST FORM D1
E: CALCULATING A WORKSPACE STANDARD (EXAMPLE) E1

FORWARD

The Real Property Management Manual is to be primarily used by Federal Protective Service (FPS) personnel as a facility planning and management tool. Other possible users of information in the Real Property Management Manual are General Services Administration (GSA) transaction managers, realty specialists, construction project managers, current and prospective private lessors, architects, and contractors. The Real Property Management Manual provides a benchmark for planning and design of new lease acquisitions, and for the evaluation and renovation of existing space. Nothing contained within this manual shall supersede DHS instruction 119-02-003; DHS Workplace Standards, September 30, 2014; OR DHS instruction 119-02-001 Revision 1, Real Property Manual, July 2, 2010. If there is any ambiguity or discrepancies the DHS manual and instruction shall be deemed overriding. Criteria can always be more stringent but cannot be less stringent.

This manual will be used by the Facilities Branch (Facilities) in accordance with DHS Directive 119-02, "Real Property Management Program," December 10, 2012, for project and program management support. The procedures outlined support division policy defined by the Administrative Services Division (ASD) Management team. FPS Design Standards ("*Standards*") contain criteria and concepts for the planning and design of FPS operated locations. The standards contain FPS organizational, operational, and functional requirements specific to the FPS component. The standards captured here ensure FPS personnel can effectively achieve mission critical core functions and objectives, while also adhering to security, safety, and building code regulations. Any deviations from the FPS Real Property Management Manual and associated standards must be approved by ASD.

In accordance with OMB Memorandum M-12-12, Section 3 "Reduce the Footprint", March 2015, spaces have been "adjusted or rightsized". The Real Property Management Manual includes room data sheets that provide written criteria and plans for personnel workspaces, office support spaces, conference/training rooms, communication spaces, fitness rooms, laboratories, secured and detention spaces and support areas. The space types consist of two components: 1) Mission Space (which does not count against our Square Footage Utilization Rate), and 2) Administrative Space (cubicles, offices, and all non-mission space). All spaces are identified using these criteria.

OVERVIEW

Application of the Real Property Management Manual criteria may be influenced by the physical characteristics of the available space such as building and room dimensions, window locations, column spacing, structural floor loading capacity, building access, vertical transportation, and site restrictions. These factors affect the room layout, furniture arrangement, space adjacencies, and compliance with federal and local building requirements for life safety and accessibility. In addition, further design requirements, such as separation between workstations and sanitary considerations shall be considered for minimization of exposure to hazards; must follow CDC and DHS guidelines for these considerations.

The Real Property Management Manual is flexible enough to adapt to building requirements and environmental conditions, but changes from the Real Property Management Manual criteria requires approval by the Director, ADFO, or ASD. The request for variance must include the following information: Mission Requirements, Cost, Square Footage, Utilization and Schedule Impact. Note: ASD must be notified of deviation by Director or ADFO and reason for the deviation.

Finally, The Real Property Management Manual outlines FPS requirements under the National Environmental Policy Act (NEPA) and other applicable environmental, historic, cultural, sustainability, energy laws and Executive Orders (EOs).

CHAPTER 1. PROJECT REQUIREMENTS

A project is defined as any request for the modification, addition, or deletion of space to include planning for these actions. The Project Requirements (PR) provide specific FPS/DHS requirements and Agency Specific Requirements ASR, which may vary, be more specific, or more stringent than those of the Request for Lease Proposal (RLP) minimum requirements and are intended to give the Offerors additional information to be fully compliant with the RLP. The PR is not intended to reduce the minimum requirements contained within the base RLP.

This document should be used in conjunction with the task order scope of work and the RLP requirements. If any ambiguity exists, the more stringent requirement shall prevail; however, if there are any conflicts between documents, they shall be brought to the attention of the FPS Project Manager (PM) for clarification.

1.1 INTENT

These Project Requirements are intended to convey the intent of the scope of work but are not to be considered exhaustive or all-inclusive. Where these specifications do not address specific criteria, the Lessor shall include systems, materials and equipment in accordance with sound design practices for similar facilities in the marketplace. Recognizing that the PR alone cannot convey all the information required for the successful completion of a project, the Government and FPS expects that the design team, having the knowledge and expertise of these facilities will interpret the intent of the PR correctly, and will supplement these documents with their expertise in order to achieve a complete, high quality and fully functional design.

1.2 INDUSTRY CODES AND STANDARDS

All construction shall, at a minimum, be performed in workmanlike manner and constructed in accordance with the latest building codes as applied or enforced by the local jurisdiction and applicable laws, rules and regulations.

1.3 DESIGN AND CONSTRUCTION GUIDANCE

1.3.1 Approving Authority

FPS shall have the sole approving authority on all matters involving aesthetic design and appearance of base building and tenant improvements, including but not limited to the exterior envelope, main lobby, landscaping and site design, lighting, and toilet rooms to the extent that they relate to the FPS owned or leased portion of the building. FPS shall coordinate and be reliant upon the design team for preparation of design and finish options.

1.3.2 Design Intent Documents

During the development of the Design Intent Documents (DID's) and Construction Documents (CD's), FPS will coordinate with GSA representative (who coordinates with the Lessor, Architect and/or Engineers to identify specific project requirements not specifically identified in the Exhibits and Lease documents).

1.3.3 Design Review

For the purposes of design review and approval prior to release for construction, GSA shall split the CD's into Shell and Core (SC) and Tenant Improvement (TI) packages, if applicable. The intent for this split is to allow GSA to manage the construction schedule through early issuances of the SC package and associated sub packages for construction work to proceed while the TI package is under development. The TI package development schedule shall consider and work in tandem with the Design Intent Drawings (DID) development process. FPS encourages the combining of the SC and TI cost after approval of the DID's if the TI Design is being done by the GSA.

1.3.4 GSA Responsibility

GSA shall prepare and provide DID's to FPS for approval. DID's, for the purposes of this project, are defined as floor plans graphically depicting the requirements set forth within the ASR (Agency Specific Requirements) and the POR (Program of Requirements).

1.3.5 Material Change(s)

Any material changes to the CD's that vary from the DID's shall require specific notice to and approval from the FPS Project Manager (PM) and Contracting Officer (if applicable).

1.3.6 FPS Review

FPS's review of the DID's and CD's does not relieve GSA from being completely responsible for the improvements required by this project. GSA is solely responsible and liable for technical accuracy of the drawing submissions in meeting all requirements of the contract.

1.4 FPS FACILITIES STANDARDS

1.4.1 FPS Specific Requirements

The FPS specific requirements, which amplify or modify the standard requirements outlined in the RLP, are stated by these Project Requirements (PR). The PR contains the Agency specific requirements which apply to the overall project.

In addition to special construction requirements there may be other building specific requirements for lighting, heating, cooling and custodial services that must be considered in the design and construction process (ASD Environmental Sustainability employee will create/handle these requirements). The unique FPS operational requirements will be considered "above standard" by GSA and will be billed as "overtime utilities" accordingly.

1.4.2 FPS Facility Construction Design

This FPS Facility Construction Design Drawings will be registered as Appendix C within this manual.

1.4.3 Utility Requirements

GSA shall equip the facilities with the required HVAC, electrical, and plumbing services as outlined during the design phase. FPS facilities, such as field offices or Mega Center's, with specific operational requirements such as shift work or extended hour beyond established core hours may require a zoned HVAC system that reflects their unique mission requirements for 24/7 activities in various parts of the facility as well as emergency stop equipment for zone shut down by area for emergencies. Note: Backup generators or UPS systems may be required due to operational requirements. This will be initiated at design.

1.4.4 FPS LAN / Radio Rooms

These spaces will contain FPS racks, servers and security and TacCom radio equipment that may require 24/7 HVAC cooling. Depending on load requirements these rooms may require separate, Computer Room Air Conditioning (CRAC) unit(s) (See Appendix C)

1.4.5 Radio/Tech/ITFO Lab

These spaces will contain FPS racks and equipment requiring 24/7 HVAC cooling (if applicable). Depending on load requirements these rooms may require separate, Computer Room Air Conditioning (CRAC) unit(s) (See Appendix C)

1.4.6 Additional HVAC Requirements

Additional spaces identified during the design phase may also require 24/7 HVAC (If determined by HVAC load calculations).

1.4.7 Cooling Requirements

Exact cooling is to be based on British Thermal Units (BTUs) emitted by equipment. The incorporation of necessary cooling is to be implemented to requirements listed in the design phase.

1.5 SECURITY REQUIREMENTS

1.5.1 Physical Security Criteria

The project shall comply with FSA Directive 15.8.1.1, Revision 2, "Facility Security Assessment," March 9, 2018 and DHS instruction 121-01-017-01 Physical Security Construction and Equipment Specification Instruction Manual, March 21, 2015. FPS has determined all new leased construction shall be based on independent site, location and occupancy variables. The necessary setback distance and mitigation strategies will be determined following a formalized Threat Assessment and Risk Analysis. A Facility Security Assessment is conducted after selection of a site and is not required if moving into an existing federal facility, unless adding FPS as an occupant changes the FSL of the facility.

1.5.2 Site Assessment

FPS shall conduct a Facility Security Assessment to determine the security requirements for this facility. They will conduct a Site/Building Risk Assessment for compliance and/or to determine the requirements for this facility.

1.5.3 Adjacency Requirements

Whenever possible, FPS facilities shall not be located adjacent to, in proximity or and/or within residential areas, drug, explosive, or weapon free zones, educational facilities, religious facilities, other citizen or immigration (such as EIOR and CIS) related facilities, and/or retail facilities. The FPS PM shall provide direction during Advertisement for Space and Market Survey phases (If applicable). DHS may determine or require other agencies to co-locate with each other as part of consolidation efforts.

1.5.4 Clearance Requirements

The Lessor shall agree to insert lease terms that conform substantially to the language of the security clearance requirements, which are conducted by GSA, and apply to all contract workers to include but not limit to, design, construction, and maintenance and cleaning service personnel. These requirements will be provided upon request to the Lessor. If applicable, a Building Access Request Form will be provided to the Lessor for use with directions for submittal of the required documentation. Unless the facility is FSL 3 or 4, these services must be paid to GSA by FPS.

1.5.5 COOP Requirement

The site may be considered a Continuity of Operations (COOP) site (Determined by DHS) in which case it may be necessary to continue FPS's mission during periods of crisis situations. This may require additional systems (e.g., a backup generator, etc.) to support operations.

1.5.6 Mechanical Electrical Plumbing (MEP) Services

The Lessor shall provide the Mechanical Engineer (ME) and Structural Engineer SE with the required HVAC and electrical services as outlined during the design phase. The facilities shall reflect and complement the appearance and construction of the exterior façade of the FPS office building.

1.6 PARKING

GSA shall provide the number of parking spaces required by the RLP, to include, but not be limited to, visitors and FPS Government fleet vehicles. These spaces shall be available on site (preferred location, if not, adjacent would be second preference) maximum distance from parking location to building exit to be 250 feet and shall be secured as required by the Real Property Management Manual described within the RLP. When parking cannot be adjacent, every effort will be made to obtain parking on the same side as the building to ensure officers in an emergency response will not have to cross active streets in urban cities to get to their vehicle to respond. Based on the facility type and size, the vehicles to be accommodated may include cars, vans and buses. This parking should be located adjacent or as close to the building as possible and shall comply with ADA guidelines for number of handicap accessible parking spaces required. For additional parking guidance and information, see 8.3 Parking Agreements

1.7 INTERIOR LAYOUTS

To assist in the design of the spaces, adjacency diagrams and prototypical blocking and stacking schemes may be provided by ASD to demonstrate possible arrangements. While the building shapes will vary in size and design, the adjacencies must be satisfied. A test fit plan with the necessary adjacencies may be required based on the shell and core design of the facility being proposed by GSA. All plans shall be ADA compliant as well as compliant with all applicable local and national building codes. This plan will serve as a schematic design for adjacency purposes only. Adjacency and specific room requirements that affect the shell design are as follows:

a. The Lobby and FPS Security requirements (See Appendix C): If FPS does not control the main lobby, the security requirements for screening and badging (as required by the FSL designation for the building) may need to be located on an upper floor or on a partial floor. In multi-floor occupancies the security stations, and the required staff, may have to be duplicated. Special attention must be given to the maintenance of egress paths and the conflicts that are typically generated in secured environments.

b. Operating hours: PSO's often operate during hours where other areas of the building may be closed. It is therefore necessary that the 24/7 personnel have access to the Break Room, Employee Restrooms (Men's and Women's) and Lobby. (May require special access to parking)

c. Visitor Restrooms: Men's and Women's restrooms and preferably a Break Room must also be open and available for use by outside contract personnel without accessing secured FPS office areas. The required adjacencies should be considered in the zoning of the HVAC system as well as for the establishment of a security hardline in the test fit. Visitor restrooms should be located outside of leased space whenever possible.

d. A Unisex restroom may be required adjacent and accessed via the FPS lobby for use by FPS public visitors.

e. The FPS Open Office Area (Administrative Area): Must be adjacent to the staff or team they serve and should be placed on the outside wall (if possible) to allow natural light to penetrate the building to the greatest possible degree.

f. Efficient use of space must be considered such as column or window spacing. For buildings of 10,000 Net Square Feet or greater column spacing cannot be greater than one column per 1000 square feet. For buildings less than 10,000 net square feet column spacing cannot be greater than one column per 500 square feet. Columns located in weapons or defense tactics rooms will not be allowed. Windows are not allowed in weapons, detention, evidence, or IT spaces.

1.8 SUSTAINABLE DESIGN

FPS is required to meet sustainable building management requirements put into effect through legislation, Executive Orders (EO), and DHS Management Directives. FPS is committed to incorporating principles of sustainable design and energy efficiency into all its building projects and will seek the applicable LEED certification as specified in the RLP. GSA must ensure the facility follows all Federal, State and local environmental protection laws and regulations.

Sustainability requirements are encapsulated in the Guiding Principles for High Performance and Sustainable Buildings.

1.9 ENVIRONMENTAL IMPACT ANALYSIS PROCEDURES

The National Environmental Policy Act (NEPA) of 1969 (42 USC 4321 et. seq.), as amended, establishes policy and requirements governing all Federal Departments with respect to protecting the environment. FPS will follow specific requirements established by NEPA and by the associated implementing regulations promulgated by the Council on Environmental Quality (CEQ) (40 CFR 1500-1508), and requirements contained in current version of DHS Directive 023-01 *Environmental Planning Program* and associated instructions. NEPA requires all Federal Departments to consider all potential environmental consequences of their activities prior to initiation of a Federal action. Specifically, Section 102(2)(c) of NEPA requires all agencies of the Federal Government to include an environmental Impact Statement "in every recommendation or report on proposals for legislation and other major Federal actions significantly affecting the quality of the human environment."

1.10 ENVIRONMENTAL REVIEW PROCEDURES

All major Federal actions above the simplified acquisition threshold must have an environmental review performed prior to the non-retrievable or recoverable expenditure. The environmental review must be completed, and documentation approved before the reimbursable work authorization is issued to the service provider.

DHS has three levels of environmental review:

- Un-asterisked Categorical Exclusions,
- Asterisked Categorical Exclusion that require a Record of Environmental Consideration (REC);
- Environmental Assessment (EA)/Finding of No Significant Impact (FONSI); and
- Environmental Impact Statement (EIS)/Record of Decision (ROD).

All environmental reviews must be conducted, and documents prepared, as required, in accordance with applicable laws and regulations, DHS Directive 023-01 *Environmental Planning Program* and associated instructions prior to the expenditure of federal funds.

When submitting project requests, the following information must be included in the package:

1. Completed FPS Environmental Impact Analysis Checklist (aka: NEPA checklist), see Appendix F1 for a copy of the checklist;
    a. Date of construction of the building is important to the analysis and shall be noted in the checklist, Section II, 11.A.
2. Copies of the GSA NEPA and Historic Preservation documents for the building or space;

Buildings that are 45 years of age or older are of priority concern as they will require additional consultations with GSA Historic Preservation Specialists and potential consultations with State Historic Preservation Offices (SHPOs).

Coordination with the FPS Environmental Compliance Office (ECO) may reduce or eliminate project timeline delays and budget increases. Note: Due to length of time required for this component, early coordination is recommended

1.11 PROJECT SCHEDULE

GSA shall provide an overall project schedule giving the dates (FPS prefers calendar days over working days) on which various phases of design and construction will be completed to coincide with FPS required occupancy date (refer to the “Lease Term Commencement Date” paragraph in the General Information section of the RLP). A preliminary schedule is to be provided within 30 calendar days after award of the lease contract and a finalized schedule no later than 60 calendar days after lease award.

CHAPTER 2. REAL PROPERTY

2.1 OVERVIEW

This section outlines the principles in planning and implementation for new spaces and the management of all space for FPS, whether located in Headquarters or the Field. These principles apply to all FPS offices.

2.2 LEASE ACQUISITION

When it has been determined that leasing a new space is the best option (assumes that FPS looks internally at their available spaces first). FPS will first attempt to acquire offices and types of special space through GSA and leverage the real estate resources that GSA makes available to their constituent agencies through the Federal Real Property Profile (FRPP). GSA is the federal government's primary federal real property and asset management agency, with 11 regional offices nationwide that oversee acquisition of real property for the federal customer. By law, GSA acts as a procurement agent for federal agencies, seeking economies of scale for the government. The GSA space procurement process typically begins with a federal agency approaching GSA with a mission-related need leading to process initiation. According to Federal Management Regulation (FMR), prior to entering a new lease, GSA must first consider existing vacant spaces in federally owned buildings, or existing government leased space in the desired area. The only exceptions to utilizing GSA services for leased facilities are as follows:

- There are unsuitable alternatives in the GSA inventory of available properties.
- The required geographical location is too remote to warrant inclusion in the GSA inventory.
- In accordance with DHS Delegation Number 00500, Revision 01 "Delegation to the Chief Readiness Support Officer", issued June 5, 2012, OCRSO real property, has the appropriate authority to issue real property warrants and can engage in real property acquisitions, as defined in the Federal Acquisition Regulation (FAR).
- GSA delegated authority (verified in writing by GSA according to guidelines in the Federal Management Regulation (FMR).

2.2.1 Leasing Evaluation Process

GSA leasing is a preferred method of acquiring space. Even when a DHS real property warrant and statutory direct authority are possessed, GSA is to be the sole provider for acquisition.

When engaging GSA for a lease evaluation, a GSA Leasing Specialist will typically ask for a requirements package (ASR, POR, and Real Property Management Manual). This information is critical and provides GSA with the necessary documentation to provide an accurate cost estimate (Independent Government Cost Estimate, IGCE).

Once the leasing evaluation is completed, a space is to be acquired through a new lease transaction. A GSA Realty Specialist will work with the appropriate FPS asset management office to:

Finalize the space requirement package, including physical security requirements specified by the appropriate Physical Security Specialist;

Develop an estimate for tenant improvement costs, including general and customized tenant allowances;

Work with the project's parameters such as location, amenities, and infrastructure, to locate suitable properties. GSA is legally obligated to seek out certain spaces over others. Priorities are given below, in order of greatest to least:

- Federally owned inventory – The Federally owned inventory is GSA's first choice for all new leasing actions.

- Advanced Acquisition Process (AAP)[1] – This GSA program leverages GSA relationships with the private-sector owners to determine upcoming vacancies in their portfolios. The program allows GSA to rapidly identify available space for acquisition on behalf of the DHS Component office.
- Market Survey – When GSA has no available space in the federal inventory, and no suitable inventory can be located in the AAP, GSA initiates a market survey. This process requires both GSA and DHS Component office participation in a Market Survey.

2.2.2 Occupancy Agreement (OA)

An Occupancy Agreement serves as a complete, concise statement of the specific financial terms and conditions by which a federal agency occupies a GSA-controlled space, whether it is government-owned or leased by GSA on the agency's behalf. When a project is initiated, an OA draft/proforma is created. There are several key components that make up an Occupancy Agreement.

Facilities and the ECO (as applicable) must review, and DHS approve, the draft OA/proforma prior to GSA's making any major contractual commitments associated with the space request. Due to changes in negotiations during the leasing process and changes of lease terms (e.g. years leased), there may be several draft OAs/proforma revisions that GSA will ask DHS to sign prior to the final version. There are two critical steps during the development of a Draft OAs that will need to be signed as a condition of the project moving forward (prior to the execution of a design contract or feasibility study for federal buildings or prior to the market study for leased space) and an updated draft OA before award of the lease contract. A Final OA is generated when the new space has been accepted by FPS and GSA, and the data has been entered into the GSA finance system. Billing begins when the Final OA is completed and verified by GSA. The Final OA does not need to be signed for the billing to begin. However, DHS needs to verify the billing information in the Final OA, and sign and return to GSA for a complete record (must be entered into Real Property Data Warehouse (RPDW).

2.2.3 Memorandum of Agreement (MOA)/Memorandum of Understanding (MOU)

A memorandum of agreement **(MOA)** is a type of agreement between two or more parties (typically between another agency or lessor and FPS) and consists of the following key components: Purpose, Scope, Authorities, Definitions, Responsibilities, Policy and Procedures and Signatures. MOA's do not require exchange of funds. If a MOA requires funding, it must be accompanied by an Inter-Agency Agreement (IAA) See 2.2.4 for funding. MOA's shall be reviewed by the ECO for compliance prior to acceptance.

A memorandum of understanding **(MOU)** is a type of agreement between two or more parties (typically between GSA and FPS) that indicate an intended common line of action. Funding may or may not be required for this agreement. This Agreement encompasses all aspects of the relationship between the two Parties and supersedes previous Memorandum of Agreements on this subject, establishing a current policy to:

a. Control the provision of and payment of operating expenses, support services, material and other related costs at [*FPS Facility Physical Address].*

b. Identify documents that describe the services and support provided, coordination and points of contact, and security policy and procedures

   Note: MOU's shall be reviewed by the ECO for compliance prior to approval

[1] This is for National Capital Region (NCR) only.

2.2.4 Inner Agency Agreement (IAA) Funding

The obligations in the IAA are subject to the availability of funds. Nothing in the IAA authorizes reimbursements for services or supplies until the IAA is incorporated into an interagency agreement that complies with 31 U.S.C. §§ 1501 and the Economy Act. No provision of the MOA will be interpreted to require obligation or payment of funds in violation of 31 U.S.C. § 1341 (the Anti -Deficiency Act).

While the Parties do not intend for the IAA be a binding commitment to transfer funds or to represent a financial obligation between the Parties, the Parties do contemplate that the IAA (or its essential terms) will be incorporated into an interagency reimbursable agreement for provision of services.

The Servicing Party will bill the Requesting Party quarterly for actual costs, which will be paid for or applied against advance payments (if any). The Requesting Party will reimburse all recurring costs of the office space on the date the interagency agreement is executed and the funding obligated. These costs are not to exceed the actual office space costs, plus the incidental costs associated with Servicing Parties responsibilities described in this MOA. The costs will be revised each fiscal year (FY) to reflect the actual space changes.

Note: If funds are being obligated, ECO shall review prior to acceptance

2.3 ACCEPTANCE

Space Acceptance is the commitment from an agency to occupy specified GSA-controlled space. After the complete buildout, there is a final inspection from the agency representatives and GSA. A punch list is generated, and a substantial completion date is developed after punch list items are corrected. GSA obtains a Certificate of Occupancy with the agreement on space measurement. Once FPS accepts the space as substantially complete, operationally functional, and acquires the keys, the rent will commence immediately.

2.4 POST OCCUPANCY

Within 60 days of occupancy, GSA shall furnish to Facilities as-build drawings of the occupied space as well as any manuals, warranties or manuals required. Any changes to the original OA terms shall be disclosed in addition to contact information regarding building management, property management, and the GSA lease administrator.

2.5 TERMINATION

Space utilization (including hiring projections and attrition), lease expirations, and other extenuating circumstances (damage or maintenance issues, rent increases) are all taken into consideration as FPS/DHS continuously monitors its property portfolio. If properties fall under the historic preservation or other environmental compliance, they shall be reviewed by the ECO. If the resulting analysis depicts spaces that need to be terminated, the following actions must occur:

2.5.1 Tenant Responsibilities

The following items are required for termination of a space (Also see Figure 1 “Process to Return/Dispose of Space” and Figure 2 “Additional Procedures to Return/Dispose of Space” below):

a. There is a minimum requirement of 1 year and 6 months before space can be terminated. A 120-day notice to terminate is required. Altogether, the occupancy requirement and required termination notice period totals 1 year and 10 months.

b. A 120-day notice must be provided to GSA to clearly address the effective date of the space release and the duration, and what specific blocks of space and/or Occupancy Agreements (OAs) will be terminated. This function is currently handled by the DHS real property (Example: FPS would like to provide official

notice of 120-day cancellations rights for OA agreement ACOXXXXX effective January 1, 2020). **Notification shall be sent to GSA regional representative.**

c. There may be associated cost with the termination of space (typically through the RWA process). The requesting party shall be responsible for paying for these costs (unless it is a forcing function in which case the forcing agency will be responsible for these costs)

d. GSA will respond with an acceptance of termination or return questions if the space is deemed not marketable. All space returned must be marketable to GSA and must have an egress not within a secured corridor that FPS has sole access to.

e. If FPS is moving to another location, the termination notice including the list of OA's to be terminated should be provided using language that addresses the completion of move-in of the new location; this is so that GSA understands that the date could fluctuate and is contingent upon the completion of another project.

f. FPS notifies DHS management of space(s) to be terminated in addition notifies the Physical Security Division, Property Branch, Fleet Branch and IT Division with an estimated termination date.

g. Occupancy Agreements should be reviewed for other real property items that are part of the OA agreement, such as parking and antenna space (rooftop and node). Although the FPS office space may terminate, the IT or Tactical Communications Division (ITD/TacCom) may still have a need for the antenna. This cost, if any shall be paid for by the Region responsible for the antenna and should be through a new OA.

h. If any conduits are going into the FPS space identified for termination, they will need to be relocated prior to the space release.

i. A comprehensive review conducted by Facilities will ensure the space was removed from Rent On The Web (ROW) 30-60 days after the date of termination. Note: GSA bills in arrears.

j. A Regional Representative shall conduct a walk through with the GSA Building Manager to review all aspects of the space.

   1) The representative should review the most recent Facility Inspection and current OA, as well.

   2) The Regional Representative and GSA Building Manager will review and define space that will or will not be needed after space reduction (such as parking, antenna, storage, Canine Explosive Storage Magazine)

   3) Above Standard Service Systems [HVAC], Overtime Utilities, or shared space [fitness center, Mat room, etc.]). Upon completion of the review, the Region Representative will annotate the Space Request Form accordingly.

k. The Regional office creates a draft SF 120 (Report of Excess Personal Property) and recommends a projected completion date in which the Region will declare, transfer or dispose of excess personal property. This completion date will provide reasonable assurance to the Region and ASD that the Region will have vacated all required space by the completion date. This completion date will be referred to as the "last billing date," which coincides with the proposed vacate date.

A transitioning out process is outlined by the following:

- In government owned property, tenants must coordinate with GSA to ensure removal of all personnel, furniture, files, equipment and trash required by lease. The FPS Region/Facilities representatives conduct a walkthrough of space to ensure everything has been removed.
- The Regional representative must either confirm the acceptance of the space or provides a list of corrective actions to successfully vacate including assistance from Facilities with the use of the form SF-120 for disposal of excess equipment. A secondary walkthrough should then be scheduled, and if deemed successful; keys and or alarm access must be returned to GSA.

Note: If any of the above items are still left in the space, the Region may be held liable to pay for rent the following month or until all items are cleared (does not relieve HQ from rent obligation).

2.5.2 Additional Requirements for IT and Specialized Equipment

In order to ensure space is released back to GSA in a timely manner and removed from inventory, the following items must be considered:

a. It is the responsibility of the ITFO and ITD to coordinate all IT items to be removed. Notice needs to be provided to GSA ahead of time if the IT rack is being abandoned in place. This is considered agency-special equipment and it is the responsibility of the agency to remove it out of the space.

b. Cables are permitted to be left in the space; when removing cables, the cables should be removed from the panel as well. This is normally included as part of GSA's shell cost offered to the incoming tenant. The same principle applies for lease space.

c. All switches, UPS, and access control systems, monitoring devices must be removed and or disabled so GSA has access. Separate HVAC units are part of Real Property and shall be abandoned in the space.

d. ECO shall review list of equipment being decommissioned for inventory/reutilization purposes

   Note: There may be fees associated with this these actions that shall be paid for by the Region. If it is determined that these items can stay per the lease and it is not cost effective to remove them, they shall remain in place.

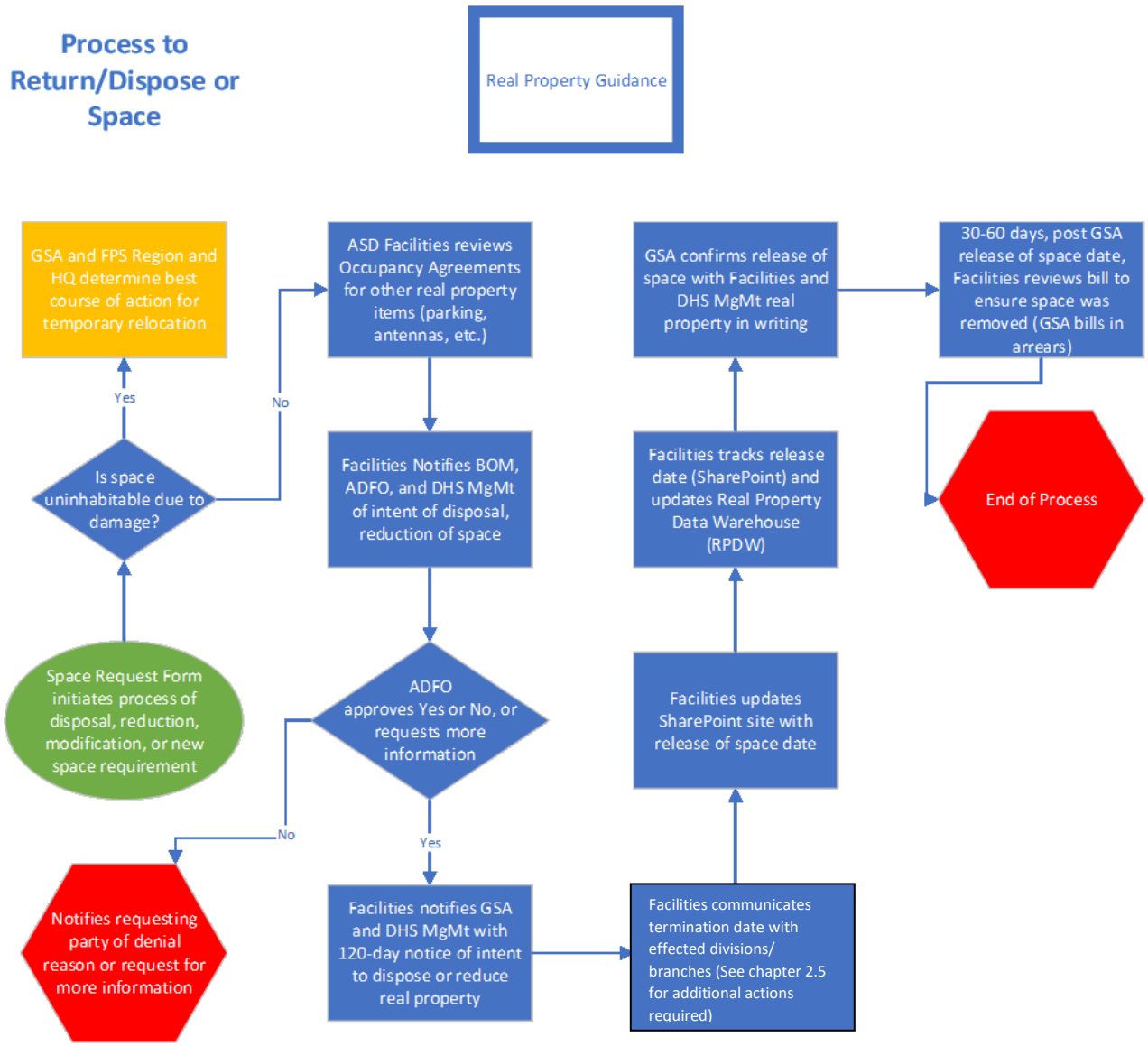
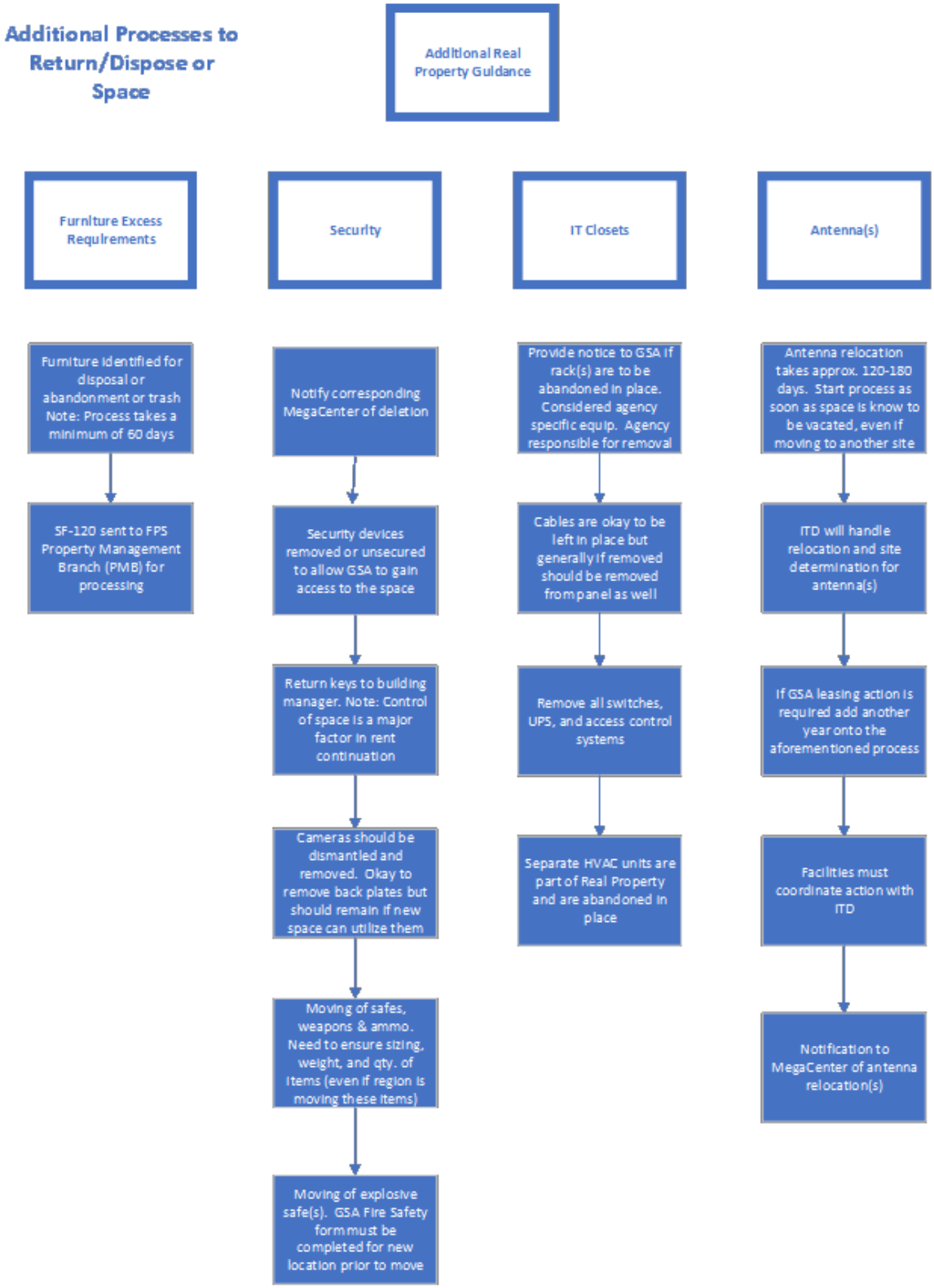


FIGURE 1: Process to Return/Dispose of Space

FIGURE 2: Additional Procedures to Return/Dispose of Space



CHAPTER 3. FURNITURE

3.1 OVERVIEW

This section outlines the procedures of acquiring furniture and appliances within Facilities. As part of the workplace standards initiative, the following policy will apply to all FPS Regions and HQ Divisions looking to procure furniture or appliances with a purchase value equal or more than $1000.00 (per individual item). For requests less than $1000.00 (per individual item) the request will be sent to the BOM for review. ASD will review requests over $1000 (per individual item) to determine the impact on the location's physical infrastructure (electrical, data/telecom) prior to authorizing the purchase request. Amounts greater than $1000 (per individual item) will require ASD approval. Centralizing the acquisition process is intended to facilitate standardization and approval.

Note: Purchase of items through the DHS Strategic Sourcing Initiative existing BPA for Office Supplies by purchase card holders is outside the scope of this manual.

3.2 FURNITURE AND APPLIANCES

The acquisition and procurement of furniture greater than $1000 for all FPS offices shall be facilitated and approved by Director, Assistant Director for Field Operations (ADFO), or ASD and shall be reviewed by ECO for NEPA compliance (unless BPA is used). This is inclusive of all furniture requests regardless of the procurement method, which includes: FPS Headquarters sponsored projects, the FPS Consolidated Contracting Group (CCG), and Procurement card (p-card) transactions. For the purposes of this policy, furniture & appliances will include, but not be limited to the following:

Furniture			
Desks	Systems-Furniture (Cubicles)	Conference Tables	Lateral File Cabinets
Credenzas	Seating	Conference Chairs	Free Standing Storage Units
Seating	Free-standing Desks	Multi-use Cabinets	Lockers
Guest Chairs	File Cabinets	Conference Storage Units	Weapons/Ammo Safes
Conference Tables	Pedestal Files	Audio/Visual Storage	Multi-use Storage Racks
Bookshelves	Overhead/Hanging Files	Side/Guest Chairs	Print/Copy Furniture
Lounge Furniture (Sofa)	Lighting	Break-Area Tables & Chairs	
Appliances			
Refrigerators	Dishwashers	Commercial Ice Makers	Supplemental Heating & Cooling Units
Microwaves	Range Units	Commercial Freezers	Water Heaters
Commercial Coffee Machines	Stove/Oven Units	Washing & Drying Machines	Disposal Units

TABLE 1: Furniture and Appliance List

Sustainable furniture products can be found on the Environmental Protection Agency's (EPA) website for Greener Products and Services here: https://www.epa.gov/greenerproducts/recommendations-specifications-standards-and-ecolabels-federal-purchasing#officereq

Sustainable appliances can be found here: https://www.energystar.gov/productfinder/

3.3 VENDORS

Vendors shall be vetted through the contracting office and made available to FPS for use through Blanket Purchase Agreement (BPA)'s and other funding vehicles, such as PCTW's or RWA's.

3.4 REPLACEMENT FURNITURE

In order to maintain a suitable work environment, FPS office furniture will be reviewed for automatic replacement once the age of the furniture reaches ten (10) years (See Figure 3, below). If it is determined that furniture needs replacing, it shall be placed on the funding list for consideration. FPS offices may request furniture replacement every seven (7) years. Furniture requests received prior to the ten (10) year period will be reviewed by ASD for approval. Prior to purchasing new furniture an audit/effort should be conducted to assess if furniture reuse is an option. Results of this effort shall be attached to the new furniture request.

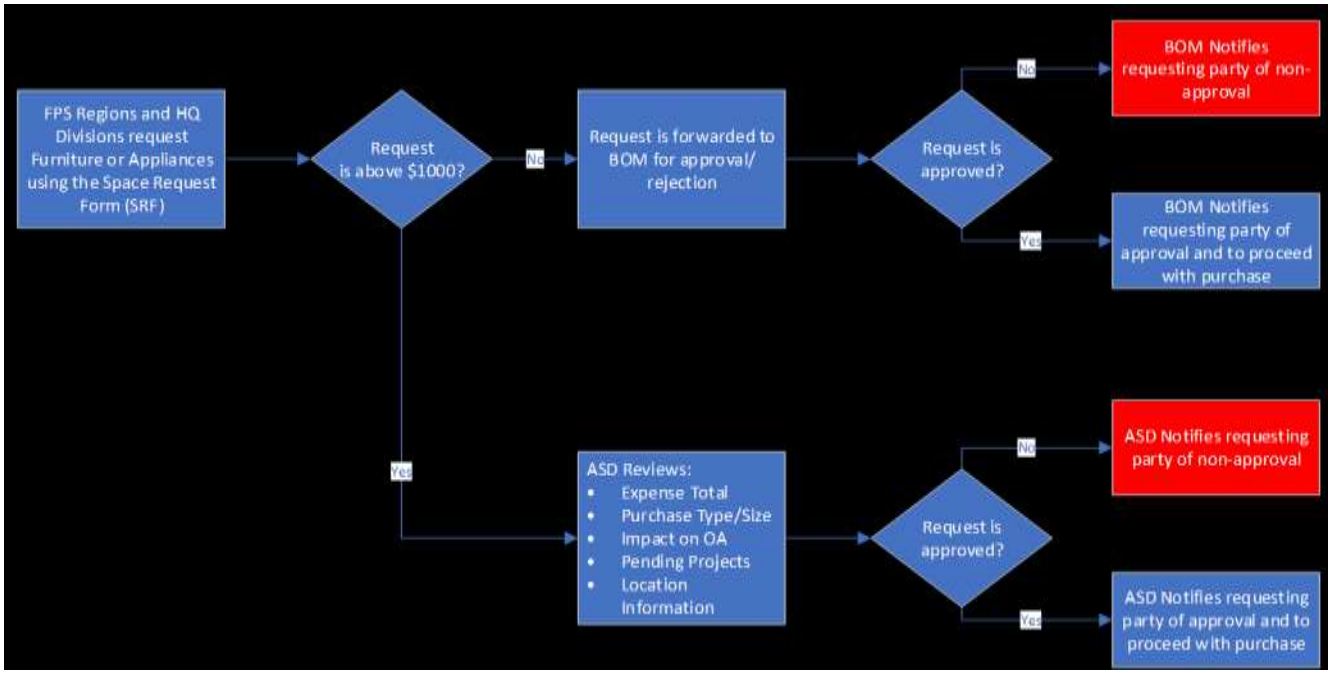


FIGURE 3: Furniture Replacement Process

3.5 TELEVISIONS

Televisions reinforcement (blocking) and conduit will be provided for new construction in all offices rated the status of Branch Chief or above. Purchase of televisions shall be the sole responsibility of the Regions except for conference rooms, break rooms, and training rooms for new construction only (ASD will purchase these). Televisions shall be wall mounted with pivot brackets typically in the middle of the wall across from the furniture (on the same side as the door location). Blocking shall be installed at the TV mount location during construction. The power outlet and cable shall be mounted at 60" above the finished door. See Appendix C for more specific details. Existing offices may be retrofitted to accommodate TVs and may require special mounting brackets in lieu of wall bracing, this may require cutting and repairing drywall to install cabling after the fact.

Energy Star and Electronic Product Environmental Assessment Tool (EPEAT) rated televisions will be purchased.

3.6 EXCESS FURNITURE

Furniture Excess disposal or abandonment is the sole responsibility of the region to initiate and coordinate. The Furniture disposal process (If FPS cannot reuse the furniture, GSA may be willing to accept the furniture allow it to remain in place) is a minimum of 60 days and should be started no later than 45 days after the notice of termination is issued to ensure all items are removed by the termination date. Please Note: Furniture being left in the space is considered hold over by tenant and will result in GSA continuing to bill rent for the space.

In accordance with FPS excess reporting procedures, all excess furniture must be reported on the SF120 and sent to fpspropertymanagement@fps.dhs.gov for processing. Refer to the Property Management Manual for guidance on the furniture disposal process.

CHAPTER 4 - ANTENNAS

4.1 OVERVIEW

Antennas play a critical role and functionality in FPS facility missions and processes (See Figure 2, Chapter 2), allowing the facility to expand communications across great distances. All efforts are made to research and account for the acquisition and installation of antennas in new construction schemes, but because of new construction (obscuring the pathway of travel), and increased requirements, installation may be required after the initial set-up.

4.2 ANTENNA ACQUISITON

At the current time, the Joint Wireless Program Management Division of DHS is working on a new initiative referred to as Tactical Wireless Communications (TacCom) to determine how many antennae are needed and how to obtain appropriate funding.

Most of the current antennae within the FPS footprint are located on federal property or alternatively on private property. Requests for antenna capabilities should be initiated through the ASD space request form (SRF) located on the SharePoint site. The request must be submitted along with a brief description of why an antenna is needed and what it's intended operational impact will be.

Antenna relocation (if deemed necessary by FPS TacCom or GSA for property disposals takes approximately 120 to 180 days. This process should start as soon as it is established that the space is being vacated if moving to another site. ITD/TacCom will handle relocation and site determination for the antenna(s). If GSA leasing action is required this may take additional time, ASD must coordinate this action with ITD/TacCom. Most antennas are located on or within historical properties, ITD/TacCom will determine if there is a requirement to engage the National Historical Society.

Note: ECO needs to review requirements for antenna program due to environmental restrictions such as migratory birds, endangered etc.

CHAPTER 5 - EXPLOSIVE SAFES

5.1 OVERVIEW

For explosive safes and training aids FPS follows FPS Directive 15.5.12.1 Firearms Policy, December 15, 2010 and GSA Explosive Canine Training Aids (ECTA) Policy for storage of Explosive Materials in GSA Owned Buildings and/or on GSA-Owned Property, 2015. The GSA Guidance is based on the National Fire Protection Act (NFPA) 49: Explosive Materials Code. This code identifies reasonable levels of safety for the manufacture, transportation, storage, sale, and use of explosive materials, including blasting agents, water gel and emulsion materials, smokeless propellants, black powder propellants, and small arms ammunition.

5.2 REQUIREMENTS FOR EXPLOSIVE SAFES

The following requisites are imperative regarding the storage of an explosive safe. These requisites ensure that storage of an explosive safe meet necessary safety precautions and remain in compliance with GSA's security standards. Note: The most recent inspection tag (with date) must be attached to the device

- Explosive safes must be protected and enclosed by 1 hour rated walls and ceilings.
- The safes must always be protected by a fire sprinkler.
- The safes must always be protected by a security system.
- The perimeter around explosive safes must be large enough for a K-9 officer to physically inspect all four sides of the explosive safe.
- The explosive safe secure room must always contain a readily accessible fire extinguisher (certified and maintained by GSA).
- Safety Data Sheet (SDS, formally MSDS) and appropriate spill or leak plan shall be posted on or near the safe or on file and accessible to employees upon request.
- The GSA approved space must only provide storage for a single indoor explosive safe or an outdoor explosive safe converted and approved by the FPS Chief of Canine Operations Branch.
- The approved space must have lighting capabilities inside to facilitate inspection of the Explosive Safe and interior of the secure room.
- An explosive safe may only be in a GSA-owned building or on GSA-leased property.

5.3 ASD FACILITIES RESPONSIBILITIES

The FPS Canine Operations Branch (COB) must review and stay current on all explosive safe locations, as well as implement the GSA Policy for the Storage of Explosive Material in GSA-owned and/or GSA-leased property. The Canine Operations Branch must notify ASD of new locations or changes in locations. The region responsible for the new explosive safe or relocation of explosive safe must likewise complete and obtain the GSA Transmittal Request form for Storage of Explosive Material, as well as the GSA 12002 Fire, Safety, and Health (FSH) Program—Potentially High-Risk Use Permit.

Once GSA has approved request, Facilities must coordinate (with region), plan, design, execute, monitor, and close-out all Explosive Safe Projects.

5.4 FPS CANINE OPERATIONS BRANCH RESPONSIBILITIES

The FPS Canine (K-9) Operations Branch must oversee the entire life-cycle management of Explosive Safes. This includes reviewing and confirming the "Data Plate" information provided by Region (serial number, date, manufactured, and manufacturer), as well as the verification that the outdoor safe is manufactured for proper (indoor/outdoor) use, and ensuring that any and all magazines are Type 2.

Additionally, the FPS Canine Operations Branch chief must approve any conversions of outdoor explosive safes for indoor use, publish, and make available to ASD, the annual or bi-annual K-9 Officer/team graduation schedules, request and monitor funding of Explosive Safe Secure Rooms projects, verify the weight of explosives for all Explosive Safe location along with the verification of all Explosive Safe locations. This published list must be kept current, updated quarterly, and notify ASD of any changes.

5.5 REGIONAL RESPONSIBILITIES

Each region must review, determine which branch/section internally is responsible, and implement the GSA Policy for the Storage of Explosive Material in GSA-owned and GSA-leased Property. Each region shall work with ASD-Facilities to design and install explosive safes and ensure completion of the ***GSA Transmittal Form Request of Explosive Material***, and assist with the completion of GSA 12002 Fire, Safety, and Health (FSH) Program – Potentially High-Risk Use Permit.

The Region must likewise ensure the event-driven update of emergency contact information as noted on the Explosive Safe, provide and monitor funding and management of re-charge, re-certification, or procurement of hand-held Fire Extinguishers within the Region, and notify the ASD-Facilities Branch and FPS Canine Branch Chief of any planned or unplanned movement of an explosive safe. Regional employees must complete a Space Request Form for any transfer, modification, or closure of an Explosive Safe Secure room or an Explosive Safe.

In addition, the Region must design, approve, install (with internal assets if desired), and fund all Explosive Safe projects, including the coordination of requests for Funding of Explosive Safes and provide funding modifications to or for the procurement of Explosive Safes.

The Region is to submit all Explosive Safe projects in total accordance with Facilities annual "FY Facilities Project Listing" or request and should plan to complete funding in the year requested and estimate the completion date for projects to occur 28 months after submitting requests. An example would be a submission for funding in May of 2019, with the knowledge that possible funding could be received as late as 2020, and an estimated completion date occurring sometime in 2021. If this timeline is not suitable, Regions may request an Unfunded Requirement (UFR), which may impact the funding portion only. A UFR will have no impact on the construction timeline and estimated completion date.

The Region is encouraged to co-locate Explosive Safes with other DHS components, or request a location on GSA-owned property. Regions may do so by submitting a Space Request Form through the FPS Share Point.

CHAPTER 6 - SPACE REQUIREMENTS

6.1 OVERVIEW

This section establishes mandatory seating priorities (when space is available) for all FPS personnel at various levels that occupy FPS facilities as a professional mission space. DHS Instruction 119-02-003, *DHS Workspace Standards*, provides guidelines for new space standards for the Department of Homeland Security. These new space standards are to assist in the space design process to develop the most efficient and effective use of space including:

- To the extent allowable by mission, consider shared workstations that minimizes the amount of dedicated and assigned employee workstations (refer to Appendix E2).
- Effective collaborative workspace; and mobile work/telework considerations.
- Net (accounting for mission space, and all contractors and FTE's) square footage must be 150 Square Foot (SqFt) Per Person Utilization Rate (UR). NOTE: The UR can be less than 150 SqFt, but 150 SqFt is the maximum.

The Workspace Standards, outlined by this document, are to be utilized in FPS provided office space for all employees, staff, contractors, visitors, FTE, etc. that require office space accommodations and apply to both alterations of existing space and to new space requirements. Reference Appendix E, "Calculating a Workspace Standard Form Example."

6.2 FACILITIES ROLE

Facilities must conduct a portfolio-wide analysis, at least annually, of FPS's real property portfolio and operations to validate the status quo or make recommendations for greater efficiency or effectiveness in addition to Operations and Maintenance, projections, building "rehab's" and addressing space concerns and requests. Facilities also plays an integral role in:

- Improvements, operational efficiencies, inventory adjustments and/or changes, or consolidations or co-locations of space.
- Assist DHS management in developing asset and portfolio management plans, and in conducting lifecycle cost/benefit analyses of strategic and tactical alternatives.
- Collateral duty such as union, acting, details (will not receive dedicated office space).
- Regulate space utilization and space effectiveness goals and metrics.
- Advocate for new development in the industry in terms of workplace strategy and real property use patterns; and research data, forecast and surveys.
- Weekly and monthly reporting for Facilities including updates to RPDW.

6.3 IDENTIFYING NEED FOR SPACE

Identifying the need for new space is the first step in the planning process. The need for space may derive out of a lease expiration, mission driven growth, operational efficiency needs or the necessity of time (i.e. – aging furniture, building issues, maintenance or other need). This is a joint effort with the Zonal PM's, regions, and operations. All parties must be in concert with each other and communicate their issues and or needs and address them/plan for them accordingly using the Space Request Form (SRF) located on the Facilities SharePoint site (See Figure 4).

6.4 BUDGET DEVELOPMENT

Once the need for space has been identified, the request is entered the SRF on the SharePoint site. This request goes to Facilities group mailbox (fpsfacilitiesbranch@fps.dhs.gov) for processing. Facilities will facilitate the space request requirements, along with the Real Property Management Manual and develop the Program of Requirements (POR). The POR, a qualified/verified space requirement, will be sent along with the Agency Specific Requirements (ASR's) to assist them in providing an Independent Government Cost Estimate (IGCE). This IGCE will be used to determine the amount of funding required. Prior to the IGCE, Facilities may choose to use historic data and past project comparisons to assist their zone with furniture issues and or equipment issues that are non-HQ responsibility such as standalone HVAC units in conference rooms (if deemed necessary by GSA during design).

FIGURE 4: Typical Space Request / Modification

6.5 SEATING

Seating request forms (for HQ personnel) or link are located on the ASD SharePoint site under Space Management. All forms must be filled out to include the employee(s) name, office/cubicle location, effective move date, and contact information. Requests for seating must be submitted directly to Facilities mailbox (fpsfacilitiesbranch@fps.dhs.gov) using the HQ Seating Assignment Request Form (Appendix D) to capture the employee correctly and determine appropriate seating space. The request must be approved by requesting Supervisor, Manager or Designee for each request.

6.5.1 Seating Priorities for FPS Personnel

Offices are provided (as space allows) to GS1-4 supervisors and senior management GS-15 and above (refer to section 6.9 Space Allocation). Offices vary in sizes depending on the differentiating levels of management and well as building design. Once building is at capacity seating will be re-prioritized by grade and seniority.

Cubicles are assigned to all non-supervisory personnel including FTEs, contractors, detailed employees, and interns. Cubicles at are standardized 36 SqFt that measures 6' x 6'. These measurements include office space for LEs and administrative personnel. Vacant cubicles and offices shall not be used for permanent storage space or used as break areas. This includes microwaves, toasters and any other small kitchen appliance.

For Headquarters seating, no workstation or office shall be assigned without written authorization from the Administrative Services Division, and Facilities. Keys to Headquarters offices are distributed through the Countermeasure Operations Division (CMOD) and keys to Headquarters workstations are distributed through the Administrative Services Branch. The seating request form is located on the Facilities SharePoint site under Space Management/Space Request Form.

Furniture shall not be removed from office or workstations. All offices and cubicles must remain complete upon exiting the agency or relocation to another workstation or office; this includes all chairs, credenzas, file cabinets and wardrobes. Keys must be placed in one of the cabinets or overhead in the offices and workstations upon exit. The Divisional Office is responsible for maintaining upkeep between employee exchanges. If personnel relocate from one cubicle to another, the rolling file cabinet and wardrobe cabinet must remain with the workstation to avoid mixed matched or lost and locked cabinets. Each individual workstation has a unique locking key set number.

6.6 DEVELOPING WORKPLACE STANDARDS

DHS Instruction, 119-02-003, DHS Workspace Standards, provides guidelines for new space standards for the Department of Homeland Security, under authority of the DHS Real Property Portfolio Management Directive (DHS Directive 119-02). FPS Facility spacing allocations are based on these standards and are to be adhered to accordingly to ensure that all FPS space is being utilized efficiently. Please see Appendix E for more detail on the calculation of workplace standards.

6.6.1 Circulation – Defining and Planning

Standards and allowances for assigning and allotting space for employee workstations and support space are identified in Section 6.9. These space standards are based on administrative type and use of the facility and will be adjusted to fit mission specific uses. The space standards are intended for use when estimating the amount of space required under a new space acquisition, or the amount of expansion space that will be needed to complete a project or mission. When configuring building space, every effort should be made to adhere to these standards as closely as possible. Reasonable exceptions to the application of these standards include:

- Currently occupied space, where no growth or change in staffing is occurring;

- Occupancy of a building of historic significance, in which interior alterations to comply with these standards would either be extremely costly or greatly alter the historic character of the building and would therefore be prohibited;
- Space that is intended for short-term occupancy (one year or less); or
- Special use space such as SCIF or MegaCenters.

For further guidelines and specifications regarding the proper execution of space, please refer to section 3 of this manual and Appendix C.

6.7 SPACE ALLOCATION

The following (Table 2.0) is the allocation of space based upon grade and or mission requirements (Offices are based upon availability of space, not everyone that rates an office may get one):

#	Grade/Responsibility	Space Allocation (in SqFt)	Typical Dimensions	Space Type	Notes
Administrative (non-mission) Spaces					
1.0	Senior Executive Service (SES) Level	180	See C9	Office	
1.1	GS-15	150	See C8	Office	
1.2	GS-14	120	See C7	Office	Must be rated as supervisor
1.3	Union Office	100	See C6	Office	If requested
1.4	Guest Office	100	See C6	Office	For regional executive suites
1.5	Cubicles - All other employees (FTE or Contractor) Note: K9 cubicle & Adjudications are mission space	36	See C5	Cubicle	There are three options: Layout, File storage, K-9
1.6	ITFO/Radio/Elec Tech Lab	150	See C26	Office	Employee resides in cubicle
1.7	Break Area Small Note: Is mission space if located adjacent to mission requirements	72	See C20	Open Area / Office	More than 10 employees
1.8	Large Break Room Note: Is mission space if located adjacent to mission requirements	120	See C21	Office	Between 18 and 30 employees: **scalable**

1.9	Conference Room – Small	120		Office	Up to 10 employees (less than 10 employees = huddle space)
1.10	Conference Room - Medium	200		Office	Up to 14 employees
1.11	Conference Room - Large / Executive	300		Office	Up to 18 employees
1.12	Conference Room - Jumbo	600		Office	HQ only – holds up to 30 employees
1.13	IT Lan / Radio Rack	50		Open Area	Based upon equipment requirements to support location
1.14	IT Lan / Radio Room - Small	72		Office	Based upon equipment requirements to support location
1.15	IT Lan / Radio Room - Large	120		Office	Based upon equipment requirements to support location
1.16	Office Support Area	72		Office	10 or more employees (72 SqFt per every 20 employees)
1.17	Huddle Room (can be open or closed)	72		Office/Open Area	5 SqFt per employee, in increments of 72 SqFt
1.18	Layout / Storage / Collaborative Area Note: Is mission when adjacent to mission requirement	100		Open Area	5 SqFt per cubicle (increments of 100)
1.19	Unsecure Reception Area	36-80		Enclosure	Based upon mission requirements
1.20	LE/CI/K9 One Employee Office	150		Office	One x 36 SqFt Cubicle, Printer support, open shelving storage
1.21	LE/CI/K9 Two Employee Office	300		Office	Two x 36 SqFt Cubicles, Printer support, open shelving, bulk storage
1.22	LE/CI/K9 Three Employee Office	450		Office	Three x 36 SqFt Cubicles, Printer support, open shelving, bulk storage, Secure Storage
1.23	LE/CI/K9 Four Employee Office	600		Office	Four x 36 SqFt Cubicles, Printer support, open shelving, bulk

					storage, Secure Storage, Small Conf Rm, SM break area
1.24	Gymnasium (Gym)	600		Office	See drawing for notes
Mission Space					
2.0	Regional Combined Training/Conf Room	1200		Office	Region offices only. Must have tactical component to be considered mission space
2.1	Mat Room (When not available within reasonable driving distance)	500		Office	Includes 80-100 SqFt for storage
2.3	Lockers/Showers Note: Mission when supporting mission essential personnel	300			See drawing for notes
2.4	Restroom	300		Enclosure	Required where Gym is required or public bathrooms unavailable
2.4	Hotel Station Note: Is mission only when adjacent to mission requirement	36		Cubicle	Shared (consider sit/stand)
2.5	Interview/Observation Room	200		Office	Usually in District Offices Only, based on mission requirements
2.6	Detainee Holding	72+		Varies	Can be open area depending on design. Scalable based on mission requirements
2.7	Explosive Safe	100		Office	Explosive safe can be combined with K-9 storage when available. There are three sizes, determined by OPS
2.8	Bulk Storage Note: Is mission when adjacent to mission requirement or contains mission essential supplies	Varies		Varies	1 to 9 employees receive open storage 10 employees and greater = 10 SqFt per person

2.9	Evidence/Secure File	Varies		Varies	1 to 7 LE's = safe, 8-14 = 120 office, above 15 = 10 SqFt per LE
2.10	Tactical Storage	Varies		Varies	1 to 9 LE's receive open shelving, 10 or more LE's = 10 SqFt per LE
2.11	Ammo / Weapons	Varies		Varies	1 to 7 LE's = safe, 8-14 = 120 office, above 15 = 10 SqFt per LE
2.12	Bike Storage	120		Office	<10 bikes do not require separate storage, >10 bikes = 120 SqFt space
2.13	SCIF	800		Office	Designated requirement by OPS/MgMt
2.14	Mission Briefing Room	120		Office	Mission briefing room must be adjacent to mission requirement

Table 2.0 Space Allocation

CHAPTER 7 - CONSTRUCTION DESIGN GUIDELINES

7.1 OVERVIEW

This chapter establishes the construction and design standards that all FPS facilities must be built. Adhering properly to the GSA-mandated building codes ensures necessary security, privacy, layout and structural integrity that is essential to carrying out administrative, storage, Sensitive Compartmented Information Facility (SCIF), and mission space purposes and projects. Listed below are the areas of appendices specifically outlining construction design codes and guidelines for obligatory FPS spaces.

7.2 ADMINISTRATIVE SPACES

Reference Appendix C pages 4 through 25 for the construction guidelines for Administrative Spaces.

7.3 MISSION SPACES

Reference Appendix C pages 26 through 28 for the construction guidelines for Mission Spaces.

7.4 STORAGE SPACES

Reference Appendix C pages 29 through 35 for the construction guidelines for Storage Spaces.

7.5 SCIFS

Reference Appendix C page 37 for the construction guidelines for SCIFS.

CHAPTER 8 – PARKING POLICY

8.1 OVERVIEW

This section establishes parking requirements, agreements, and technical processes enacted when acquiring an FPS parking space. As part of the Occupancy Agreement and Space Management program, ASD is chartered with controlling parking at all FPS locations nationwide. The need for parking is dependent on the office type, individual employee position, LE categorization, fleet allocation, and the geographic location of the facility. For parking allowances see Section 8.3.1, Table 3, Occupancy Agreements. This policy is directed to FPS LE personnel only. Non-LE personnel and parking needs will be reviewed and allocated based on OA/Lease terms, parking space market rates, and need. See the DHS Parking Program Directive 123-01 for additional information on parking.

8.2 SHARED PARKING SPACES AND PARKING NOTATIONS

Shared parking spaces are allocated using a 2:1 ratio for LE (non-supervisory and Police Officers) personnel. This is determined by the function, job duties, and percentage of time everyone spends within the office.

Select regional offices may be approved for Dedicated/Unreserved parking spaces specific for FPS usage if spaces are used for spare vehicles or inclement weather presents a risk to FPS personnel. Written justification for additional parking spaces must be submitted by the Region's DRD or RD to ASD for consideration and approval.

8.3 PARKING AGREEMENTS

8.3.1 Occupancy Agreements (OA)

Parking is included in the occupancy agreement for LE personnel and Government vehicles only (this does not include HQ parking required by LE personnel). Personal vehicles are not permitted government funding on an OA. The LE vehicle ratio for an FPS office is 2 to 1 or two LE sharing one parking space. GSA shall provide handicap parking in accordance with ADA guidelines (based on total number of spots required). GSA controls structure and surface parking on a first-come, first-served basis. However, if any additional parking is needed, the "Facilities Request and Submission Form (FRSF)" must be submitted through the ASD SharePoint site. The following table outlines the current parking protocol for Law Enforcement and Senior Level management.

FPS Position	Parking Space Type	Spaces	Notes
Assistand Director of Field Operations (ADFO)	Dedicated Reserved	1	
Deputy Assistand Director of Field Operations	Dedicated Reserved	1	
Regional Director	Dedicated Reserved	1	
Deputy Regional Director	Dedicated Reserved	1	
LE - District Commander	Dedicated Unreserved	1	
LE - Area Commander	Dedicated Unreserved	1	
LE - (K9) Officer	Dedicated Unreserved	1	
LE - Criminal Investigator	Shared Unreserved	0.5	
Police Officer	Shared Unreserved	0.5	
Criminal Investigator	Shared Unreserved	0.5	
Visitor Parking Space	Dedicated Unreserved	1	Regional & District offices **only**, one each
Administrative Vehicle	Dedicated Unreserved	1	Regional offices **only**
Spare Vehicle	Dedicated Unreserved	1	RD & DC = 1 spare per 15 LE assigned, AC only if >10 LE assigned

TABLE 3: Protocol for OA Parking

CHAPTER 9 - CONSTRUCTION REQUIREMENTS

9.1 OVERVIEW

The following section establishes a comprehensive set of requirements when it comes to the construction of FPS facilities. Compliance with General Services Administration (GSA) specifications and/or lease, Underwriters Laboratory (UL)), National Institute of Standards and Technology (NIST), Federal Information Processing Standards, Interagency Security Committee (ISC) Security Standards for Leased Space, DHS Office of Security "Physical Security Construction and Equipment Specifications Handbook" and Homeland Security Presidential Directive 12 is required for all FPS construction projects. GSA is additionally responsible for ensuring that all local codes and ordinances are adhered to as well.

9.2 PHYSICAL/SECURITY REQUIREMENTS

9.2.1 Contractor Security Requirements

FPS Countermeasure Operations Division (CMOD) / Personal Security Division (PSD) may require that the Contractor have the following qualifications: FBI Fingerprint checks and NCIC checks as needed for contracted personnel completed prior to allowing access as per GSA Lease.

9.2.2 Perimeter, Demising and Secure Wall Requirements

Reference Appendix C pages 1 through 3 for wall requirements. (Note: Ceiling height shall be minimum of 6'-8")

9.2.3 Perimeter Wall

Typically, a perimeter wall is a building exterior wall or an interior wall that abuts non-public core space. It is a wall located on the outermost perimeter of FPS occupied space that is now also a demising wall separating FPS from adjacent tenants or public common building space. Perimeter walls should meet the lease standards. The Lessor shall provide a level of security that prevents unauthorized entry to the space during non-duty hours and deters loitering or disruptive acts in and around the space leased.

9.2.4 Demising Wall

A full height, slab to slab wall with acoustical batting (3"), that separates FPS occupied spaces from adjacent tenants or public common building spaces. Demising walls within federal buildings will adhere to the GSA PBS P-100 (Facility Standards for the Public Buildings Service) criteria for Tier 1 High Performance Metal Stud Partitions. CMOD will evaluate the overall security of the facility to ascertain if secure walls are required for demising walls, new or existing. Those recommendations will be forwarded to the ASD.

9.2.5 General Construction of New Demising Walls

In the absence of a contractual or code requirement, the following stipulations must be adhered to at a minimum.

Slab to slab, sixteen (16) gauge metal runner, at the top and bottom, anchored with Power-actuated fasteners (PAF) spaced at six inches (6") O.C., three quarter inch (3/4") deep; Sealant placed top and bottom, both sides; Sixteen (16) gauge metal studs spaced at sixteen inches (16") On Center (O.C.); One layer of type "X" five eighths inch (5/8") gypsum wall board on both sides; taped and finished with joint compound and painted slab to slab. Three inch (3") acoustical batting, the entire height and width of wall.

Sheet metal ducting into the space will have man bars on a steel angle frame, framed at the wall at duct opening. If security mesh is required, add one layer of (9 or 10) gauge metal security mesh inside the wall board, on the threat side, welded or screwed to the metal framing at six inches (6") O.C. vertically at each stud and horizontally along the

true floor and true ceiling plates. If screwed, use diamond shaped fender washer designed for that purpose. Joints will overlap at the studs to provide strength.

9.2.6 Secure Wall (New or Existing)

A full height, slab to slab wall with acoustical batting (3") (if applicable) and security mesh, that separates FPS secured spaces from adjacent FPS space, adjacent tenant space or public common building space. CMOD will evaluate the building condition to ascertain if secure walls are required to be slabbed to slab or due to site-specific circumstances, terminated at a suitable height and then integrated into a hard ceiling over the secure space. Those recommendations will be forwarded to the OAFM Project Manager.

9.2.7 General Construction of Secure Walls

Secure wall must be slab to slab, sixteen (16) gauge metal runner, at the top and bottom, anchored with PAF spaced at six inches (6") O.C., three quarter inch (3/4") deep; Sealant placed top and bottom, both sides; Sixteen (16) gauge metal studs spaced at sixteen inches (16") O.C.; One layer of type "X" five eighths inch (5/8") gypsum wall board on both sides; taped and finished with joint compound and painted slab to slab. Three inch (3") acoustical batting the entire height and width of wall as required. Sheet metal ducting into the space will have man bars on a steel angle frame, framed at the wall at duct opening. Also, add one layer of (9 or 10) gauge metal security mesh inside the wall board, on the threat side, welded or screwed to the metal framing at six inches (6") O.C. vertically at each stud and horizontally along the true floor and true ceiling plates. If screwed, use diamond shaped fender washer designed for that purpose. Joints will overlap at the studs to provide strength.

9.3 PERIMETER, DEMISING AND SECURE AREA DOOR REQUIREMENTS

These requirements will apply for those areas of the project that are not covered in specific space requirements. For security reasons, the number of perimeter suite and facility doors will be minimized.

9.3.1 Construction Requirements for High Security Doors

Doors shall be constructed of solid wood with a minimum of measurement of one- and three-quarter inches (1 ¾") thick with a welded steel door frame assembly mounted to sixteen (16) gauge metal studs. The door can also be constructed of sixteen (16) gauge metal cladding over wood or composition materials measuring a minimum of one- and three-quarter inches (1 ¾") thick. The metal cladding shall be continuous and cover the entire front and back surface of the door.

Facility perimeter, metal fire, or acoustical protection doors will be a minimum of one and three quarters inches (1 ¾") thick. High security doors must be hung in a metal frame. Steel doors hung in a metal frame are acceptable if that is the building standard door. High security door frames must be of sufficient strength to preclude distortion that could cause improper alignment of door alarm sensors, improper door closure or degradation of audio security hardware.

In addition to a card reader and/or high security locks, all doors for secure area require a minimum one-inch (1") throw deadbolt lock (refer to DHS Management Directive 11030.1, Physical Protection of Facilities and Real Property (Issue Date April 21, 2003).

Special Note:
Perimeter double doors, glass doors, and doors with louvers are not acceptable, with the only exception being the public door leading into a reception area. High security door hinge pins must be installed internal to FPS space. When those doors must be installed, if the hinge pins are exposed in the unsecured area, hinges with non-removable hinge pins and security pegs must be installed.

A metal outside escutcheon plate will be installed for the approved lockset on high security doors. All door installations must retain the anti-shim features of the locksets used. On doors which swing outward, a steel protector plate which precludes access to the latch bolt must be installed. High security doors require a heavy-duty commercial grade automatic door closer.

9.3.2 High Security Locks (Perimeter Doors and where applicable)

All door hardware is required to be Heavy Duty Grade A Mortised Hardware storeroom function lock with a minimum 1" throw deadbolt and must accept high security cylinders compatible with pyramid key control meeting Underwriters Laboratory (UL) Standard 437 Key Locks, American National Standards Institute (ANSI) Standard A156.30-2003, American National Standards for High Security Cylinders, and ANSI Standard 156.5-2001, American National Standards for Auxiliary Locks and Associated Products.

This applies to those doors indicated in the specific space requirement, Perimeter doors and other doors identified by the FPS OPR/SMU Physical Security Facility Construction Project Manager.

Doors to be utilized for emergency exiting only are to have no exterior hardware.

9.3.3 Duct Work Openings

All vents, ducts, and similar openings in excess of ninety-six (96) square inches that enter or pass through a suite perimeter wall identified by CMOD must be protected with either man bars or grills on a steel angle frame, framed at the wall at duct opening. CMOD must verify and inspect the materials used and the construction of the vents to verify barrier installation. An access port to allow visual inspection of the protection in the vent or duct must be installed inside the secure perimeter of the space. If the inspection port must be installed outside the secure perimeter, it must be able to be locked.

If one dimension of the duct measures less than six inches (6"), or the duct is less than ninety-six (96) square inches, bars are not required. If bars are used, they must be one half inch (½") diameter steel welded vertically and horizontally six inches (6") O.C.; if grills are used, they must be of thirteen (13) gauge expanded steel; if commercial sound baffles are used, the baffles or wave forms must be metal permanently installed and no farther apart than six inches (6") in one dimension. A deviation of one-half inch (½") in vertical and/or horizontal spacing is permissible.

9.3.4 Exterior Windows

All Exterior windows must meet the GSA Standard Test Method for Glazing and Window Systems Subject to Dynamic Overpressure Loadings 3b rating of protection.

9.4 OFFICE AND CUBICLE IDENTITY SIGNAGE

All signage such as cubicle identity plate identifying cubicle or office number must remain visible on that office or cubicle at all times. Employees shall not remove or modify this identification. However, updating the name insert is permitted. The font protocol shall comply with Policy, Communications & Engagement (PCE).

Signs must have the names of the individuals that will occupy the space.

9.5 INFORMATION TECHNOLOGY BUILD-OUT STANDARDS

The following policy is to establish a standard for items related to Information Technology, including: Network Connectivity & Communications, Video Tele-Conference (VTC), and Audio/Video (A/V). For ASD space projects, all requesters are to submit an Information Technology Business Requirements (ITBR) form to the IT branch representative. The attached RACI *(Responsible, Accountable, Consult, and Inform)* developed between HQ ASD and ITD establishes roles & responsibilities for the completion and processing of the ITBR.

9.6 Network Connectivity and Communications:

Office buildouts will use a standard network connection plate consisting of two (2) RJ-45 ports and one (1) RJ-11 analog phone line. Optional VOIP system may be used.

FPS Office Size (Headcount Total)	Connection Type
Total < 6 People	High-Speed DSL*
Total > 6 People	T1 Connection
* Connectivity is contingent on service availability. If service is not available or efficient, the use of Wireless Air-cards and Tokens may be issued for network access.	

TABLE 4: Connection Type

9.7 VIDEO TELECONFERENCE (VTC)

FPS Video Teleconference systems (inclusive of business Skype, Adobe Connect, Microsoft teams or other approved IT meeting software) are intended to provide remote meeting and communication capabilities between FPS offices and other federal agencies at a national level. Standard placement for VTC systems is approved for the following offices: HQ, ADFO offices, Regional offices. Approved FPS offices will be equipped with one (1) VTC system. All equipment selected shall be identified on the FPS ITD approved and non-classified technology list. All equipment selected shall be ENERGY Star and EPEAT rated. EPEAT level rating shall be stated in request forms.

Requirements for service, installation, training, and non-standard hardware will be coordinated through and approved by FPS HQ – ITD. FPS VTC hardware costs are capped at $18,000.00. Estimates and/or requests that exceed this approved price cap must be submitted to the ITD for approval. In accordance with the FPS Personal Property Instruction Manual 15.2.4.4-01, Section 1.4.1 – FPS Accountable Property Officers (APO), VTC equipment is considered personal property and is loaded and tracked through Sunflower.

CHAPTER 10 - OPERATIONS AND MAINTENACE

10.1 OVERVIEW

This chapter deals with processes and procedures for managing the operations of building space after the space is occupied by FPS.

Operations and Maintenance (O&M) covers a wide array of services that together deliver a properly and efficiently functioning facility. These services range from janitorial services to the daily operation of the building systems to scheduled maintenance programs. Operations and maintenance are inextricably linked, as proper operation is dependent upon proper maintenance.

A comprehensive Operations and Maintenance (O&M) Program promotes effective and efficient use of resources by preserving physical assets in a safe, operable and dependable condition. Facilities with successful O&M Programs are more efficient, reliable and have lower operational costs. Properly implemented O&M programs will also extend the useful life of most facility equipment. Where standards are outlined for owned facilities, components in leased facilities can use the standards to ensure that service level requirements are met by GSA and/or applicable service providers.

10.2 OPERATIONS AND MAINTENANCE WORK (O&M)

Facility operations and maintenance work is classified as minor maintenance and repair on a building, utility system, real property installed equipment, mobile emergency generator (if required), roads, pavements or natural habitat costing less than $25,000 per work order. It does not include construction or alteration. O&M work must be routed through GSA for approval unless if facilitates the construction and alterations in which case an RWA will be required. It is funded from the regional program funds. Coordination with the ECO is required outside of minor repairs. Any repairs for buildings older than 45 years requires ECO coordination.

10.3 BUILDING SERVICES

Buildings within the NCR are managed by Facilities. Facilities is responsible for the ongoing O&M of these buildings. Outside of the NCR, the Region is responsible for the ongoing O&M of their buildings.

FPS and its Environmental Compliance Analyst (ECA) must provide occupancy services that substantially conform to nationally recognized standards.

As needed, the ECA may adopt other standards for buildings and services in federally controlled facilities to conform to statutory requirements and to implement cost reduction efforts.

Building services, such as custodial, solid waste management (including recycling), heating and cooling, tenant alterations, minor repairs, building maintenance, integrated pest management, signage, parking, and snow removal, are to be provided at appropriate levels to support Federal agency missions.

Operations, maintenance, and repair functions at FPS facilities shall be supported with a combination of funding, space, equipment, and staffing that is sufficient to operate, maintain, and repair the facilities in accordance with applicable Federal standards and recognized industry standards relevant to the use of buildings or other facilities of similar types, age, and physical condition.

Life cycle costs for all non-standard HVAC systems, appliances, copiers, any equipment (non-IT) that is purchased by FPS and not covered under a lease or maintenance contract

10.4 GSA MANAGEMENT SERVICES

GSA Management Services provides for the standard operation and maintenance of all government occupied space assigned to federal agencies. GSA's Building Manager is responsible for ensuring that all equipment is properly maintained in operating condition and all building space is fully maintained as detailed in the lease. Such items include but are not limited to:

- Carpet repairs and installation;
- Janitorial services;
- Government-owned HVAC equipment;
- Government-owned generator;
- Door hardware and keys (restrooms, private offices, and suite entry) - does not include PAC systems;
- Installation and removal of government owned artwork, whiteboards, and tack boards;
- Removal to include repairs to walls, ceiling and flooring; and
- Post-occupancy building alterations: walls, lighting, HVAC, electrical, telephone and data access points, and related building finishes.

10.5 REIMBURSABLE WORK AUTHORIZATION (RWA'S) FOR MAINTENANCE

FPS will provide funds to GSA through RWAs to maintain equipment installed to meet specific FPS/DHS requirements, such as supplemental HVAC equipment. On an annual basis, Facilities will issue RWAs for maintenance and repairs of equipment installed for FPS in each occupied space. Facilities will also issue RWAs for preventative maintenance (PM) contracts for regularly scheduled maintenance and repairs for the following:

- Government-owned HVAC;
- Overtime utilities (where applicable);
- Government-owned generator;
- Re-fueling for the generator;
- Regions are required to provide the funds for these RWAs; and
- FOB monitors all vendor work in support of equipment maintenance and repairs.

Facility Equipment Malfunctions: Breakdowns of facility equipment should be reported to the respective building manager. ASD works with GSA and the Lessor's Property Manager or contractor to execute repairs on a 24/7 basis.

Coordination with the FPS Environmental Office is required outside of minor repairs, especially if in buildings that are 45 years of age or older. Note: May require review by historic preservation specialist to determine threshold

10.6 FUNDING AND FINANCIAL

Facilities is authorized to maintain oversight control of all funding and financial matters concerned with the building spaces and other real property occupied and owned by the Directorate. Accordingly, the FPS regions will provide the appropriate information to Facilities as required.

10.7 PREVENTIVE MAINTENANCE PROGRAM GUIDELINES

These are preventive maintenance standards, developed, for equipment and systems commonly found at FPS facilities. They are to be used as the basis of the facility maintenance plan if O&M manuals do not exist or are not available.

Coordination with the FPS Environmental Office will be required for actions on buildings 45 years of age or older.

10.7.1 Preventive Maintenance

Preventative maintenance is regarded as an activity based on set time or interval established for the purpose of maintaining facilities, systems or components at a specified level of performance. Preventive Maintenance is an essential part of the upkeep regarding FPS facility equipment and space and should be budgeted for and scheduled accordingly. See section 10.9 for more information on maintenance budgeting as a facility process.

10.7.2 Breakdown Maintenance

Breakdown Maintenance is regarded as an activity involving the restoration of failed or failing equipment or system to a defined level of performance. Breakdown maintenance should be budgeted into facility processes regarding equipment or system upkeep. Section 10.11 establishes how to properly facilitate breakdown maintenance regarding the system's Expected Useful Life (EUL).

10.8 RENT

FPS pays GSA a fee for occupying GSA-assigned space (excludes GSA owned space such as control room(s) and electrical closets. Control rooms would be paid for on a pro rata basis shared by the agencies requiring the guards. Rent payments go into the Federal Buildings Fund, a revolving fund from which GSA allocates its facility purchases, facility maintenance, repair, alteration, construction projects, and leases. Each Rent charge is calculated by adding a small surcharge to the appraised fair-market rental of the space, and it is updated every three years.

10.9 OPERATIONS AND MAINTENANCE BUDGETING

Each region typically is assigned to develop the annual O&M budget. This entity is also responsible for controlling costs within the allocated budget for each building under its control as well as ensuring the correct performance of tasks by the building/facility owner. A typical O&M budget would include, but is not limited to, items such as:

- Energy and Other Utilities;
- Janitorial Services;
- Security;
- Preventive/recurring maintenance; and
- Antennas.

10.9.1 Maintenance Budgeting

Maintenance is the upkeep of property to offset serious deterioration, including the preservation of certain types of equipment and special characteristics of historic property. The primary means of preservation are; inspection, adjustment, lubrication, cleaning and the making of minor repairs. Ordinary maintenance is routine recurring work that is incidental to everyday operations; preventive maintenance is work programmed at scheduled intervals. A properly established preventive maintenance program will reduce energy consumption, increase equipment life, and reduce operational costs. Component maintenance divisions provide standards and requirements for FPS facilities.

Typical maintenance activities that should be planned, budgeted for, and managed include, but are not limited to, the following:

- Preventive Maintenance;
- Predictive Testing & Inspection (PT&I);
- Programmed Maintenance (PGM);
- Repair;
- Trouble Calls;
- Replace of Obsolete Items; and
- Service Requests.

10.9.2 Monitoring Maintenance for Leases

Maintenance, as well as certain operations activities, included in the lease, need to be monitored. Monitoring ensures that contract terms under a lease are fulfilled by the landlord. The lease document will have a list of the items that need to be enforced, such as cleaning, landscaping, parking lot upkeep (cleaning and snow removal). For GSA leases, Facilities is the POC for discussions between GSA and the lessor, to ensure lease compliance. Note: ECO shall also review and perform audits for compliance and or recommendations.

10.10 EXPECTED USEFUL LIFE (EUL) MATRIX

ASD shall be responsible to determine when the annualized cost to maintain a building system or component exceeds its annualized replacement cost, it has then exceeded its expected useful life (EUL). In these circumstances a suitable repair need should be identified, which could be replacement of the system or component. The following organizations have published standard guides for use in calculating EUL data for various building systems and components:

- Building Owners & Managers Association (BOMA);
- RS Means or applicable cost tracking mechanism; and
- Building Cost Information Service (BCIS).

Assessors shall use these guides when identifying EUL information. Assessors shall adjust the standard EUL data to reflect individual conditions such as location, exposure, levels of maintenance, etc. Assessors should also identify systems and components that are likely to reach the end of their expected useful life during the assessment forecast period or before the next planned assessment. The unexpired life should be recorded as the RUL, and a repair need should be identified and triggered at the end of the RUL. Repair needs may not simply reflect physical deficiencies but may be required due to age and maintenance costs.

10.11 MAINTENANCE MANUALS

Operations and Maintenance Manuals are essential to the activation and long-term care of FPS facilities. Provisions in the construction or design-build contract should require the development of a consolidated operations and maintenance manual for the entire facility in both hard copy and electronic soft copy. A copy of the manual should be kept and maintained by the OPC's facilities management office and the OPC's operation and maintenance field office. The manual shall include:

- A copy of all warranties;
- As built / Record drawings of project;
- A list of all training requirements and a roster of trainees (kept at Region except for HQ NCR);
- All information necessary to optimize operations and maintenance of facility equipment and systems;
- Specific operational protocols for special and highly sophisticated equipment (such as Magnetometers);
- Standard operating procedures and parameters; and
- Commissioning results as a baseline for validation and facility performance expectations.

CHAPTER 11 - MOVES AND TERMINATION (HQ)

11.1 OVERVIEW

This section asserts the required processes regarding an FPS Space and Facility move request, relocation, forced move, box move, and the requirements that ensue for each type of relocation. Following these established processes will enable an efficient facility transition of missions, operations, and property during the event of a lease termination.

11.2 OFFICE MOVE REQUESTS

Office move requests must be submitted on the Facilities SharePoint website through the Move Request Form under Facilities/Space Management/Move Request form (Appendix D-1) no later than 14 days prior to the expected move date. Security items are handled at a regional level. When moving, it is the sole responsibility of the Region to appropriate funds for the transfer or relocation or disposal of security systems. Security devices such as cypher locks and access control systems should be removed or unsecured so that GSA can freely gain access to the facility space. Control and access of space is a major factor to stop GSA rent expense.

Additionally, keys to the space must be returned to the building manager. Cameras should be dismantled and removed. It is permissible to remove the back plates; however, they should remain intact if the new space already has a need for them. Verification of weight and quantity of weapons, safes, and ammo must be established at the Regional level. Prior to moving an explosive bunker, a GSA fire safety form must be completed for transition to a new location prior to the move.

11.3 RELOCATION

If the agency or GSA determines relocation is necessary at the expiration of an OA for either Federally owned or leased space, FPS is responsible for all costs associated with relocation at that time.

11.4 FORCED MOVE

If a GSA customer agency, or GSA, forces the relocation of FPS prior to the expiration of the customer's OA, the “forcing” agency is responsible:

- For all reasonable costs associated with FPS’s, including architectural-engineering design, move coordination and physical relocation, telecommunications, antenna’s and any other un-amortized TI cost; and
- To FPS for undepreciated amount of any lump sum payment already made for alterations.

11.5 MOVE REQUIREMENTS

When moving, delegating an individual and alternate individual to inform the group of expectations during an anticipated move will help the process to run more smoothly. A DHS move form must filled out and submitted to ASD. Similarly, it is a good principle to share this move form and seating chart with all staff and require some form of acknowledgement, this avoids staff members making or requesting last-minute, unauthorized changes which in turn add confusion for the move team and IT staff. The appointed delegate should inform personnel of the date of the physical move, the date self-packing material will arrive and be accessible to staff, and the date self-packed items are scheduled to be recovered by the moving vendor.

Additionally, the individual delegating the move should ensure that all staff is aware of maintaining location of any FPS issued laptops, Mi-Fis, tablets and cell phones (movers are instructed not to pack or touch these items) as well as making sure everything is properly labeled (items in plain site are often the ones most frequently overlooked and misplaced during a move).

Prior to moving, the FPS staff should ensure that all perishable items are removed from facility fridges, all trash cans are emptied, and that the facility area is clean after the movers have removed all the items (it is suggested to schedule staff to clean the building area at the conclusion of the move). A final walk through of the space after all moving processes have taken place is mandatory to making sure that the move can properly conclude.

At the time of the move, ITD will disconnect and reconnect all the equipment. ITD may elect to verify all hand receipts at the conclusion of the move. The movers will pack, label, and transport all monitors, desktop printers and HSPD-12 equipment as well as phones (if required) and peripherals. The copier vendor moves copier machines. No furniture is to be moved, relocated, or disposed of without the expressed permission (SF-120) of ASD Property Branch.

When transporting sensitive material, documents and files containing SBU and PII must be packed, wrapped and labeled in accordance with DHS Privacy Office's *Handbook for Safeguarding Sensitive PII*. Documents and files containing SBU and PII must be remain under watch when not under locked transport i.e. Employee Name 482K 1 of 4, 2 of 4, 3 of 4, 4 of 4. HPSD 12 room 487 (items/files/equipment - Employee Name 1 of 2).

Note: When moving, ensure SAMS is updated based on the new physical location of accountable equipment – Contact assigned APO.

APPENDIX A: DEFINITIONS

1. **Adjacencies**: A list of applicable spaces that are complimentary and/or required to be adjacent to the described space type.

2. **Agency Code**: Code GSA assigns to identify an agency in its lease portfolio.

3. **Annual Rent**: is determined by multiplying the rate by rentable square feet.

4. **Broker**: An individual or entity that acts on behalf of another person as an agent to negotiate for the lease, purchase, or sale of office space, buildings, land, or any other real estate. Sellers and Lessors are often represented by a broker, and the Government sometimes retains a broker to represent it in lease procurements. A Broker may not bind the United Sates or perform any other inherently governmental functions. The acronym "LCO/LS" is used throughout this guide to represent all leasing staff (Lease Contracting Officer, Leasing Specialist, and sometimes Broker).

5. **Building ID**: Identification number of a specific building in GSA's lease portfolio.

6. **Clauses**: Special conditions of the agreement.

7. **Communications**: The description of telecommunications requirements that include Phone/Data outlet and other special communications items.

8. **Construction**: The descriptions of the facilities, mission spaces, rooms, and all built assets residing in FPS facilities that must remain in compliance to GSA-mandated structural codes. Some of these descriptions include but are not limited to type, material, size, rating, door frame type, and hardware set.

9. **Contracting Officer (CO**): A warranted non-real estate CO for services and construction with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

10. **Contracting Officer's Representative (COR)**: A qualified individual appointed by a CO to assist in the technical monitoring or administration of a contract or lease. A COR must be a Government employee and possess the necessary qualifications (training) and experience commensurate with the responsibilities delegated to him or her. A COR can be a GSA employee, or someone selected and nominated by the client agency and then formally appointed to the contract by the Contracting Officer. Designation of COR must be in writing and enumerate the specific authorities being delegated by the CO to the COR.

11. **Direct Lease Agreement**: The official agreement made between the Agency and the General Services Administration (GSA). This agreement details the terms, rent, use and care of premises, utilities, alterations, cyclical paint and carpet. FPS does not have the delegated authority to directly lease space with lessors or sub-lease to other agencies. This process must be done through GSA.

12. **Electrical**: Electrical lighting, power, and receptacles requirements are listed and shown on plans.

13. **Financial Terms**: Costs the agency pays to GSA over the length of a term of an OA. Rent costs are determined by several factors, the rate, rentable square feet, monthly and annual.

14. **Fixed Furnishings and Equipment**: Fixed furnishings include custom millwork and other casework requirements that are commercially manufactured cabinets or furniture. Specialties and equipment sizes are based on the best available information and need to be verified for each facility.

15. **Furniture**: The proper inclusion of furniture within an FPS office space in accordance to FPS room standards; these room standards establish how space and furniture are to be utilized efficiently per the administrative level of the employee.

16. **Handshake Agreement**: An agreement made directly between the agency with GSA and or Lessor without HQ approval, written documentation and financial agreement. Not permitted by FPS personnel.

17. **Interior Finishes**: A list of materials and finishes for each space type. The list includes floor, base molding, walls, ceiling materials, and finished ceiling height.

18. **Janitorial Services**: Building services provided to the tenant agency for the operating expense portion of the rent that is made part of the lease contract related to internal and external daily and routine building cleaning. Additional or upgraded services beyond those identified in the lease shall be provided to GSA on a reimbursable basis using a Reimbursable Work Authorization (RWA).

19. **Lactation Room**: **Private r**oom provide to nursing mothers to express milk; it must be made available upon request. This space can be an office or huddle room.

20. **Last Date Modified**: Date GSA modifies document.

21. **Lease Administration Manager (LAM)**: An individual who possesses a COR's Delegation of Authority from the LCO and is responsible for day- to-day lease management and verifying Lessor's compliance with lease terms and conditions. This role may include employees who have responsibilities in both federally owned and leased buildings.

22. **Lease Contracting Officer (LCO)**: An individual holding a valid Government-issued warrant providing authority to enter and administer leases on the Government's behalf. The LCO job classification is GS-1170, Realty Specialist. The LCO has exclusive authority to enter, amend, and administer leases on the Government's behalf to the extent provided in his or her certificate of appointment as LCO. The acronym "LCO/LS" is used throughout this guide to represent all leasing staff (Lease Contracting Officer, Leasing Specialist, and sometimes Broker) during the transition process.

23. **Leasing Specialist (LS)**: Individual who assists LCOs and may perform all duties that do not legally obligate the Government. The LS's job classification is GS-1170, Realty Specialist. The acronym "LCO/LS" is used throughout this guide to represent all leasing staff (Lease Contracting Officer, Leasing Specialist, and sometimes Broker) during the transition process.

24. **Location**: Agency address for which the agreement is assigned.

25. **Mechanical**: The description of all HVAC system, Air Pressure (including exhaust) and Plumbing requirements.

26. **Memorandum of Agreement (MOA)**: is a document that describes very broad concepts of mutual understanding, goals and plans shared by parties. Funding may be required under this agreement depending on the agreeing parties.

27. **Monthly Rent**: is determined by dividing the annual rent by 12 months.

28. **Mutual Agreement**: This mutual agreement is a five-year policy document that does not obligate funding, require reimbursable work to be performed, and/or directly authorize fund transfers between the parties.

29. **Occupancy Agreement (OA) Number**: GSA assigned number to an operating agreement.

30. **Overtime Utilities**: Costs for utilities and associated services that exceed those provided during the standard building operating hours of 10 hours per day. The overtime utilities estimating process normally begins in May-June of each year with communications between GSA and the tenant agency. Confirmation of OTU needs and the necessary approvals are completed by July. The estimates are validated and signed with the agency in August, and subsequent RWAs from the customer begin in October.

31. **Photo**: Photos are only to represent an example of the space, furniture layout or function. It is not to be used as the final design or selection of finishes.

32. **Rent Rate**: Rate above and beyond the agencies usable square footage to compensate for elevator cores and other common areas. The rent rate is usually around 1.1 but may be higher due to design.

33. **Real Property**: Buildings and structures permanently affixed to land that are not equipment. Real property includes offices, warehouses, labs, housing, museums, schools, data centers, prisons, hospitals, post offices and any building as defined in the Federal Real Property Council Guidance for Real Property Reporting.

34. **Reimbursable Work Authorization (RWA)**: RWA is an agreement between GSA and a client agency, whereby GSA agrees to provide goods and services and the client agency agrees to reimburse GSA for the cost of these goods and services, indirect costs, and fees. It is a written statement from another Federal agency or non-Federal source (when authorized by statute) requesting GSA to procure commodities and services on its behalf.

35. **Remarks**: Includes supplemental information related to the criteria or use of the space, including appropriate specifications.

36. **Rentable Square Feet**: The gross area of the full floor less the area of all vertical penetrations (elevator shafts stairwells, mechanical shafts etc.)

37. **Space Description**: A generic description of the space function.

38. **Squatting**: Office space used as a workplace without authorization and rent agreement from GSA or the Agency. Not permitted by FPS personnel.

39. **Term Period**: Length of term may vary from 6 months to 10 years or more.

40. **Usable Square Feet (USF)**: The square footage used exclusively by the tenant, including the main workstation and collaboration areas, special space and circulation within the tenant space. It does not include building common areas.

41. **Version Number**: Number of versions of document as GSA makes modifications.

42. **Wall Construction**: The type of enclosing and internal wall construction the space requires.

43. **Windows**: The descriptions of the interior windows (if applicable) include frame material, frame size and glazing and exterior windows treatments (if applicable).

APPENDIX B: REFERENCES

OMB Management Procedures Memorandum No. 2015-01, Implementation of OMB Memorandum M-12-12 Section 3: "Reduce the Footprint (RTF Memo)," March 2015

US Code, Chapter 42, U.S.C. § 4321-4335 (The National Environmental Policy Act of 1969)

Chapter 36 Code of Federal Regulations (CFR) Chapter VIII, Part 800, "Protection of Historic Properties," July 2012

Public Law 111-292, "Telework Enhancement Act," December 2010

Interagency Security Committee, "Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, 2nd Edition," November 2016

GSA Explosive Canine Training Aids (ECTA) - Policy for Storage of Explosive Materials in GSA Owned Buildings and/or on GSA-Owned Property", 2015

DHS Delegation Number 00500 Revision 01, "Delegation to the Chief Readiness Support Officer," issued June 5, 2012 and incorporating Change 1 issued May 25, 2018

DHS Directive 119-02, "Real Property Management Program," December 10, 2012

DHS Instruction 119-02-001 Revision 1, "Real Property Manual," July 2, 2010
DHS Instruction 119-02-003, "DHS Workplace Standards," September 30, 2014

DHS Instruction 121-01-017-01, "Physical Security Construction and Equipment Specification Instruction Manual," March 21, 2015

DHS Directive 023-01 Revision 01, "Implementation of the National Environmental Policy Act," October 31, 2014

DHS Instruction 256-05-001, "Worksite Lactation Program," May 19, 2016

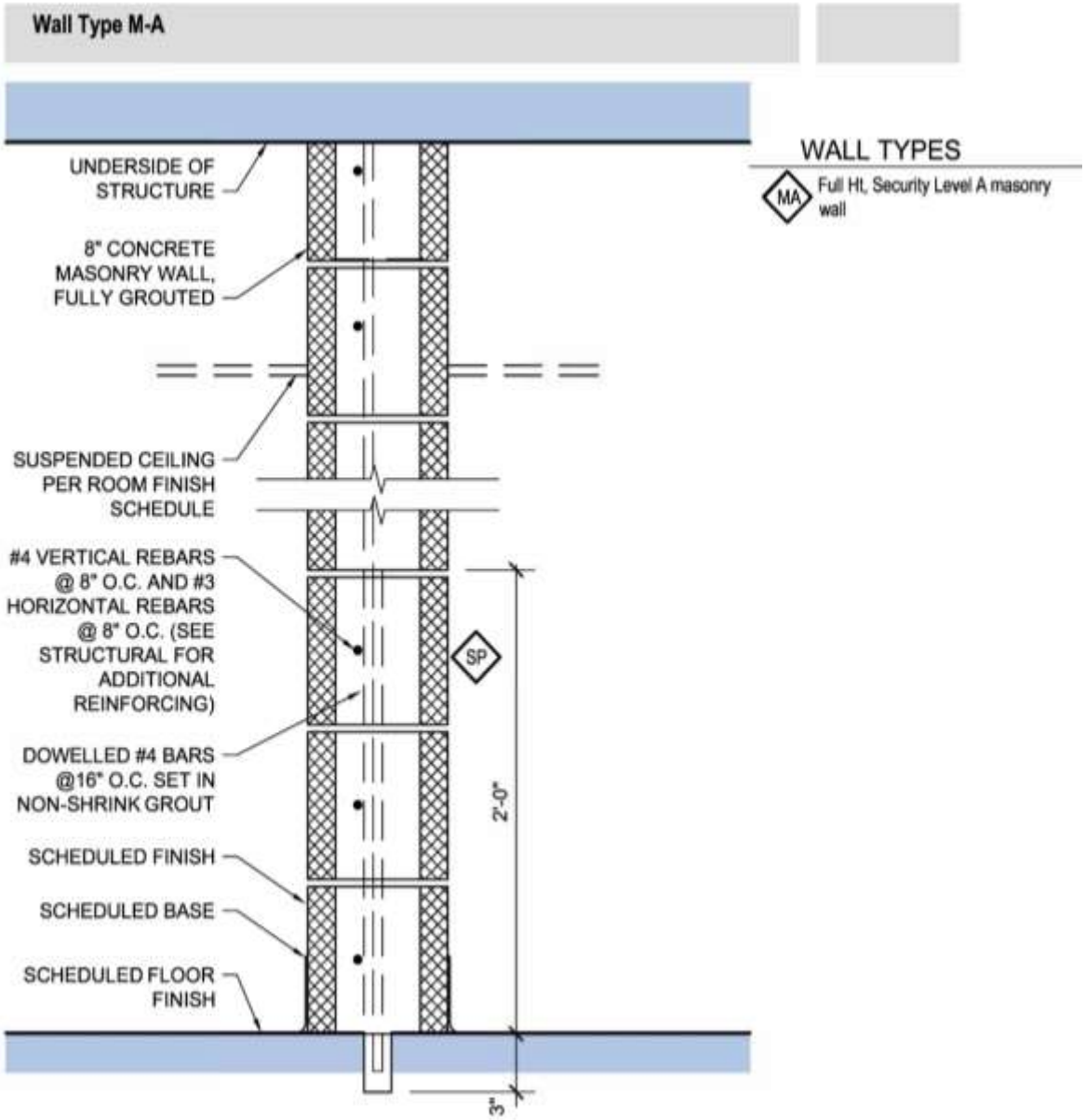
FPS Directive 15.8.1.1, Facility Security Assessment

FPS Directive 15.5.12.1, "Firearms Policy," December 15, 2010

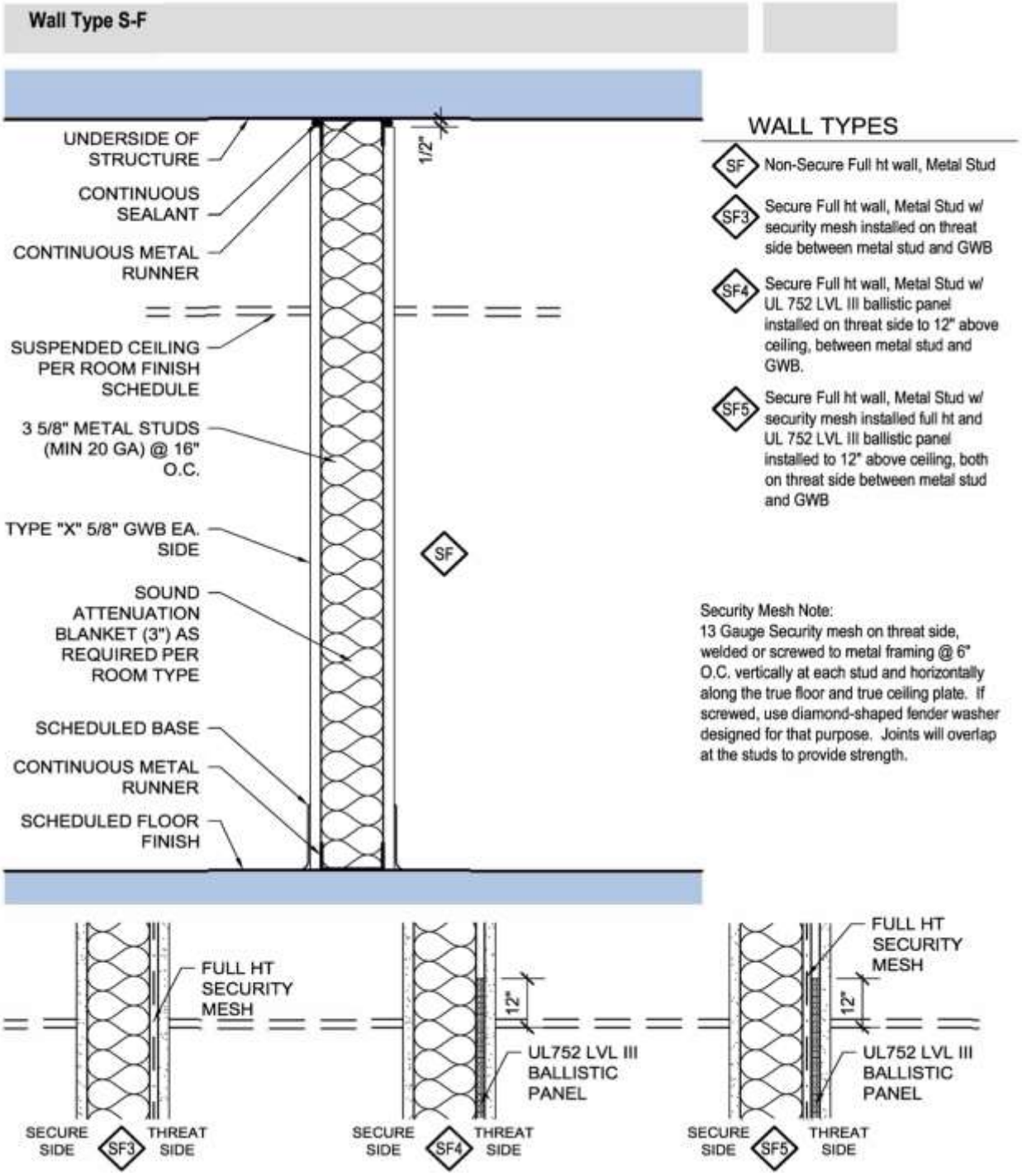
FPS Directive 15.4.7.1, "Worksite Lactation Program," May 10, 2016

APPENDIX C: FACILITY CONSTRUCTION DESIGN GUIDELINES

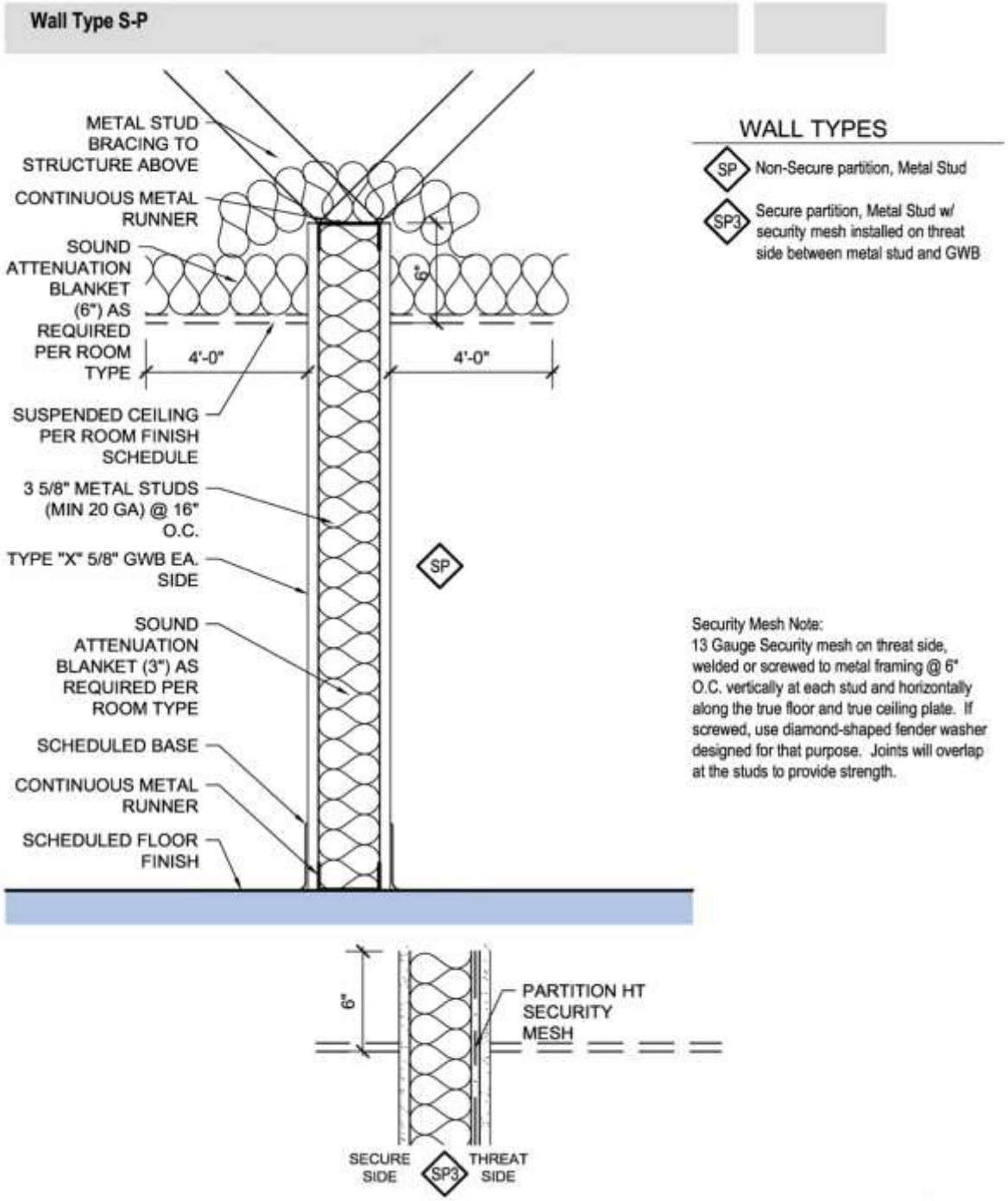
WALL CONSTRUCTION



WALL CONSTRUCTION

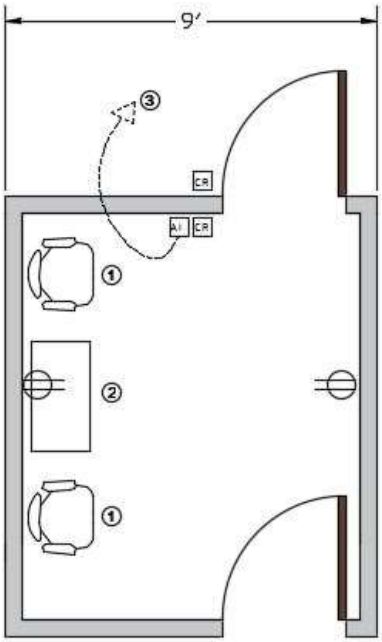


WALL CONSTRUCTION



ADMINISTRATIVE SPACES

1.19 Non-secure Foyer – 36-80 SqFt, based on mission requirements



ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS
FLOORS: BUILDING STANDARD
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: NONE
HINGES: NONE
HARDWARE: NONE
DOOR LOCKS: NONE
DOOR CLOSER: NONE
GLAZING: NONE
PLUMBING: HOT/COLD WATER WHERE APPLICABLE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: NONE
POWER: SPECIAL PLUG MAY BE REQUIRED FOR COPIER MACHINE

FURNITURE - EQUIPMENT

1. TYPICAL GUEST CHAIR
2. 18x24 TABLE
3. AI PHONE CONNECTED TO AGREED TO ACCESS POINT (CAN BE ATTACHED TO DESK, CUBICLE, OR WALL)

LEGEND:

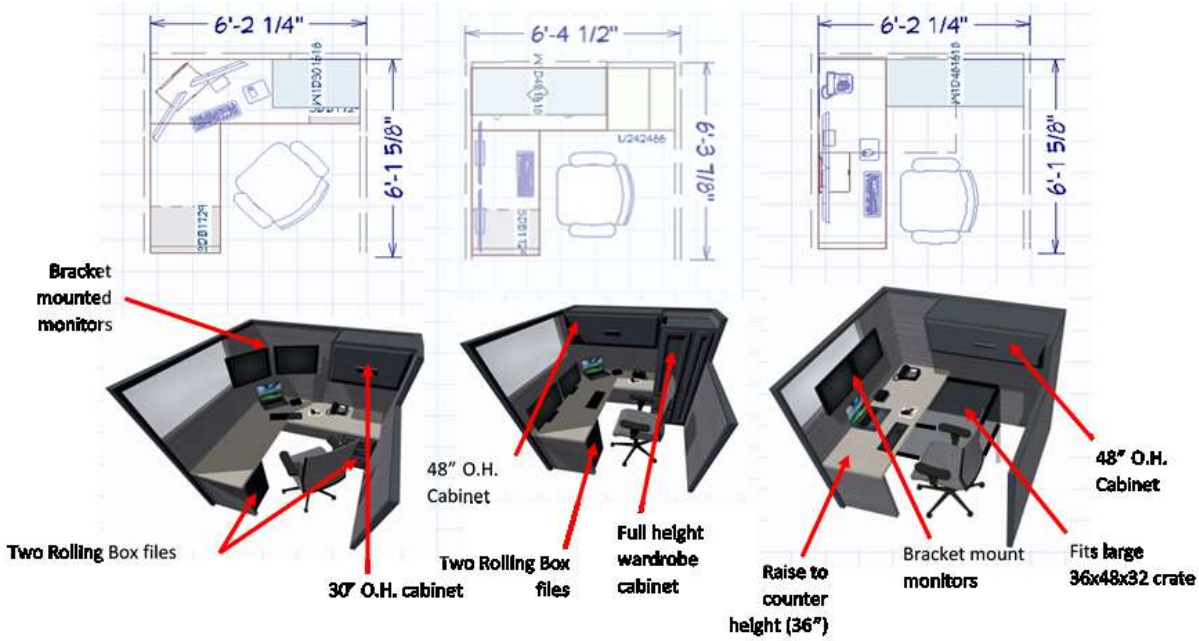
CR	CARD READER		VOICE/DATA
AI	AI PHONE		DUPLEX OUTLET
#	KEYED NOTES		

ADMINISTRATIVE SPACES

1.5 Workstations – 36 SqFt

2.4 Hotel Station – 36 SqFt

1.5 Adjudications – 36 SqFt



Maximum Layout Space Option

Standard Cubicle W/wardrobe

Canine Configuration (K-9)

ROOM SPECIFICATIONS

WALLS: TYPICAL METAL/FABRIC CUBICLE WALLS (COLORS TO MATCH FPS STANDARDS
FLOORS: BUILDING STANDARD
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: N/A
HINGES: PER CABINET MANUFACTURER
HARDWARE: STANDARD CABINET HINGES
DOOR LOCKS: STANDARD CABINET LOCK W/ INTERCHANGEABLE CORES (ALL LOCKS TO BE KEYED ALIKE)
DOOR CLOSER: N/A
GLAZING: PER MANUFACTURER/DRAWING
PLUMBING: NONE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEYED LOCKS
COMMUNICATIONS: TWO DATA AND ONE PHONE
POWER: POWER PREFERRED TO BE FED FROM ADJACENT WALL OR IN UNDER FLOOR CIRCUIT
FURNITURE: PROCURED AND INSTALLED BY FPS – FURNITURE VENDOR. VENDOR TO PROVIDE WHIPS. LESSOR TO PROVIDE POWER TO WORKSTATIONS (POWER POLES TO BE AVOIDED IF POSSIBLE). LESSOR TO PROVIDE VOICE/DATA CABLING AND BOXES (ONE PHONE TWO DATA FOR ALL CUBICLES)

FURNITURE - EQUIPMENT

1. 24" X 48" SIT/STAND DESK
2. 48" RETURN (CAN BE MOUNTED TO SIT STAND. DELETE O.H. IF PART OF SIT STAND
3. 15" BOX FILE ON WHEELS
4. 48" O.H. CABINET
5. 24" UTILITY CABINET W/FILE DRAWER, WARDROBE HOOKS AND SHELVES
6. OFFICE CHAIR
7. GUEST CHAIR

LEGEND:

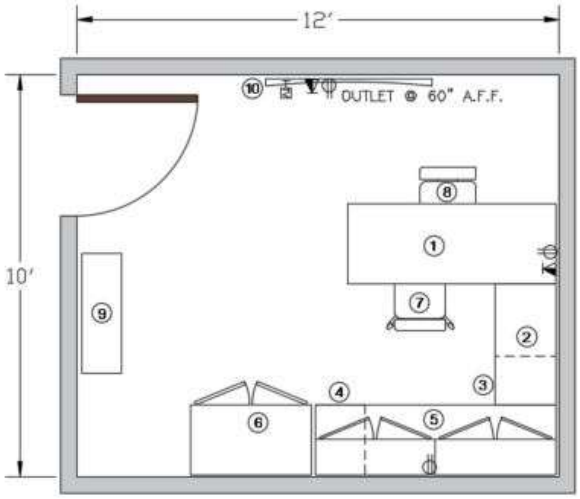
VOICE/DATA — DUPLEX OUTLET

(#) KEYED NOTES

ADMINISTRATIVE SPACES

1.2 Private Office Medium – 120 SqFt

2.14 Mission Briefing Room – 120 SqFt NOTE: Mission briefing room must be adjacent to mission support to constitute as mission space



LEGEND:

- TV
- VOICE/DATA
- KEYED NOTES
- DUPLEX OUTLET

ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID-CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20-GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON-SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE-1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE-A CERTIFIED, HIGH-SECURITY LOCK W/APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON-HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

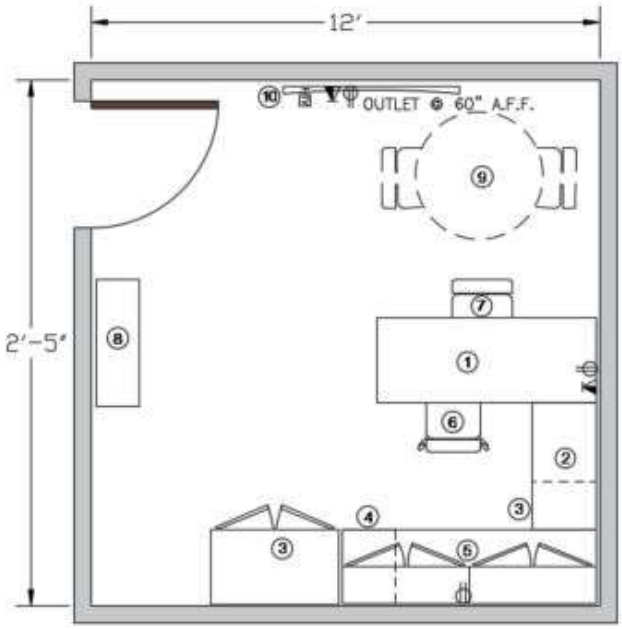
COMMUNICATIONS: TWO DATA AND ONE PHONE

FURNITURE - EQUIPMENT

1. 24" X 60" SIT/STAND DESK
2. 36" RETURN (ATTACHED TO SIT STAND)
3. 15" ROLLING BOX FILE
4. CREDENZA
5. HUTCH W/OH STORAGE
6. WARDROBE CABINET W/DRAWERS AND SHELVES
7. DESK CHAIR
8. SIDE/GUEST CHAIRS
9. BOOKCASE
10. FLAT SCREEN WALL MOUNTED TV W/CABLE

ADMINISTRATIVE SPACES

1.1 Private Office Large – 150 SqFt, GS-15



LEGEND:

- TV
- VOICE/DATA
- KEYED NOTES
- DUPLEX OUTLET

ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID-CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20-GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON-SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE-1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE-A CERTIFIED, HIGH-SECURITY LOCK W/APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON-HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

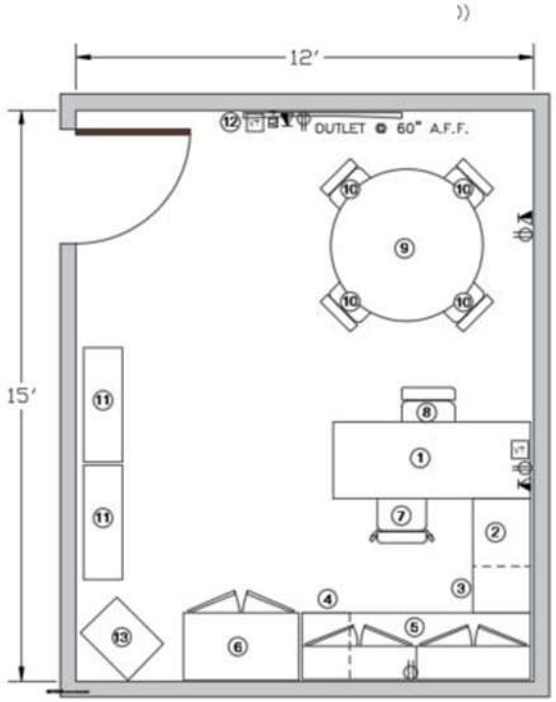
COMMUNICATIONS: TWO DATA AND ONE PHONE

FURNITURE - EQUIPMENT

1. 24" X 60" SIT/STAND DESK
2. 36" RETURN (ATTACHED TO SIT STAND)
3. 15" ROLLING BOX FILE
4. CREDENZA
5. HUTCH W/OH STORAGE
6. DESK CHAIR
7. SIDE/GUEST CHAIRS
8. BOOKCASE
9. OPTIONAL 3' ROUND TABLE AND CHAIRS
10. FLAT SCREEN WALL MOUNTED TV W/CABLE

ADMINISTRATIVE SPACES

1.0 Private Office Large – 180 SqFt,
SES Level



LEGEND:

- TV
- VOICE/DATA
- KEYED NOTES
- DUPLEX OUTLET
- VIDEO TELECONF. OUTLET

ROOM SPECIFICATIONS

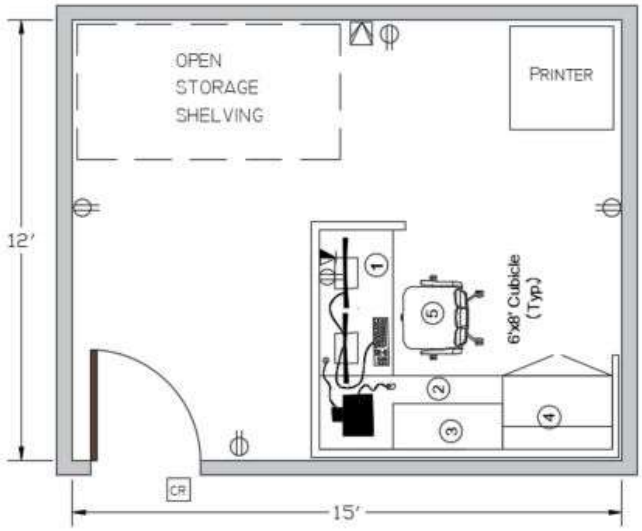
WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS
FLOORS: BUILDING STANDARD
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: BUILDING STANDARD OR SOLID-CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20-GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE
HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON-SITE ASSESSMENT BY PHYSICAL SECURITY REP.
HARDWARE: BHMA/ANSI GRADE-1 CYLINDRICAL OR MORTISE LEVER SET
DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE-A CERTIFIED, HIGH-SECURITY LOCK W/APPROVED CYLINDER HOUSING
INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.
DOOR CLOSER: NON-HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.
GLAZING: NONE
PLUMBING: NONE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: TWO DATA AND ONE PHONE
GENERAL: INSTALL 2" CONDUIT W/PULL LINE FROM CENTER OF WALL TO CENTER OF FLOOR W/BOX

FURNITURE - EQUIPMENT

1. 24" X 60" SIT/STAND DESK
2. 36" RETURN (ATTACHED TO SIT STAND)
3. 15" ROLLING BOX FILE
4. CREDENZA
5. HUTCH W/OH STORAGE
6. 36" UTILITY CABINET W/FILE DRAWER, WARDROBE HOOKS AND SHELVES
7. DESK CHAIR
8. SIDE/GUEST CHAIRS
9. 48" ROUND CONFERENCE TABLE
10. CONFERENCE CHAIRS
11. BOOKCASE
12. FLAT SCREEN WALL MOUNTED TV VTC & CABLE
13. STE PHONE/SECURE FAX

ADMINISTRATIVE SPACES

1.20 LE/CI/K9 One Employee Office – 150 SqFt



LEGEND:

- (#) KEYED NOTES
- DUPLEX OUTLET
- IDS MOTION SENSOR
- CR CARD READER
- VOICE/DATA

ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20 GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON-SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE 1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE A CERTIFIED, HIGH SECURITY LOCK W/APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

COMMUNICATIONS: TWO DATA AND ONE PHONE

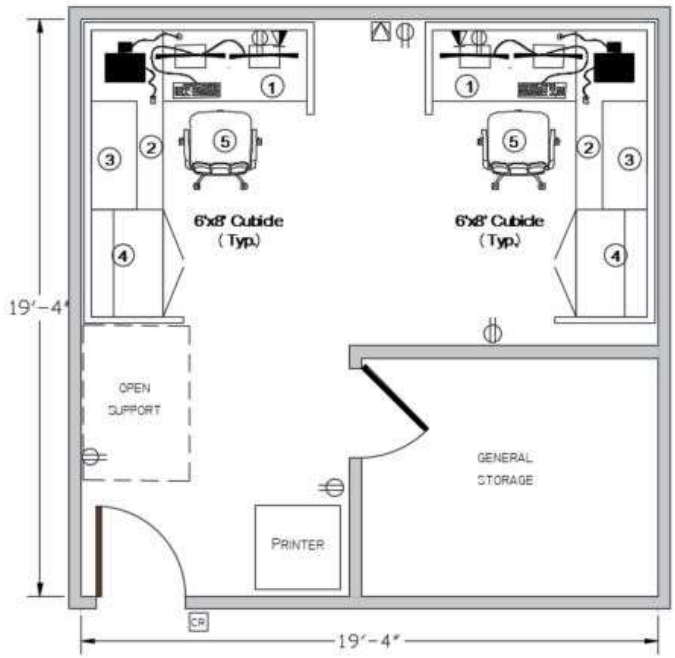
GENERAL: INSTALL 2" CONDUIT W/PULL LINE FROM CENTER OF WALL TO CENTER OF FLOOR W/BOX

FURNITURE - EQUIPMENT

1. SIT/STAND DESK
2. BRIDGE (ATTACHED TO SIT STAND)
3. 15" BOX FILE W/WHEELS
4. CREDENZA
5. HUTCH W/OH STORAGE
6. DESK CHAIR
7. SIDE/GUEST CHAIRS
8. 48" ROUND CONFERENCE TABLE
9. CONFERENCE CHAIRS
10. BOOKCASE
11. FLAT SCREEN WALL MOUNTED TV (VTC OR EQUIV.)
12. STE PHONE/SECURE FAX

ADMINISTRATIVE SPACES

1.21 LE/CI/K9 Two Employee Office – 300 SqFt



LEGEND:

- # KEYED NOTES
- DUPLEX OUTLET
- IDS MOTION SENSOR
- CR CARD READER
- VOICE/DATA

ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20 GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE 1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE A CERTIFIED, HIGH SECURITY LOCK W/APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

COMMUNICATIONS: TWO DATA AND ONE PHONE

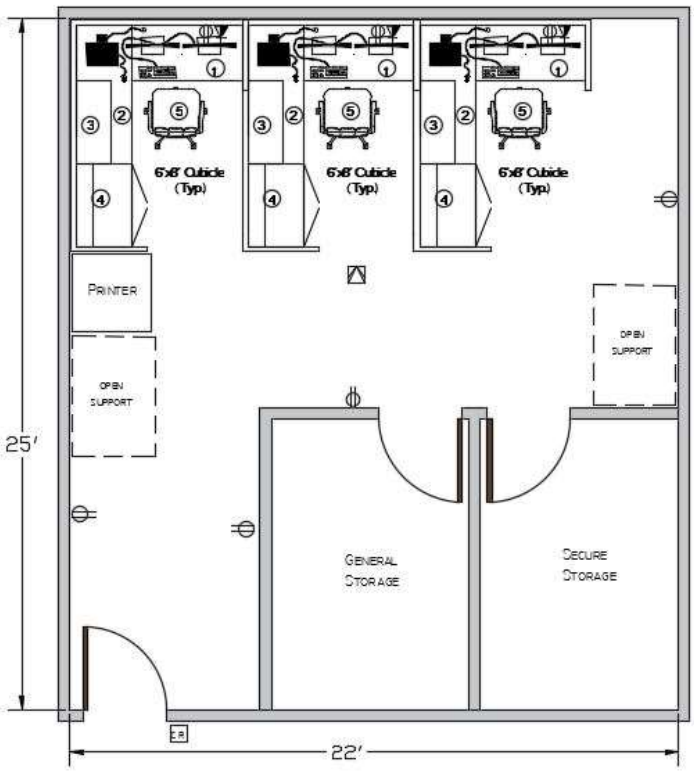
GENERAL: INSTALL 2" CONDUIT W/PULL LINE FROM CENTER OF WALL TO CENTER OF FLOOR W/BOX

FURNITURE - EQUIPMENT

1. 24" x 48" SIT/STAND DESK
2. 24" x 60" WORK SURFACE
3. 36" O.H. CABINET
4. 36" UTILITY CABINET W/FILE DRAWER, WARDROBE HOOKS AND SHELVES
5. OFFICE CHAIR
6. K-9 CRATE

ADMINISTRATIVE SPACES

1.22 LE/CI/K9 Three Employee Office – 450 SqFt



ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID-CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20-GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON-SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE-1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE-A CERTIFIED, HIGH-SECURITY LOCK W/APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON-HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

COMMUNICATIONS: TWO DATA AND ONE PHONE

GENERAL: INSTALL 2" CONDUIT W/PULL LINE FROM CENTER OF WALL TO CENTER OF FLOOR W/BOX

FURNITURE - EQUIPMENT

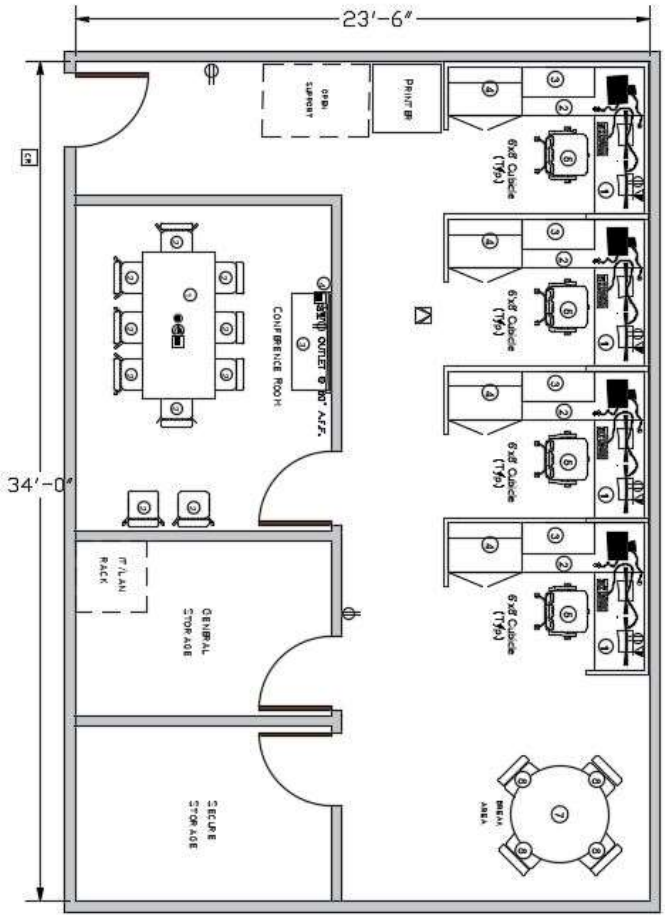
1. 24" x 48" SIT/STAND DESK
2. 24" x 60" WORK SURFACE
3. 36" O.H. CABINET
4. 36" UTILITY CABINET W/FILE DRAWER, WARDROBE HOOKS AND SHELVES
5. OFFICE CHAIR
6. K-9 CRATE

LEGEND:

- (#) KEYED NOTES
- DUPLEX OUTLET
- IDS MOTION SENSOR
- CR CARD READER
- VOICE/DATA

ADMINISTRATIVE SPACES

1.23 LE/CI/K9 Four Employee Office – 600 SqFt



LEGEND:

- # KEYED NOTES
- DUPLEX OUTLET
- IDS MOTION SENSOR
- CR CARD READER
- VOICE/DATA

ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID-CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20-GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON-SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE-1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE-A CERTIFIED, HIGH-SECURITY LOCK W/APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON-HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

COMMUNICATIONS: TWO DATA AND ONE PHONE

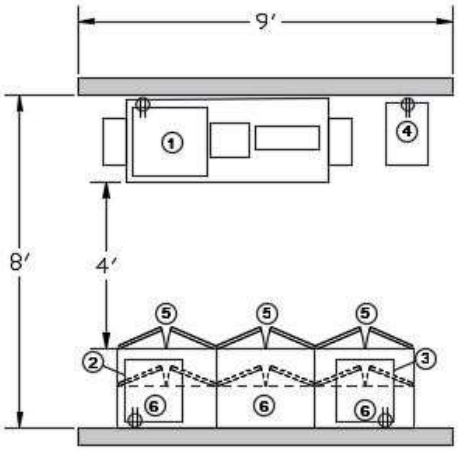
GENERAL: INSTALL 2" CONDUIT W/PULL LINE FROM CENTER OF WALL TO CENTER OF FLOOR W/BOX

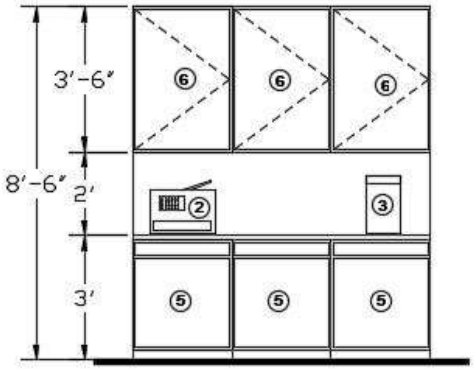
FURNITURE - EQUIPMENT

1. 24" X 48" SIT/STAND DESK
2. 24" X 60" WORK SURFACE
3. 36" O.H. CABINET
4. 36" UTILITY CABINET W/FILE DRAWER, WARDROBE HOOKS AND SHELVES
5. OFFICE CHAIR
6. K-9 CRATE

ADMINISTRATIVE SPACES

1.16 Office Support Area – Scalable (10 or more employees, 72 SqFt per every 20 employees)





ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ ACOUSTIC BATTS
FLOORS: BUILDING STANDARD
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: NONE
HINGES: NONE
HARDWARE: NONE
DOOR LOCKS: NONE
DOOR CLOSER: NONE
GLAZING: NONE
PLUMBING: HOT/COLD WATER WHERE APPLICABLE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: NONE
POWER: SPECIAL PLUG MAY BE REQUIRED FOR COPIER MACHINE

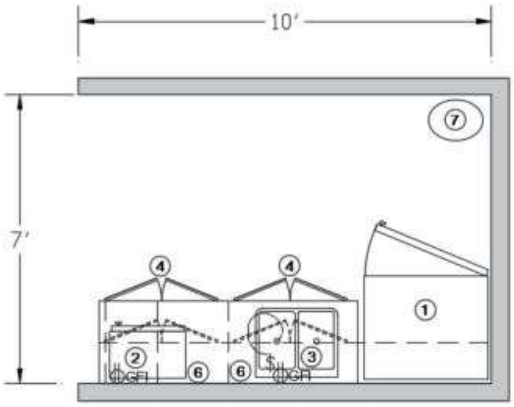
FURNITURE - EQUIPMENT

1. LARGE VOLUME COPIER/PRINTER/SCANNER
2. SECURE FAX
3. SHREDDER
4. PAPER BIN
5. BASE CABINET WITH TOP DRAWER AND SHELVES
6. WALL CABINET WITH SHELVES

LEGEND:

ADMINISTRATIVE SPACES

1.7 Break Room SM – 72 SqFt



LEGEND:

- TV
- VOICE/DATA
- KEYED NOTES
- DUPLEX OUTLET
- SWITCHED OUTLET
- GROUND FAULT INTERRUPT DUPLEX OUTLET

ROOM SPECIFICATIONS

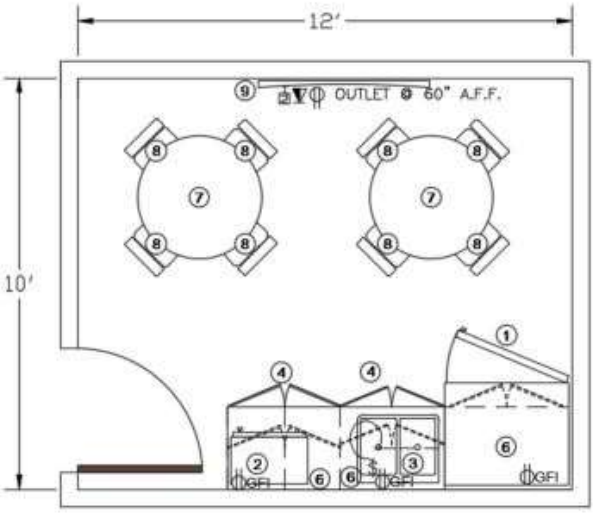
WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS
FLOORS: BUILDING STANDARD
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: NONE
HINGES: NONE
HARDWARE: NONE
DOOR LOCKS: NONE
DOOR CLOSER: NONE
GLAZING: NONE
PLUMBING: HOT/COLD WATER WHERE APPLICABLE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: NONE

FURNITURE - EQUIPMENT

1. 36" REFRIGERATOR/FREEZER W/ICE/WATER (WHERE APPLICABLE)
2. 1000 WATT INDUSTRIAL MICROWAVE
3. SINK (HOT/COLD) W/SPRAYER & DISPOSAL
4. SINK BASE CABINET
5. BASE CABINET W/DRAWERS
6. O.H. CABINET
7. TRASH

ADMINISTRATIVE SPACES

1.8 Break Room LG - 120 SqFt



LEGEND:

- TV
- VOICE/DATA
- KEYED NOTES
- DUPLEX OUTLET
- SWITCHED OUTLET
- GROUND FAULT INTERRUPT DUPLEX OUTLET

ROOM SPECIFICATIONS

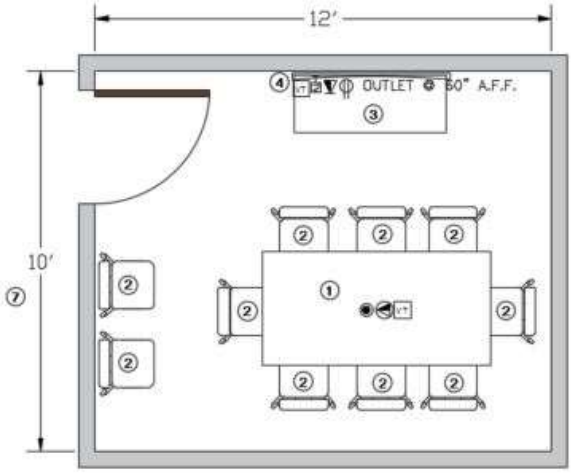
WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS
FLOORS: VCT
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: BUILDING STANDARD A/SCWD OR C / FLUSH WD W/VISION PANEL
HINGES: BUILDING STANDARD
HARDWARE: BHMA/ANSI GRADE I CYLINDRICAL OR MORTISE LEVER SET
DOOR LOCKS: INTERIOR - BUILDING STANDARD OR 05/F05
DOOR CLOSER: HOLD OPEN STOPPER/LATCH
GLAZING: NONE
PLUMBING: NONE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: TWO DATA AND ONE PHONE
CASEWORK: PLASTIC LAMINATE CABINET (BASE & UPPER) WITH SOLID SURFACE OR PLASTIC LAMINATE COUNTERTOP

FURNITURE - EQUIPMENT

1. 36" REFRIGERATOR/FREEZER W/ICE/WATER - WHERE APPLICABLE (1 REFRIGERATOR PER 15 PERSONNEL)
2. 1000 WATT INDUSTRIAL MICROWAVE
3. SINK (HOT/COLD) W/SPRAYER & DISPOSAL
4. SINK BASE CABINET
5. BASE CABINET W/DRAWERS
6. O.H. CABINET
7. 30X72 TABLE
8. CAFETERIA STYLE CHAIR
9. FLAT SCREEN WALL MOUNTED TV W/CABLE

ADMINISTRATIVE SPACES

1.9 Conference Room SM, 120 SqFt



ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20 GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE 1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE A CERTIFIED, HIGH SECURITY LOCK W/APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

COMMUNICATIONS: TWO DATA AND ONE PHONE

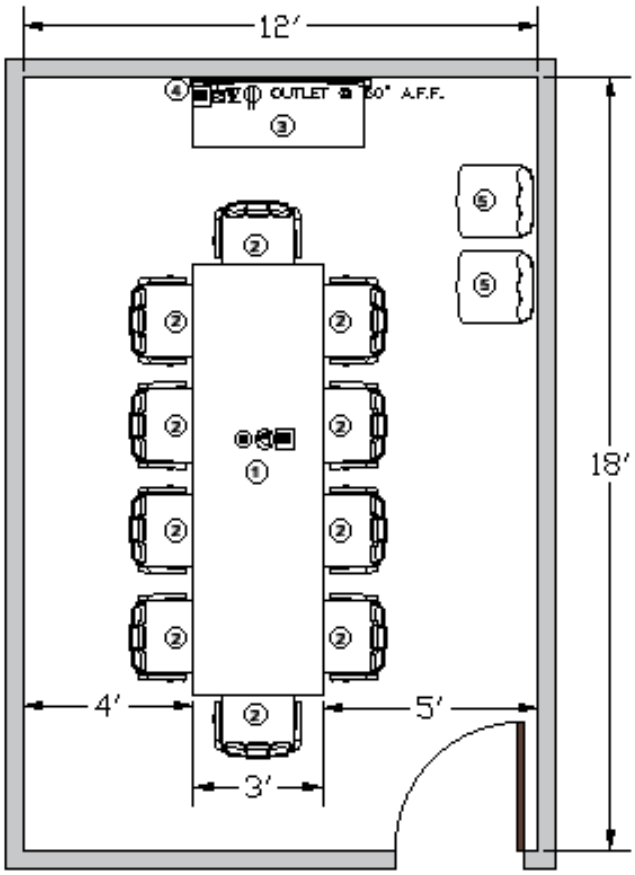
GENERAL: INSTALL 2" CONDUIT W/PULL LINE FROM CENTER OF WALL TO CENTER OF FLOOR W/BOX

FURNITURE - EQUIPMENT

1. 30X60 TABLE
2. OFFICE CHAIR
3. MEDIA CREDENZA
4. WALL MOUNTED FLAT SCREEN TV W/VTC OR EQUIV.

ADMINISTRATIVE SPACES

1.10 Conference Room Med, 200 SqFt



ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID-CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20-GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON-SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE-1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE-A CERTIFIED, HIGH-SECURITY LOCK W/APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON-HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

COMMUNICATIONS: TWO DATA AND ONE PHONE

GENERAL: INSTALL 2" CONDUIT W/PULL LINE FROM CENTER OF WALL TO CENTER OF FLOOR W/BOX

LEGEND:

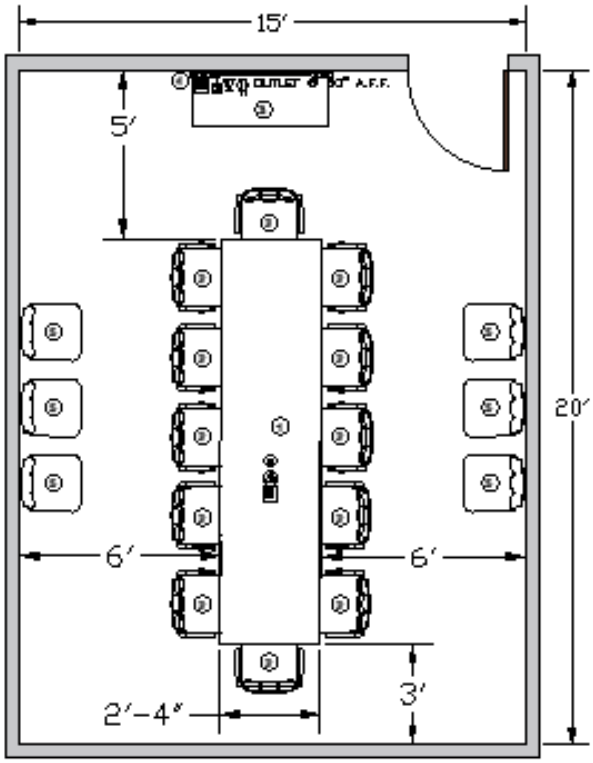
- TV
- VOICE/DATA
- KEYED NOTES
- DUPLEX OUTLET
- FLOOR MOUNTED VOICE/DATA
- FLOOR MOUNTED DUPLEX OUTLET
- VT VIDEO TELECONF. OUTLET

FURNITURE – EQUIPMENT

1. 36X120 TABLE
2. OFFICE CHAIR
3. MEDIA CREDENZA
4. WALL MOUNTED FLAT SCREEN TV W/VTC OR EQUIV. (TV SUPPLIED BY LOCAL OFFICE)
5. GUEST CHAIR (NO WHEELS)

ADMINISTRATIVE SPACES

1.11 Conference Room LG/Executive -300 SqFt



ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID-CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20-GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON-SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE-1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE-A CERTIFIED, HIGH-SECURITY LOCK W/APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON-HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

COMMUNICATIONS: TWO DATA AND ONE PHONE

GENERAL: INSTALL 2" CONDUIT W/PULL LINE FROM CENTER OF WALL TO CENTER OF FLOOR W/BOX

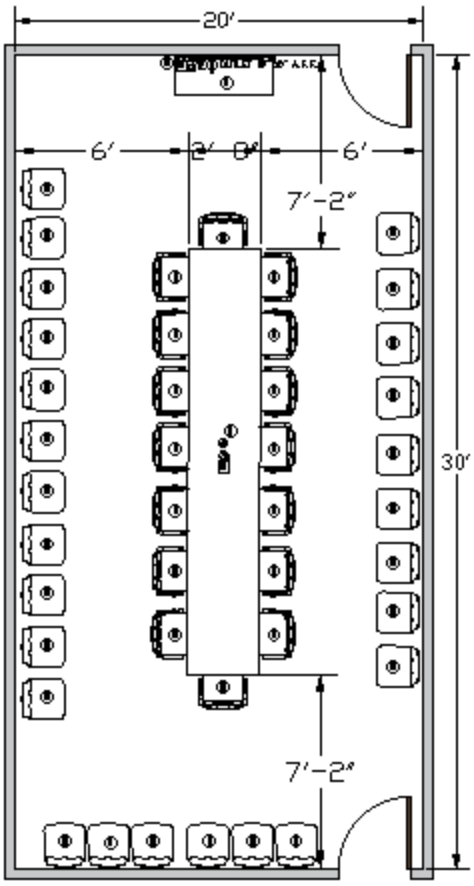
LEGEND:

- TV
- VOICE/DATA
- KEYED NOTES
- DUPLEX OUTLET
- FLOOR MOUNTED VOICE/DATA
- FLOOR MOUNTED DUPLEX OUTLET
- VT VIDEO TELECONF. OUTLET

FURNITURE – EQUIPMENT

1. 30X60 TABLE
2. OFFICE CHAIR
3. MEDIA CREDENZA
4. WALL MOUNTED FLAT SCREEN TV W/VTC OR EQUIV. (TV SUPPLIED BY LOCAL OFFICE)
5. GUEST CHAIR (NO WHEELS)

1.12 Conference Room Jumbo -600 SqFt



ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID-CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20-GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON-SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE-1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE-A CERTIFIED, HIGH-SECURITY LOCK W/ APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON-HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

COMMUNICATONS: TWO DATA AND ONE PHONE

GENERAL: INSTALL 2" CONDUIT W/PULL LINE FROM CENTER OF WALL TO CENTER OF FLOOR W/BOX

LEGEND:

- TV
- VOICE/DATA
- KEYED NOTES
- DUPLEX OUTLET
- FLOOR MOUNTED VOICE/DATA
- FLOOR MOUNTED DUPLEX OUTLET
- VT VIDEO TELECONF. OUTLET

FURNITURE - EQUIPMENT

1. 30X60 TABLE
2. OFFICE CHAIR
3. MEDIA CREDENZA
4. WALL MOUNTED FLAT SCREEN TV W/VTC OR EQUIV. (TV SUPPLIED BY LOCAL OFFICE)

ADMINISTRATIVE SPACES

Lactation Room

Private room for nursing mothers to express milk, must be made available upon request. This space can be an office or huddle room provided it meets the criteria below. This room shall comply with FPS Directive 15.4.7.1 Worksite Lactation Program, November 14, 2013

Components of this space:

- A non-bathroom space to express breast milk, must be free from intrusion of co-workers and the public.
- Must contain a flat surface or table (not the floor), and a place to sit

Optional Amenities:

- A comfortable seat.
- Priority access.
- Lockable from the inside, but still allows access by Emergency Response Personnel.
- Can be temporary.
- Clean with natural/soft lighting and proper ventilation.
- Electricity to operate a pump.
- Lockable refrigerator or a refrigerator with a freezer section.
- Comfortable temperature.
- Microwave for sterilization.
- Table, Clock, Mirror, Sink
- Room Schedule Sign-up sheet (if needed for multiple nursing mothers)

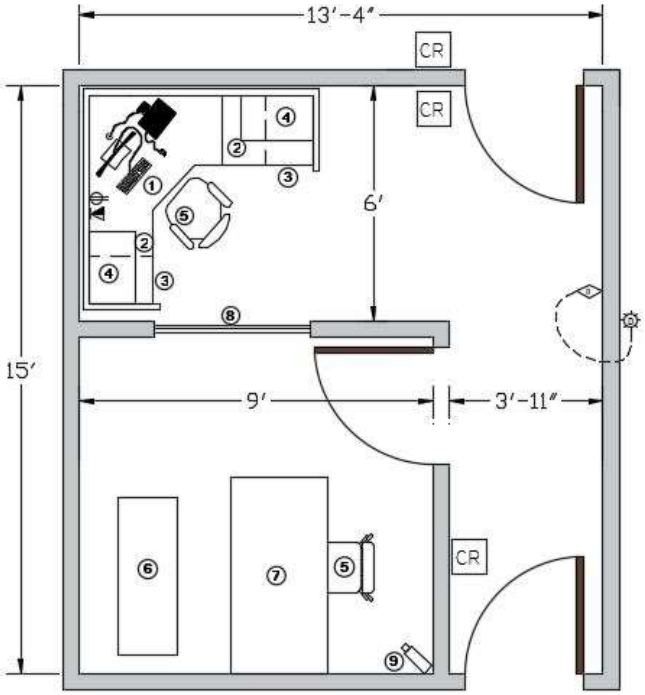
Responsibilities of Facilities

- Provide a Nursing Mother access to Nursing Room / Space for one year after her child's birth.
- Work with Region Resource Management Branch Chief to identify potential spaces such as:
- Vacant office/space in or near Expectant Mother's place of work

MISSION SPACES

2.5 Interview/Observation Room – 200 SqFt

(Size may be larger depending on mission requirements)



LEGEND:

- # KEYED NOTES
- D DURESS LIGHT CEILING/WALL
- D DURESS BUTTON
- VOICE/DATA
- DUPLEX OUTLET
- CR CARD READER

ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID-CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20-GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON-SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE-1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE-A CERTIFIED, HIGH-SECURITY LOCK W/APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON-HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

COMMUNICATIONS: TWO DATA AND ONE PHONE

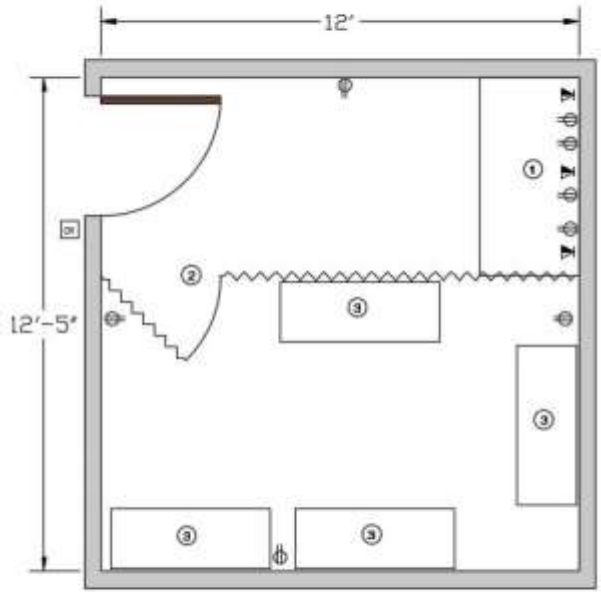
FURNITURE - EQUIPMENT

1. 48" X 48" SIT/STAND DESK W/ OPTIONAL 30" RETURNS
2. 30" RETURN (CAN BE MOUNTED TO SIT STAND. DELETE O.H. IF PART OF SIT STAND
3. 15" BOX FILE ON WHEELS
4. 24" O.H. CABINET (DELETE IF RETURN BELOW IS ATTACHED TO SIT/STAND
5. OFFICE CHAIR
6. BOLT DOWN HANDCUFF BENCH W/HANDCUFF RINGS
7. INTERVIEW TABLE
8. ONE WAY MIRROR (TYPE 5 SAFETY GLASS) USE BLINDS OR A CURTAIN
9. CCTV CAMERA TO BE TOWARDS INTERVIEWEE AND PROVIDE 100% COVERAGE PER SECURITY SOW

MISSION SPACES

1.6 Radio/Elec/ITFO Lab – 150 SqFt

(Employee has separate cubicle not in this space)



LEGEND:

- (#) KEYED NOTES
- VOICE/DATA
- CR CARD READER
- DUPLEX OUTLET

ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID-CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20-GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON-SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE-1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE-A CERTIFIED, HIGH-SECURITY LOCK W/APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON-HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

COMMUNICATIONS: TWO DATA AND ONE PHONE

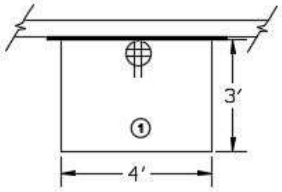
FURNITURE - EQUIPMENT

1. 30x60 POWERED WORKBENCH (DEDICATED CIRCUIT)
2. CHAIN LINK FENCE WITH DOOR AND CIPHER LOCK
3. 18x48 HEAVY DUTY STORAGE RACKS

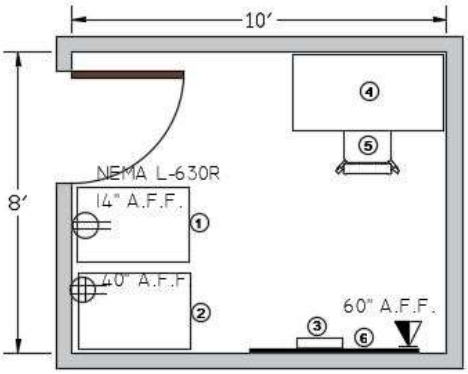
MISSION SPACES

Sizes of IT space are based upon equipment required to support mission

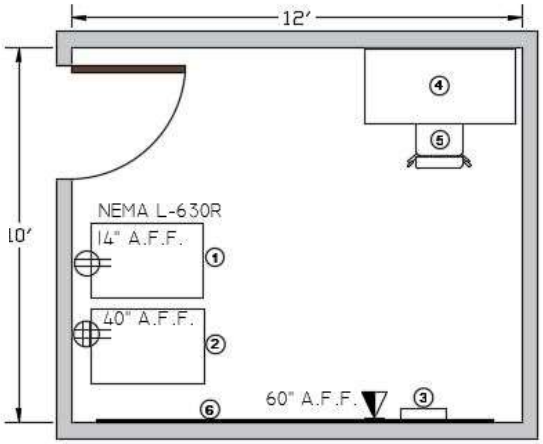
1.13 LAN / Radio Rack –



1.14 LAN / Radio Room – Small – 72 SqFt



1.15 LAN / Radio Room – Large - 120 SqFt



LEGEND:

- (#) KEYED NOTES
- VOICE/DATA
- DEDICATED DUPLEX OUTLET
- DUPLEX OUTLET

ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID-CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20-GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON-SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE-1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE-A CERTIFIED, HIGH-SECURITY LOCK W/APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON-HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

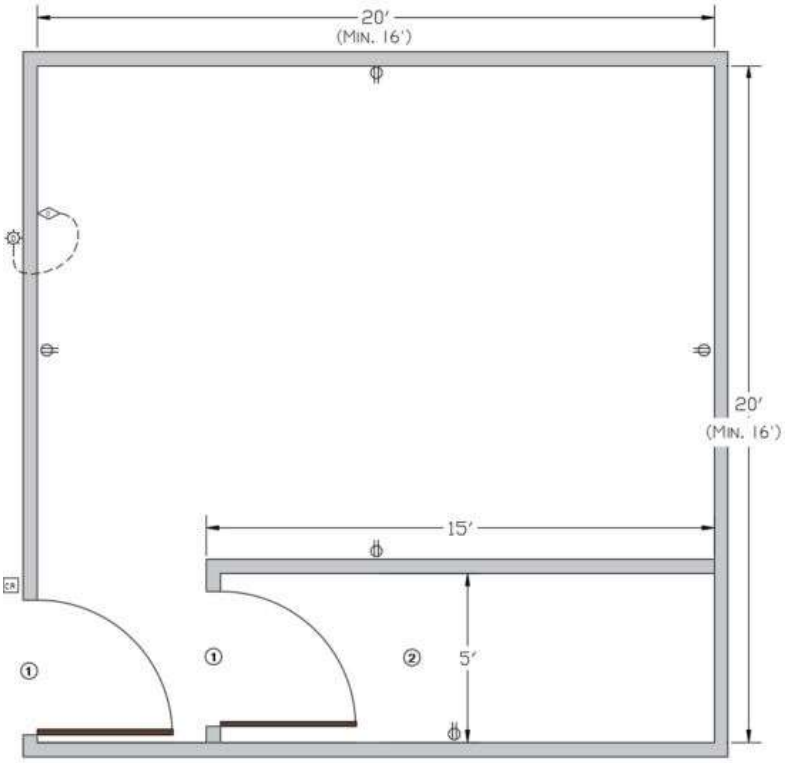
COMMUNICATIONS: TWO DATA AND ONE PHONE

FURNITURE - EQUIPMENT

1. IT EQUIPMENT RACK (WALL MOUNTED SINGLE UNIT FOR ALL IT/CCTV/IDS IF LESS THAN 5 PERSONNEL)
2. CCTV EQUIPMENT RACK
3. IDS BOX MOUNTED 60" A.F.F
4. DESK FOR PACS
5. TYP. GUEST CHAIR
6. 3/4" FRT PLYWOOD ATTACHED TO WALL

MISSION SPACES

2.1 Mat Room – 500 SqFt



LEGEND:

- # KEYED NOTES
- D DURESS BUTTON
- D DURESS LIGHT CEILING/WALL
- DUPLEX OUTLET
- CR CARD READER

ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD W/ACOUSTIC BATTS (ADD 8' 0" X 3/4" PLYWOOD ON WALLS THAT RECEIVE PADS + HARDWARE TO HANG PADS AT APPROX. 6' HIGH)

FLOORS: INTERLOCKING RUBBER TILE MATS OR ROLL RUBBER MATS HOT WELDED

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: BUILDING STANDARD OR SOLID CORE WOOD (WHICHEVER IS STRONGER SHALL BE USED), MIN. 1 3/4" THICK, INSTALLED IN WELDED STEEL FRAME ASSEMBLY MOUNTED TO 20 GAUGE METAL STUDS. KNOCK DOWN (COLLAPSIBLE JAM AND HEADER) OR ALUMINUM FRAMES ARE NOT ACCEPTABLE

HINGES: PREFERRED ON INTERNAL SIDE OF DOOR; IF EXTERNAL, HINGES MAY HAVE TO BE PINNED BASED ON A JOINT ON SITE ASSESSMENT BY PHYSICAL SECURITY REP.

HARDWARE: BHMA/ANSI GRADE 1 CYLINDRICAL OR MORTISE LEVER SET

DOOR LOCKS: PERIMETER - UL 437 AND BHMA/ANSI A156.3, GRADE A CERTIFIED, HIGH SECURITY LOCK W/APPROVED CYLINDER HOUSING

INTERIOR - BUILDING STANDARD UNLESS DETERMINED OTHERWISE BY A JOINT ASSESSMENT BY THE PHYSICAL SECURITY REP.

DOOR CLOSER: NON HOLD OPEN DOOR CLOSER ON ALL PERIMETER DOORS AND ANY INTERIOR DOOR EQUIPPED WITH CARD READER.

GLAZING: NONE

PLUMBING: NONE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

DURESS SYSTEM: WALL MOUNT

COMMUNICATIONS: TWO DATA AND ONE PHONE

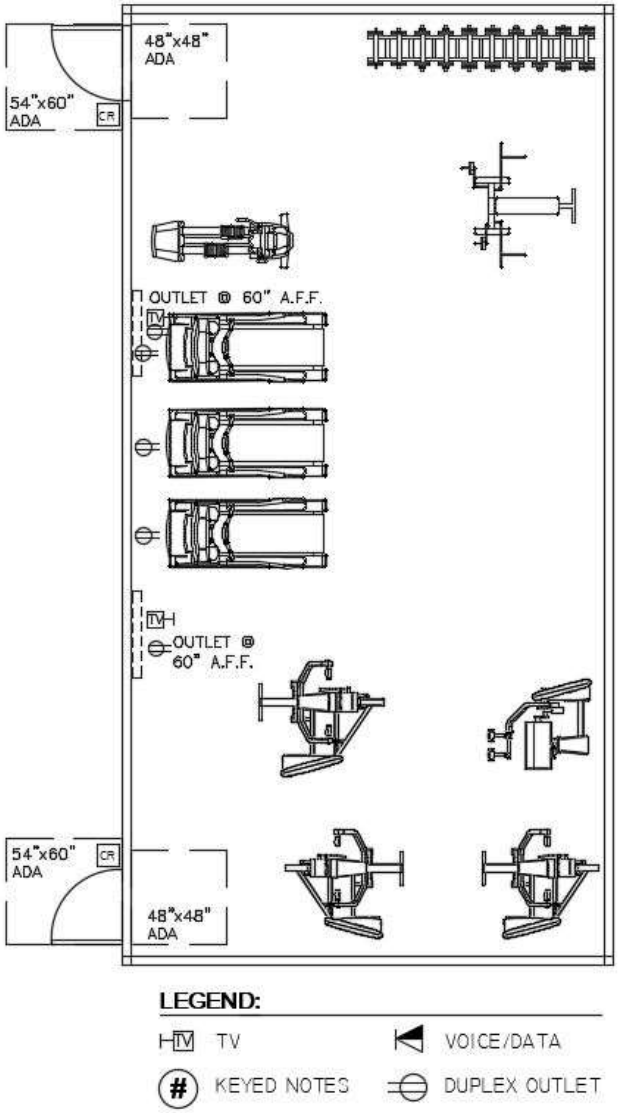
GENERAL: INSTALL 2" CONDUIT W/PULL LINE FROM CENTER OF WALL TO CENTER OF FLOOR W/BOX

FURNITURE - EQUIPMENT

1. 48" A.D.A DOOR
2. MAT STORAGE AREA (IF POSSIBLE)

ADMINISTRATIVE SPACES

1.24 Fitness Center – 600 SqFt



ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS
FLOORS: BUILDING STANDARD
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: NONE
HINGES: NONE
HARDWARE: NONE
DOOR LOCKS: NONE
DOOR CLOSER: NONE
GLAZING: NONE
PLUMBING: HOT/COLD WATER WHERE APPLICABLE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: NONE
POWER: SPECIAL PLUG MAY BE REQUIRED FOR COPIER MACHINE

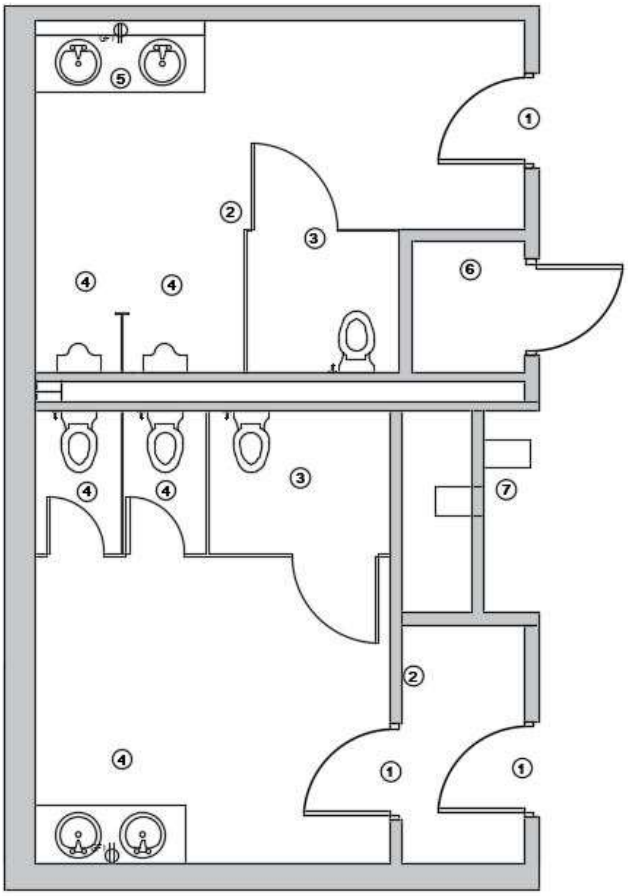
FURNITURE - EQUIPMENT

1. LARGE VOLUME COPIER/PRINTER/SCANNER
2. SECURE FAX
3. SHREDDER
4. PAPER BIN
5. BASE CABINET WITH TOP DRAWER AND SHELVES
6. WALL CABINET WITH SHELVES

MISSION SPACES

2.4 Restrooms Scalable, typ. 300 SqFt, may vary with proportion of men to women (typical design is to have restrooms combined with showers)

3.4I REQUIRED WHERE GYM IS REQUIRED OR PUBLIC BATHROOMS ARE UNAVAILABLE



LEGEND:

(#) KEYED NOTES

DUPLEX OUTLET

GFI GROUND FAULT INTERRUPT DUPLEX OUTLET

M

ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS
FLOORS: BUILDING STANDARD
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: NONE
HINGES: NONE
HARDWARE: NONE
DOOR LOCKS: NONE
DOOR CLOSER: NONE
GLAZING: NONE
PLUMBING: HOT/COLD WATER WHERE APPLICABLE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: NONE
POWER: SPECIAL PLUG MAY BE REQUIRED FOR COPIER MACHINE

GENERAL NOTES:

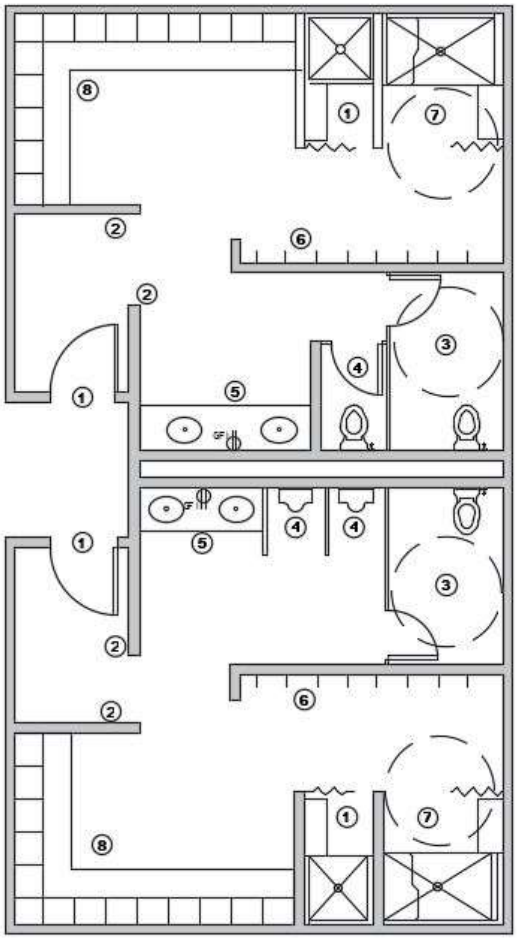
1. BATHROOM ONLY REQUIRED WHEN PUBLIC RESTROOM NOT AVAILABLE OR GYM IS WITHIN FPS SPACE
2. BATHROOM SIZE TYPICALLY 300 SQUARE FEET BUT WILL VARY WITH FIXTURE COUNT, CODE, AND REQUIREMENTS.
3. FIXTURE RATION: 25% FEMALE AND 75% MALE

KEYED NOTES:

1. 48" A.D.A DOOR
2. PRIVACY WALL (VARIES WITH DESIGN)
3. ADA COMPLIANT FIXTURE
4. STANDARD TOILET FIXTURE (NUMBER OF FIXTURES IS BASED UPON NUMBER OF EMPLOYEES AND CODE REQUIREMENTS)
5. ADA COMPLIANT SINK
6. STORAGE (WHERE DESIGN AND BUDGE ALLOW, NOT REQUIREMENT)
7. WATER FOUNTAIN (WHEN BUDGET AND REQUIREMENTS ALLOW)

MISSION SPACES

2.3 Shower/Locker Typ. 600 SqFt (may vary with proportion of men to women)



LEGEND:

(#) KEYED NOTES

DUPLEX OUTLET

GFI GROUND FAULT INTERRUPT DUPLEX OUTLET

ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: NONE

HINGES: NONE

HARDWARE: NONE

DOOR LOCKS: NONE

DOOR CLOSER: NONE

GLAZING: NONE

PLUMBING: HOT/COLD WATER WHERE APPLICABLE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

COMMUNICATIONS: NONE

POWER: SPECIAL PLUG MAY BE REQUIRED FOR COPIER MACHINE

GENERAL NOTES:

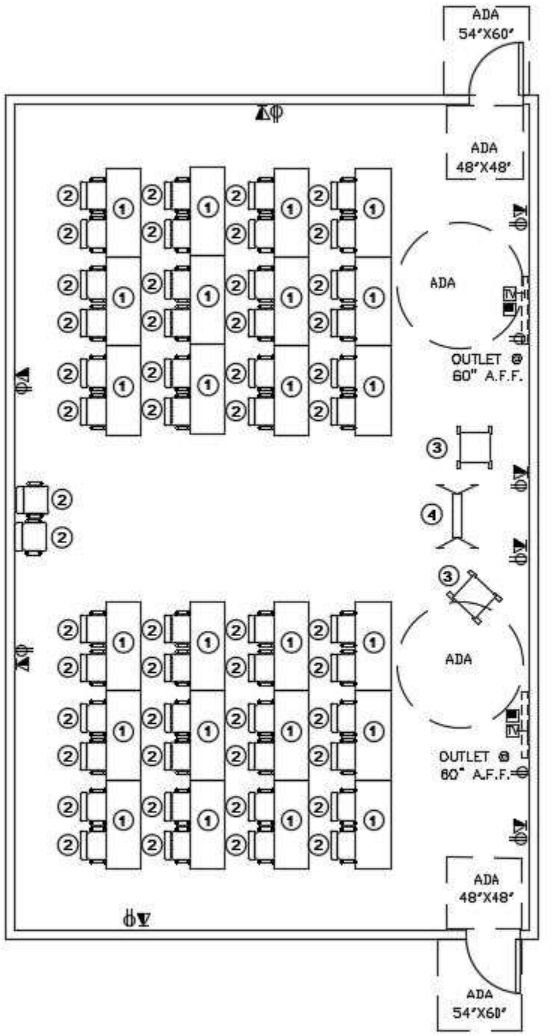
1. SHOWER/LOCKER SIZE TYPICALLY 600 SQUARE FEET BUT WILL VARY WITH FIXTURE COUNT, CODE, AND REQUIREMENTS.
2. FIXTURE RATION: 25% FEMALE AND 75% MALE

KEYED NOTES:

1. 48" ADA DOOR
2. PRIVACY WALL (VARIES WITH DESIGN)
3. ADA COMPLIANT FIXTURE
4. STANDARD TOILET FIXTURE (NUMBER OF FIXTURES IS BASED UPON NUMBER OF EMPLOYEES AND CODE REQUIREMENTS)
5. ADA COMPLIANT SINK
6. TOWEL PINS
7. ADA COMPLIANT SHOWER (FOLDING SEAT IN SHOWER AND OUTSIDE OF SHOWER)
8. BENCH SEATS WITH LOCKERS ABOVE (DESIGNS FOR LOCKER LOCATIONS MAY VARY)

MISSION SPACES

2.0 Regional HQ PSO/Training Mat Room – only mission space if there is a tactical function such as PSO or Mat



LEGEND:

- TV
- VOICE/DATA
- KEYED NOTES
- DUPLEX OUTLET
- VIDEO TELECONF. OUTLET

ROOM SPECIFICATIONS

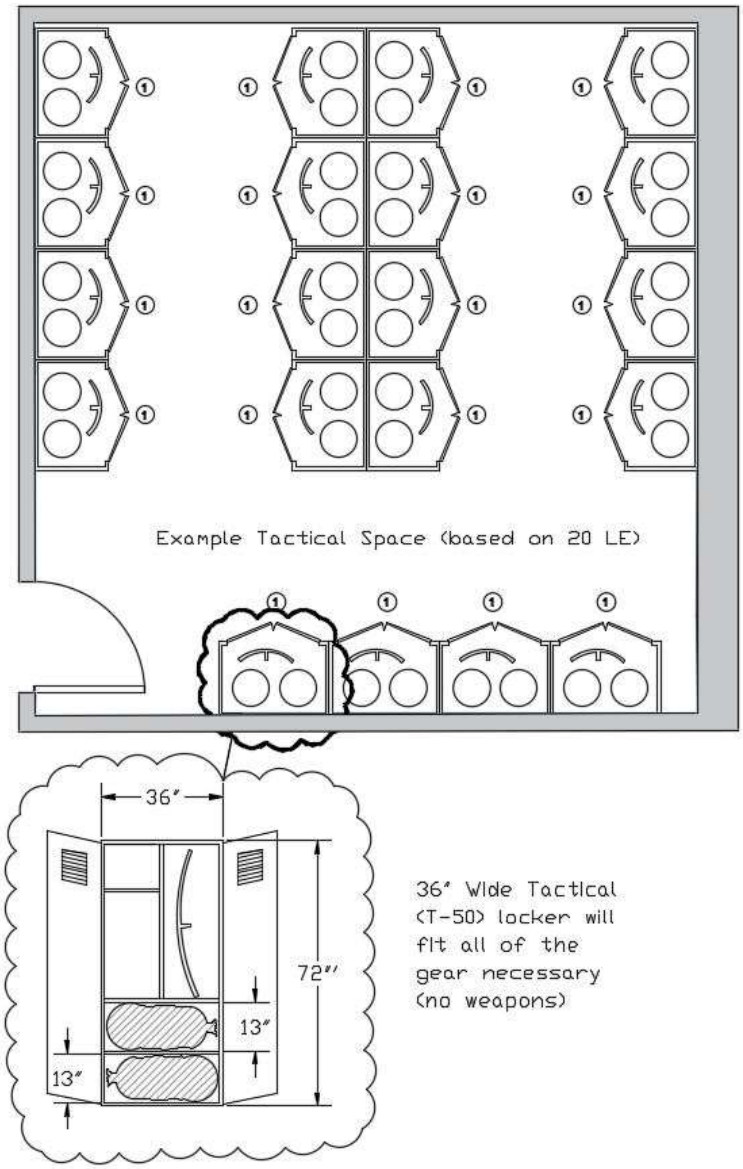
WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS
FLOORS: BUILDING STANDARD
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: NONE
HINGES: NONE
HARDWARE: NONE
DOOR LOCKS: NONE
DOOR CLOSER: NONE
GLAZING: NONE
PLUMBING: HOT/COLD WATER WHERE APPLICABLE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: NONE
POWER: SPECIAL PLUG MAY BE REQUIRED FOR COPIER MACHINE

FURNITURE - EQUIPMENT

1. 30X60 TABLE W/NEST CAPABILITY
2. TASK CHAIR (REMOVABLE ARMS) W/NEST CAPABILITY
3. ROLLING PODIUM
4. ROLLING WHITE BOARD/FLIP BOARD

MISSION SPACES

2.8 Tactical Storage - Scalable



ROOM SPECIFICATIONS

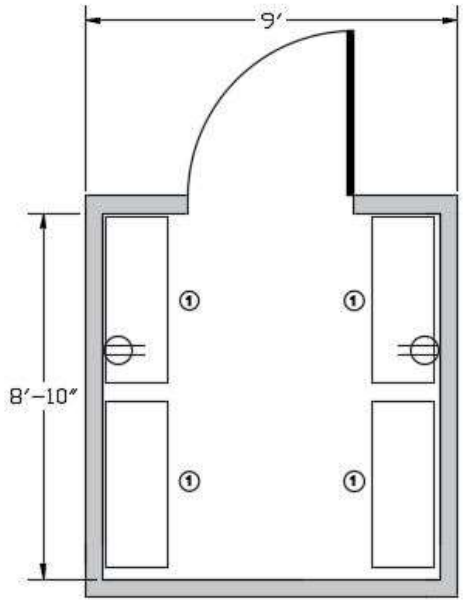
WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS
FLOORS: BUILDING STANDARD
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: NONE
HINGES: NONE
HARDWARE: NONE
DOOR LOCKS: NONE
DOOR CLOSER: NONE
GLAZING: NONE
PLUMBING: HOT/COLD WATER WHERE APPLICABLE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: NONE
POWER: SPECIAL PLUG MAY BE REQUIRED FOR COPIER MACHINE

FURNITURE - EQUIPMENT

1. T-50 TACTICAL LOCKER

MISSION SPACES

2.6 Storage Bulk – Scalable (1-9 Employees = open storage, greater than 10 = 10 SqFt per person



LEGEND:

(#) KEYED NOTES DUPLEX OUTLET

ROOM SPECIFICATIONS

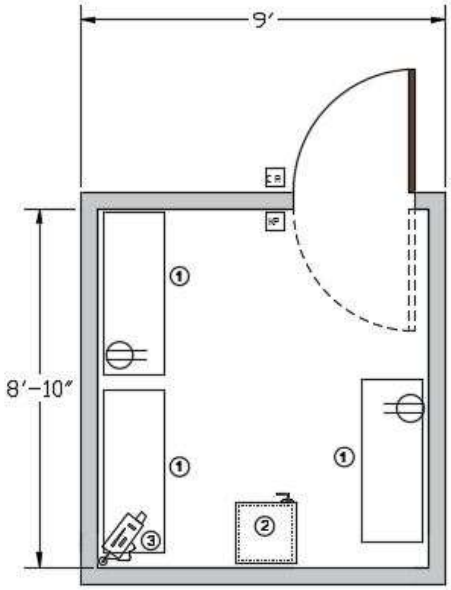
WALLS: BUILDING STANDARD (W/ ACOUSTIC BATTS
FLOORS: BUILDING STANDARD
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: NONE
HINGES: NONE
HARDWARE: NONE
DOOR LOCKS: NONE
DOOR CLOSER: NONE
GLAZING: NONE
PLUMBING: HOT/COLD WATER WHERE APPLICABLE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: NONE
POWER: SPECIAL PLUG MAY BE REQUIRED FOR COPIER MACHINE

FURNITURE - EQUIPMENT

1. HEAVY DUTY 24X48 STORAGE SHELVES (MECHANICALLY ATTACH TO WALLS TO PREVENT TIPPING)

MISSION SPACES

2.7 Secure File/Evidence Scalable (1-7 LE's = Safe, 8-14 = 120 Office, greater than 15 LE's = 10 SqFt per LE



ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS
FLOORS: BUILDING STANDARD
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: NONE
HINGES: NONE
HARDWARE: NONE
DOOR LOCKS: NONE
DOOR CLOSER: NONE
GLAZING: NONE
PLUMBING: HOT/COLD WATER WHERE APPLICABLE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: NONE
POWER: SPECIAL PLUG MAY BE REQUIRED FOR COPIER MACHINE

FURNITURE - EQUIPMENT

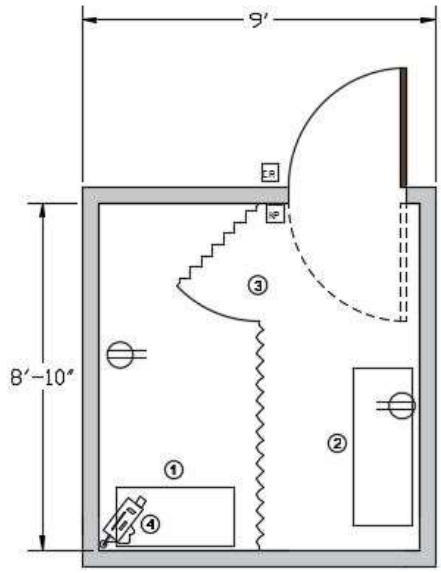
1. HEAVY DUTY SHELVING (QUANTITY WILL DEPEND ON SIZE AND DESIGN)
2. HIGH RISK DRUG EVIDENCE SAFE (GSA CLASS 6, 4 DRAWER LEGAL SIZE W/SINGLE COMBINATION LOCK (QUANTITY AND SIZE TO BE DETERMINED)
3. CCTV CAMERA (MUST HAVE COMPLETE COVERAGE)

LEGEND:

#	KEYED NOTES	KP	KEYPAD
CR	CARD READER		DUPLEX OUTLET

MISSION SPACES

2.9 Ammo/Weapons – Scalable (1-7 LE's = Safe, 8-14=120 Office, Greater than 15 = 10 SqFt per LE)



LEGEND:

CR	CARD READER	KP	KEYPAD
#	KEYED NOTES		DUPLEX OUTLET

ROOM SPECIFICATIONS

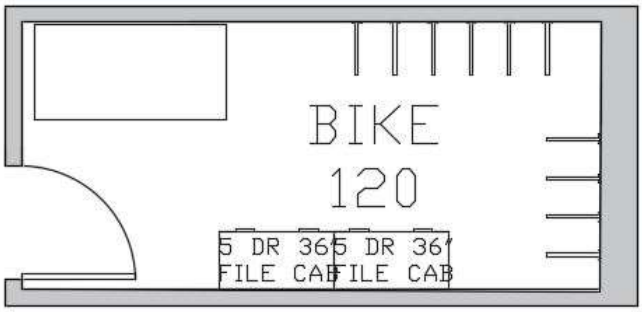
WALLS: SECURE FULL HT. W/1 LAYER UL 752 LVL III BP AND SECURITY MESH. BALLISTIC RATED SECURE PERIMITER
FLOORS: FLOOR LOAD FOR AMMUNITION STORAGE NEEDS TO BE CONSIDERED
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: TYPE A-LVL III (INCLUDING FRAME)
HINGES: NONE
HARDWARE: E6
DOOR LOCKS: NONE
DOOR CLOSER: NONE
GLAZING: NONE
PLUMBING: HOT/COLD WATER WHERE APPLICABLE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: NONE
POWER: SPECIAL PLUG MAY BE REQUIRED FOR COPIER MACHINE

FURNITURE - EQUIPMENT

1. 18"x36" HEAVY DUTY STORAGE UNIT FOR AMMO STORAGE
2. 18X48 WEAPONS LOCKER FOR LONG GUNS WITH SHELVES ON TOP FOR HAND GUN STORAGE
3. CHAIN LINK FENCE (MIN. 10 GAUGE) WITH LOCK
4. CCTV CAMERA (MUST HAVE COMPLETE COVERAGE)

STORAGE SPACES

2.10 Bike Storage – 120 SqFt (<10 bikes no special storage required, >10 bikes = 120 sqft)



ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS
FLOORS: BUILDING STANDARD
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)
DOORS: NONE
HINGES: NONE
HARDWARE: NONE
DOOR LOCKS: NONE
DOOR CLOSER: NONE
GLAZING: NONE
PLUMBING: HOT/COLD WATER WHERE APPLICABLE
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: NONE
POWER: SPECIAL PLUG MAY BE REQUIRED FOR COPIER MACHINE

FURNITURE - EQUIPMENT

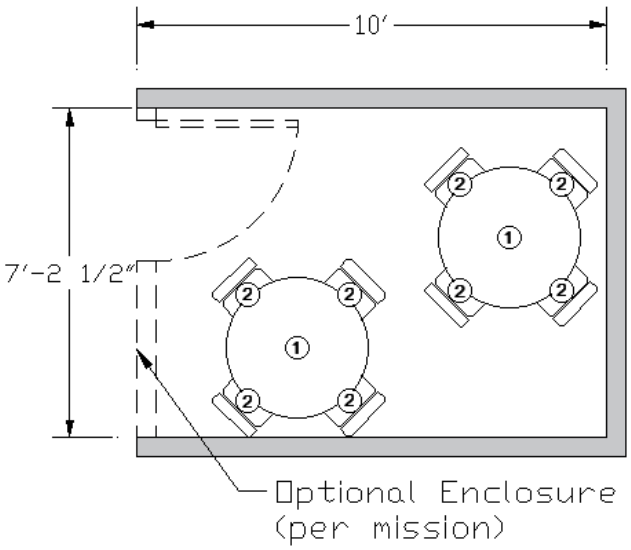
1. LARGE VOLUME COPIER/PRINTER/SCANNER
2. SECURE FAX
3. SHREDDER
4. PAPER BIN
5. BASE CABINET WITH TOP DRAWER AND SHELVES
6. WALL CABINET WITH SHELVES

LEGEND:

TV	VOICE/DATA
KEYED NOTES	DUPLEX OUTLET
SWITCHED OUTLET	GROUND FAULT INTERRUPT DUPLEX OUTLET

STORAGE SPACES

1.17 Huddle Room - 72 SqFt - Scalable (10+ Employees, 5 SqFt per Employee in 72 SqFt Increments) Open unless Mission Requirements Dictate Otherwise



ROOM SPECIFICATIONS

Walls: Building standard (w/acoustic batts
Floors: VCT or Equiv.
Ceiling: Building standard (w/acoustic batts above)
Doors: None
Hinges: None
Hardware: None
Door Locks: None
Door Closer: None
Glazing: None
Plumbing: N/A
HVAC: Typical building standard
Lighting: Typical building standard
Security: Key lock entry
Communications: none

FURNITURE - EQUIPMENT

1. 48" Round Conference Table
2. Conference Chairs

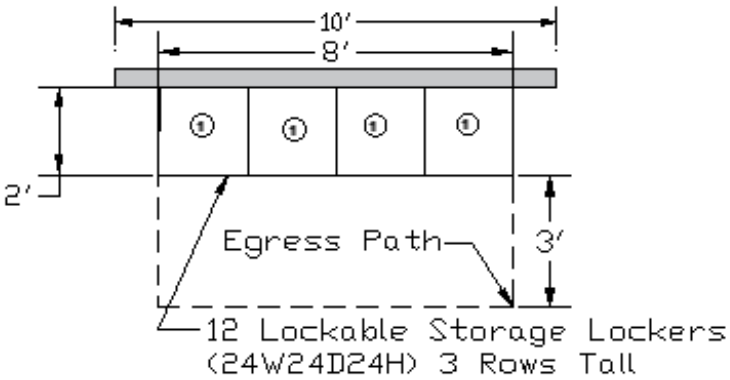
STORAGE SPACES

1.18 Layout/Lockers/File – Scalable 5 SqFt Per LE, increments of typ. 72 SqFt

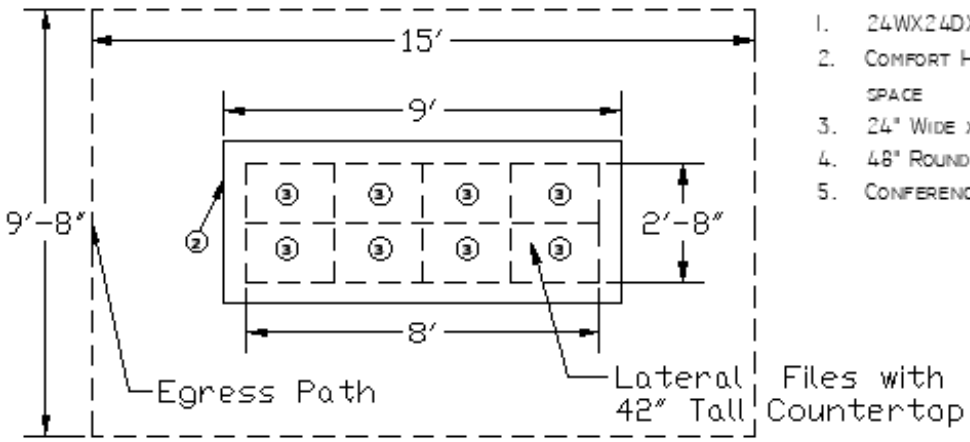
ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ACOUSTIC BATTS
FLOORS: BUILDING STANDARD
CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE
DOORS: NONE
HINGES: NONE
HARDWARE: NONE
DOOR LOCKS: NONE
DOOR CLOSER: NONE
GLAZING: NONE
PLUMBING: N/A
HVAC: TYPICAL BUILDING STANDARD
LIGHTING: TYPICAL BUILDING STANDARD
SECURITY: KEY LOCK ENTRY
COMMUNICATIONS: NONE

LOCKER SPACE



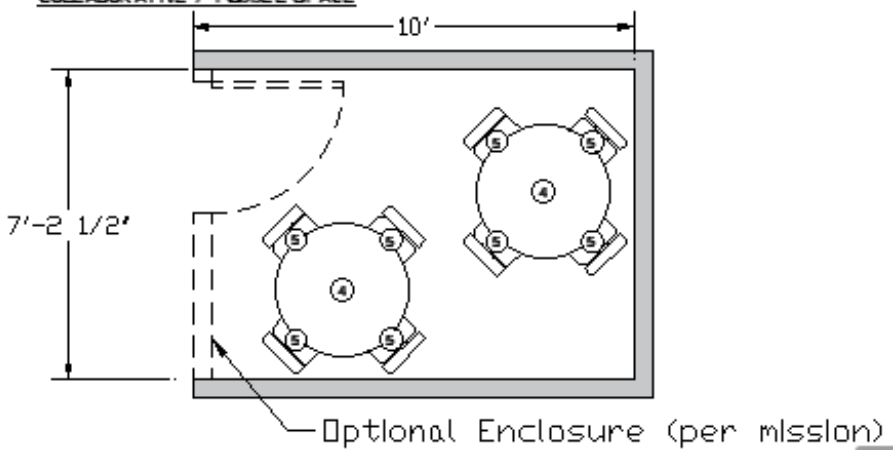
LAYOUT SPACE



FURNITURE - EQUIPMENT

1. 24WX24DX24H LOCKABLE LOCKERS
2. COMFORT HEIGHT (42") COUNTERTOP FOR LAYOUT SPACE
3. 24" WIDE X 18" DEEP LATERAL FILE STORAGE
4. 48" ROUND CONFERENCE TABLE
5. CONFERENCE CHAIRS

COLLABORATIVE / HUDDLE SPACE



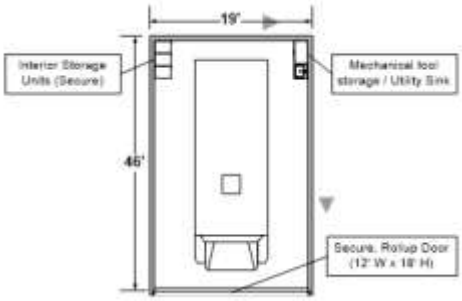
STORAGE SPACES

ASD Storage/Garage Requirements (Large MCV Unit)

The Mobile Command Vehicle program supports the FPS mission through the provision of mobile on-site platforms for command, control and communications during terrorist attacks, natural disasters, National Special Security Events and other similar occurrences. The MCVs can rapidly deploy to any location in the continental United States where the communications infrastructure is adequate or has been disrupted, or where enhanced interoperability among law enforcement agencies is needed.

Contingent on availability, FPS will exhaust all efforts to co-locate MCV/SUV units with other Federal, state, or local government agencies at a free or reduced rate. Storage locations will either be exterior, secured lots or interior garage structures. MCV storage locations should be in a centralized area within the Region that is easily and quickly accessible (access < 1-hour driving distance from an authorized MCV operator).

Location Measurements	Interior Requirements/Equipment
18' Ceiling Height (minimum)	Dedicated 100AMP Circuit
12' Width (minimum)	Building standard electrical outlets
50' Length (minimum)	Dedicated telecom line: RJ-11 (dual)
Ramp entry (10') with 50K load limit	Dedicated network jack: RJ-45 (dual)
Entry/Exit – 25' turning radius (minimum)	Small utility sink
Storage	Accessible faucet for vehicle washing
Lockable storage cabinet	First-aid station w/first aid kit(s)
Mechanical tool storage cabinet	Emergency eye-wash station
Two (2) uniform lockers	Wall mounted Fire Suppressant System



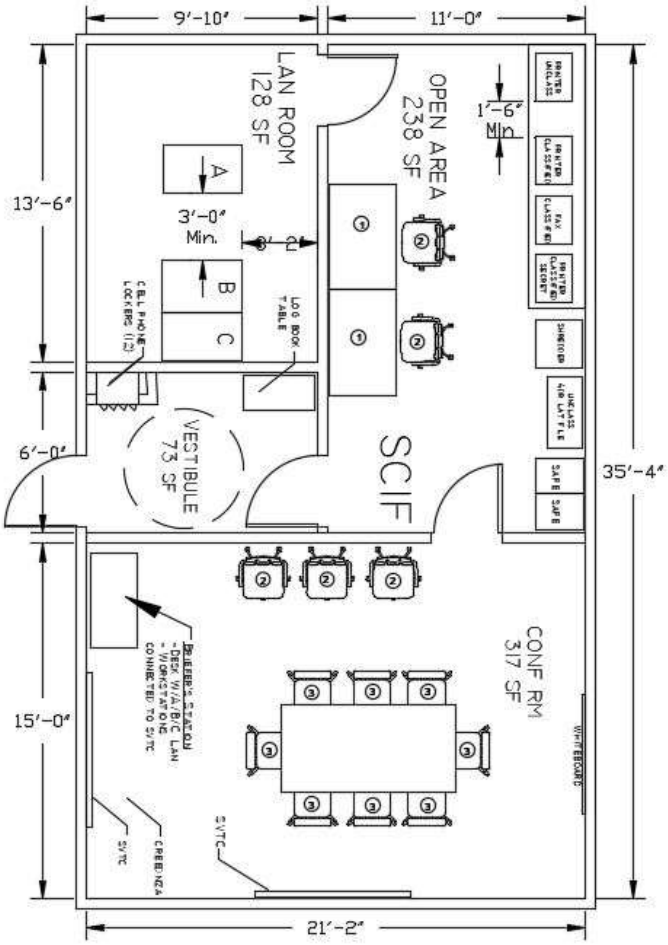
ASD Storage/Garage Requirements (SUV Based MCV Unit: "Rabbit")

The FPS SUV-based mobile communications vehicle ("Rabbit") is a smaller verison of the full-size MCV units. The Rabbits provide most of the same communications capabilities as the MCVs, but lack the command and control space and workstations. The Rabbits afford a rapid deployment capability, as well as the ability to navigate tight spaces and unimproved roads, which allows projection of communications services into areas that would otherwise be inaccessible.

SCIF

SCIF

3.41 REQUIREMENT PROVIDED BY OPS/MGMT



LEGEND:

TV — VOICE/DATA

KEYED NOTES — DUPLEX OUTLET

ROOM SPECIFICATIONS

WALLS: BUILDING STANDARD (W/ ACOUSTIC BATTS

FLOORS: BUILDING STANDARD

CEILING: BUILDING STANDARD (W/ACOUSTIC BATTS ABOVE)

DOORS: NONE

HINGES: NONE

HARDWARE: NONE

DOOR LOCKS: NONE

DOOR CLOSER: NONE

GLAZING: NONE

PLUMBING: HOT/COLD WATER WHERE APPLICABLE

HVAC: TYPICAL BUILDING STANDARD

LIGHTING: TYPICAL BUILDING STANDARD

SECURITY: KEY LOCK ENTRY

COMMUNICATIONS: NONE

POWER: SPECIAL PLUG MAY BE REQUIRED FOR COPIER MACHINE

FURNITURE - EQUIPMENT

1. 30" x 60" WORK SURFACE
2. OFFICE CHAIR
3. CONFERENCE ROOM CHAIR
4. 4' x 10' CONFERENCE TABLE

APPENDIX D: FPS HQ SEAT ASSIGNMENT REQUEST FORM

FPS HQ Seat Assignment Request Form

Office Information	
Requestor:	
Requestor Phone Number:	
FPS Office:	
Date Submitted:	
Name FTE:	
Name Contractor:	
Email Address of FTE/Contractor:	
Suggested Move/Start Date:	
From Building:	
Suite Number	
Office/Cubicle Number:	
To Building:	
Suite Number:	
Office/Cubicle Number:	
Office move requests shall be submitted to Facilities Office NLT 14 days prior to move date	
Comments:	
Requesting Office Approval Signature/Date:	
ASD Approval Signature/Date:	
	Version Date 01/02/19

APPENDIX E: Calculating a Workspace Standard (example)

- An office of 120 employees: 5 managers in Private Offices
- 15 staff Desk Bound Concentrative
- 20 staff Internally Mobile Concentrative
- 75 staff Externally Mobile Interactive
- Private Offices – total space for private offices 2 x 180 and 3 x 100 = 660 NSF*

Workstation Space - Multiply the usable square feet noted in each of the work patterns that apply, taking into consideration the typical workstation used for the office (6x6)

For Desk Bound Concentrative work pattern, we are assuming a 6x6 workstation 48 NSF workstation x 25 staff = 1,200 NSF

For Internally Mobile Interactive work pattern we are assuming a 6x6 workstation 36 NSF workstation x 15 staff = 540 NSF

For Externally Mobile Interactive work pattern we are assuming 2 types of workstations, a 4x6 touchdown station and a 6x6 workstation 24 NSF workstation x 10 staff = 240 NSF; 48 NSF workstation x 65 staff = 3,120 NSF; Total Workstation Space - based on the Work Patterns identified above = 5,100 NSF

Desk Sharing Ratio - Apply desk sharing ratio assuming approximate 50% of employees are 1 desk: 1 employee and 50% are 1 desk: 2 employees for average office sharing ratio of 1:1.5.

Desk Sharing Ratio - (divide by the ratio) 5,100/1.5 = 3,400 NSF

Collaboration Space - Match each Work Pattern with the collaborative space sharing rations in the Appendix – Part 2 (ratios are one room per number of employees for that work pattern);

Desk Bound Concentrative (DBC 20 staff)

- person closed meeting room 1:16 = 1 x 42 NSF= 42 42
- person closed meeting room 1:24 = 1 x 90 NSF= 90
- 6 person closed meeting room 1:40 = 1 x 150 NSF= 150
- 2-person open meeting (at desk)
- person open meeting N/A
- person open meeting N/A

Internally Mobile Interactive (IMI 20 staff)

- person closed meeting room 1:08 = 3 x 42 NSF= 126
- person closed meeting room 1:24 = 1 x 90 NSF= 90
- 6 person closed meeting room 1:32 = 1 x 150 NSF= 150

- 2-person open meeting (at desk)
- person open meeting 1:16 = 1 x 60 NSF
- person open meeting 1:24 = 1 x 90 NSF

Externally Mobile Interactive (EMI 80 staff)

- person closed meeting room 1:24 = 3 x 42 NSF = 126
- person closed meeting room 1:24 = 3 x 90 NSF = 270
- 6 person closed meeting room 1:40 = 2 x 150 NSF= 300
- 2-person open meeting (at desk)
- person open meeting N/A
- person open meeting N/A

General Office Area - Work Station Space (adjusted for Desk Sharing) + Private Offices + Collaboration space; 3,400 + 660 + 1,494 = 5,554 NSF

Special Space - Work Station Space (without desk sharing ratio applied) + Private Offices; 5,760 X .20 = 1,152 NSF

Circulation Factor - 38% circulation factor for an open office configuration (uses a 1.61Circulation Multiplier) - applied to General Office Area + Special Space; 5,554 + 1,152 = 6,706 x 1.61 = 10,797 USF*

New Workspace Standard – 10,800 USF / 120 staff = 90 USF/pp

Federal Protective Service

Area Command Office

Construction Requirements

All Federal Protective Service requirements are in the agency or the Department of Homeland Security Real Property Manual.

Weapons/Ammunition Storage

Wall type: SF4 Interior wall SF5 Perimeter wall.
Floor: Vinyl tile
Ceiling Acoustic tile
Door Solid core
IDS
CCTV
Card reader

For an FPS Federal Law Enforcement Officers Area Command, a weapons and ammunition storage room is treated as a high-risk, exclusion-level space. Requirements are driven by:

- Interagency Security Committee (ISC) Risk Management Process
- DHS/FPS facility security policies
- Applicable life-safety and fire codes (e.g., NFPA)
- Component firearms and armory policies

1. Physical construction and location

- Security zone:
  - Classified as a Restricted or Exclusion Area, not general office space.
- Walls and ceiling:
  - Full-height walls from floor slab to structural deck (no plenum bypass).
  - Construction robust enough to resist forced entry for the delay time specified by the risk assessment.
- Door and frame:
  - Solid-core or steel door with reinforced frame.
  - Security-grade hinges and hardware; no removable hinge pins on the unsecured side.
- Interior layout:
  - Dedicated weapons racks and lockable storage for firearms.
  - Separate, clearly marked storage for ammunition, with fire/life-safety compliance.

2. Access control (PACS) and keys

- Electronic access control:
  - Door controlled by a DHS-approved, PIV-enabled PACS (FIPS 201 compliant).
  - Access restricted to designated armorers and specifically authorized law enforcement personnel.
- Authentication:

    - Multi-factor (PIV + PIN; biometric where required by risk level or policy).
- Two-person integrity (where required):
    - Policy may require two authorized individuals present for certain actions (e.g., issuing or returning weapons, inventory).
- Audit trail:
    - All access attempts (granted and denied) logged with user ID, date/time, and door ID.
- Mechanical backup:
    - High-security mechanical lock with tightly controlled key issuance and key control records.

3. Intrusion detection system (IDS)

- Perimeter detection:
    - Door position switch on all doors.
    - Interior motion detectors cover the entire room.
- Tamper protection:
    - Supervised circuits and tamper switches on IDS devices and panels.
- Monitoring:
    - 24/7 alarm monitoring by a staffed security operations center or guard post.
- Alarm conditions:
    - Forced door, door held open, motion when armed, tamper, and system trouble.
- Arming/disarming:
    - Restricted to authorized personnel; all events logged.

4. CCTV / video surveillance

- Coverage:
    - Camera(s) covering the entrance/vestibule to the weapons room.
    - Often, additional coverage of the immediate interior issue/return area (subject to policy).
- Performance:
    - Sufficient resolution and lighting to positively identify individuals.
    - Time-synchronized with PACS/IDS for event correlation.
- Recording and retention:
    - Continuous or event-triggered recording.
    - Retention period consistent with DHS/FPS and component policy (commonly 30–90 days minimum, often longer for weapons rooms).

5. Weapons and ammunition–specific controls

- Inventory control:
    - Formal inventory procedures (daily/shift checks, periodic full inventories).
    - Reconciliation of physical counts with records; discrepancy reporting procedures.
- Issuance and return:

    - Documented sign-out/sign-in process (electronic or paper) tied to individual officers.
    - Procedures for after-hours access and emergency issuance.
- Ammunition storage:
    - Stored separately from weapons where required by policy or code.
    - Compliance with fire/life-safety and quantity-distance requirements, as applicable.
- Segregation:
    - Segregated storage for specialty weapons, less-lethal munitions, and training vs. duty ammunition, per policy.

6. Governance and approvals

- Risk-based design:
    - Final measures are based on the Facility's Security Level (FSL) and FPS risk assessment.
- FPS involvement:
    - FPS Physical Security Specialist/Inspector typically reviews and validates design and installed countermeasures.
- Component policy:
    - Must align with FPS guidance and the component's firearms/armory directives (e.g., issuance rules, inventory frequency, reporting).

Non-Lethal Weapon Storage
Wall type: SF3
Floor: Colored epoxy floor similar to Florock.
https://www.florock.net/polymer-flooring/florochip/
Ceiling: Acoustic tile
Door: Solid core
Card Reader

1. Storage location and physical security

- Controlled area:
    - Non-lethal weapons should be stored in a locked, controlled space—often within an armory, equipment room, or secure supply room, not in open office areas.
- Lockable containers:
    - Use lockable cabinets, cages, or lockers that are bolted or otherwise secured to the structure.
    - Construction should be sturdy enough to resist casual forced entry (not flimsy furniture-grade cabinets).
- Segregation:
    - Separate storage for:
        - Duty vs. training munitions
        - Specialty less-lethal munitions (e.g., impact rounds, chemical agents)

2. Access control and accountability

- Limited access:
    - Access restricted to authorized FPS personnel (e.g., supervisors, equipment custodians, designated officers).

- Key or PACS control:
  - Keys or combinations tightly controlled and documented; or
  - Storage is located inside a PACS-controlled room (PIV card access) with a smaller lockable container inside.
- Issuance and return records:
  - Sign-out/sign-in logs (paper or electronic) for individually assigned non-lethal weapons and munitions.
  - Records should show who has what, when it was issued, and when it was returned or expended.

3. Inventory and inspection

- Periodic inventories:
  - Regular inventories (e.g., monthly or quarterly) of non-lethal weapons and munitions, with reconciliation against records.
- Spot checks:
  - Supervisory spot checks to confirm proper storage, condition, and accountability.
- Discrepancy procedures:
  - Written procedures for reporting and investigating missing or damaged non-lethal weapons or munitions.

4. Safety and environmental considerations

- Manufacturer guidance:
  - Storage conditions (temperature, humidity, orientation) should follow manufacturer recommendations, especially for OC, CEW cartridges, and chemical/impact munitions.
- Segregation from ignition sources:
  - Less-lethal munitions stored away from heat sources or conditions that could degrade propellants or casings.
- Packaging and labeling:
  - Clearly labeled containers for different types and calibers of less-lethal munitions to avoid misuse.

5. Integration with broader FPS security posture

- Co-location with firearms armory (common):
  - Many FPS locations store non-lethal weapons inside or adjacent to the firearms armory, inheriting the higher security level of that space.
- Risk-based adjustments:
  - Higher-risk facilities or missions may require:
    - Storage inside an armory-grade room
    - Additional CCTV coverage
    - Tighter access controls and more frequent inventories

Huddle room
Wall type: SF3
Floor: Carpet
Ceiling: Acoustic tile
Door: Solid core

A huddle room supporting an FPS Area Command Office in an 80 sq ft footprint needs furniture that enables short meetings, rapid coordination, and secure conversations without overcrowding the space. The requirements below balance function, durability, circulation, and federal workspace standards.

Purpose and functional expectations

The huddle room must support brief meetings, virtual calls, and small-group discussions for 2–3 personnel at a time. Furniture must fit within the limited footprint while maintaining clear circulation and accessibility.

- Designed for short-duration collaboration, not long-term occupancy.
- Must support in-person and virtual communication.
- Must maintain a professional, secure environment appropriate for FPS operations.

Space and layout requirements

The layout must preserve usable floor area and avoid obstructing movement.

- Total furniture footprint must allow at least 36 inches of clear circulation from the door to the seating area.
- Furniture arranged to avoid blocking the egress point.
- Wall-mounted or compact furniture preferred to maximize usable space.

Table and work surface requirements

A compact, durable meeting surface is required for laptops, notetaking, and small equipment.

- One small meeting table (round or square) sized approximately 30–36 inches in diameter/width.
- Table must be commercial-grade, stable, and easy to clean.
- Optional wall-mounted fold-down table permitted if space constraints require it.

Seating requirements

Seating must support short meetings while fitting within the limited footprint.

- Two to three chairs maximum, depending on final layout.
- Chairs must be armless to reduce space consumption and improve maneuverability.
- Chairs must be commercial-grade, durable, and easy to clean.

- Stackable or lightweight seating preferred for flexibility.

Technology and accessory furniture

The room must support FPS operational needs for virtual meetings and quick coordination.

- Wall-mounted monitor (up to 43") or display bracket to avoid consuming floor space.
- Small equipment shelf or wall-mounted ledge for camera, speakerphone, or collaboration tools.
- Cable management channels to keep cords off the floor.
- Optional small whiteboard or glass board for quick planning sessions.

Storage and accessory requirements

Storage must be minimal to preserve space.

- No floor-standing storage cabinets unless required for mission-specific items.
- One wall-mounted floating shelf permitted for small supplies or reference materials.
- Coat hook or small wall-mounted rack allowed if needed.

Durability and safety considerations

Furniture must meet federal workspace durability and safety expectations.

- All furniture must be commercial-grade and compliant with fire and safety codes.
- Rounded corners preferred to reduce injury risk in tight spaces.
- Slip-resistant flooring clearance maintained around furniture.

Acoustic and privacy considerations

Because huddle rooms often support sensitive discussions:

- Furniture placement should support clear sightlines for virtual meetings.
- Soft seating or acoustic panels may be used if needed to reduce echo.
- Door must close fully without obstruction from furniture.

IT LAN Closet
Wall type: SP
Fire resistant plywood to be mounted on 4 walls
Floor: Colored epoxy floor similar to Florock.
https://www.florock.net/polymer-flooring/florochip/
Ceiling Acoustic tile
HVAC 6,000 BTU cooling required
Card reader
IDS
Details of equipment placement required in design

Room to house IT, VOIP, IDS and CCTV equipment.

Office Support Area
Install dedicated 110V 20Amp electrical circuit for copy machine.

1. Office Support Space Requirements

1.1 Room Size & Layout

- Provide a dedicated alcove or room sized to accommodate:
  - Copier/MFD footprint
  - 36" minimum clearance on all service sides
  - Space for paper storage and consumables
- Maintain a minimum of 5 ft clear turning radius for equipment movement and maintenance.

1.2 Environmental Conditions

- Temperature: 68–75°F
- Relative humidity: 30–60%
- Avoid direct sunlight, heat sources, or HVAC supply blowing directly onto the machine.

1.3 Flooring

- Use durable, static-resistant flooring (LVT, sealed concrete, or commercial carpet tile).
- Avoid high-pile carpet.

1.4 Noise & Placement

- Locate copier away from:
  - Workstations
  - Conference rooms
  - Sensitive operational areas
- Provide acoustic ceiling tiles (NRC 0.55+) to reduce noise.

1.5 Storage

- Provide adjacent storage for:
  - Paper reams
  - Toner
  - Maintenance kits
  - FPS forms and administrative supplies

2. Electrical Requirements

2.1 Dedicated Circuit

- Provide a dedicated 120V, 20A circuit for the copier/MFD.
- Circuit must serve **no other equipment**.

2.2 Receptacle Type & Location

- NEMA 5-20R receptacle.
- Mount at 18" AFF unless otherwise required by ADA or equipment specs.
- Locate receptacle directly behind or adjacent to the copier's power inlet.

2.3 Power Quality

- Voltage tolerance: ±10%
- Provide surge protection or UPS if required by FPS IT.
- Ensure grounding meets NEC requirements.

2.4 Additional Outlets

- Provide two general-purpose outlets nearby for:
    - Laptop servicing
    - Shredders
    - Auxiliary office equipment

3. IT & Network Requirements

3.1 Network Connectivity

- Provide one (1) Cat6 or Cat6A data drop terminated at:
    - A wall plate behind the copier, or
    - A floor box if required by layout
- Drops must be home-run to the FPS-designated network closet.

3.2 Network Configuration

- Copier must connect to FPS network via:
    - Wired Ethernet (preferred)
    - Wireless is not permitted for FPS devices unless explicitly authorized.

3.3 Security Requirements

- All network connections must comply with:
    - FPS IT security policies
    - DHS cybersecurity requirements
- Copier must support:
    - Encrypted print (TLS 1.2 or higher)
    - Secure erase
    - Access control (PIN or CAC if required)

3.4 Print Server / IP Assignment

- Provide static IP assignment capability.
- Coordinate with FPS IT for:
    - VLAN placement

    - Firewall rules
    - Print server integration

4. Ventilation & Safety Requirements

- Provide adequate ventilation to dissipate heat from the copier.
- Avoid enclosed cabinets or tight alcoves without airflow.
- Ensure the space complies with:
    - NFPA standards
    - Local fire code
    - Clearance around electrical equipment

5. Accessibility Requirements

- Copier controls must be reachable within 48" max height.
- Provide clear floor space for wheelchair access per ADA guidelines.

6. Installation & Coordination Requirements

- A&E must coordinate:
    - Copier dimensions
    - Service clearances
    - Power and data locations
    - Delivery path and door widths
- Provide a scaled equipment layout showing:
    - Copier footprint
    - Clearances
    - Outlet locations
    - Data jack locations

Bulk storage room
Wall type: SF
Floor: Colored epoxy floor similar to Florock.
https://www.florock.net/polymer-flooring/florochip/
Ceiling: Acoustic tile
Door: Solid core

A bulk storage room supporting seven law enforcement officers and two administrative staff in a Federal Protective Service (FPS) office needs to provide secure, organized, and durable storage within a 120 sq ft footprint. The requirements below outline the expected space, security, furniture, and functional features appropriate for an FPS operational environment.

Space purpose and functional expectations

The room must support day-to-day operational storage needs for a small FPS office, including equipment, supplies, and administrative materials.

- Designed for non-sensitive bulk items, not weapons, evidence, or controlled materials.
- Layout must allow safe circulation and access to all storage units without obstruction.
- Clear floor area maintained for loading/unloading items.

Physical space and construction requirements

The room must be built to support secure and durable storage.

- Minimum 120 sq ft, configured as a rectangular or near-rectangular room for efficient shelving layout.
- Full-height walls from floor slab to structural ceiling to prevent overhead access.
- Solid-core door with commercial-grade hardware.
- Adequate lighting for visibility across all shelving rows.
- Slip-resistant, easy-to-clean flooring.

Access control and security

Because the room stores operational equipment and administrative supplies, access must be controlled.

- Door secured with a keyed lock or PACS-controlled access, depending on facility standards.
- Access limited to designated FPS personnel (LEOs and administrative staff).
- Door position switch recommended if located within a restricted suite.
- No public or visitor access.

Storage furniture requirements

Furniture must maximize vertical space while maintaining safe access in a compact room.

- Four to six heavy-duty metal shelving units, adjustable, with a minimum load rating suitable for equipment and supply storage.
- One lockable storage cabinet for items requiring additional control (e.g., uniforms, electronics, consumables).
- Open shelving for bulk items such as cleaning supplies, PPE, office consumables, and operational gear.
- Clear labeling areas on shelves and cabinets for inventory organization.
- Optional rolling cart for moving supplies in and out of the room.

Layout and circulation

The arrangement must support efficient use of space and safe movement.

- Shelving placed along perimeter walls and, if space allows one central row with at least 36 inches of aisle clearance.
- Storage cabinet positioned near the entrance for quick access to frequently used items.
- No shelving placed behind the door swing.
- Items stored by frequency of use to reduce congestion.

Environmental and safety considerations

The room must support safe storage of typical FPS operational supplies.

- Adequate ventilation to prevent heat buildup around stored items.
- Fire-safe materials for shelving and cabinetry.
- No flammable or hazardous materials are stored unless room is specifically rated for such items.
- Trash and recycling receptacles placed outside the storage room to maintain cleanliness and reduce clutter.

Operational considerations for FPS

The storage room must support the workflow of a mixed law enforcement and administrative team.

- Sufficient capacity for shared equipment (e.g., PPE, radios, training materials, office supplies).
- Durable furniture is capable of withstanding daily use.
- Organized layout to reduce time spent retrieving items.
- Inventory system (manual or digital) is recommended for tracking consumables and equipment.

Open Break Area, small
Open break room large enough to accommodate table seating for 4 personnel. Counter seating for 4 if space is available.

Wall type: SP
Floor: LVT, Sealed concrete, or an epoxy resin flooring with slip-resistant finish
Ceiling: Acoustic tile

The break area should be arranged as a linear or L-shaped galley to maximize circulation and keep appliances accessible without obstructing movement. A minimum 36-inch clear walkway should be maintained for safe passage, even when seating is occupied.

- Countertop length sufficient to support a sink, microwave, coffee maker, and small appliances without crowding.
- Seating for four using compact café-style chairs, a small table, or a built-in counter with stools to conserve floor space.
- Clear separation between food-prep surfaces and seating to avoid congestion during peak use.

Sink and disposal requirements

The sink and disposal must be sized and installed to support daily use while meeting plumbing and electrical safety standards.

- Single-basin sink with hot and cold-water supply.
- Garbage disposal rated for light commercial or high-use residential duty.
- Dedicated switch for disposal, placed safely away from the sink edge.
- GFCI-protected outlets in all locations required by code.

- Under-sink cabinet for plumbing access, disposal housing, and cleaning supplies.
- Adequate ventilation to prevent moisture accumulation.

Electrical and appliance requirements

The galley must safely support the electrical load of common break-area appliances.

- Dedicated circuits for microwave and refrigerator to prevent overload.
- GFCI-protected outlets above the counter for coffee maker and small appliances.
- Space and power for:
  - One microwave
  - One mid-size refrigerator
  - One coffee maker
  - Optional water dispenser or compact appliance
- Proper clearance around appliances for heat dissipation and safe operation.

Water line requirement – FPS galley-style kitchen refrigerator

(Filtered water dispenser & ice maker)

- Water supply type:
  - Cold potable water only, from building domestic cold water system.
- Pipe size & material:
  - Minimum 1/4" OD dedicated supply line.
  - Acceptable materials: Type L copper tubing or stainless-steel braided flexible line rated for potable water and appliance use.
- Shutoff & isolation:
  - Provide a dedicated, accessible shutoff valve (¼-turn ball valve) serving only the refrigerator.
  - Valve to be located in the same room, within 6 ft of the appliance, not behind permanently fixed casework.
- Backflow & code compliance:
  - Provide backflow protection as required by applicable plumbing code (integral to valve, device, or appliance as approved).
  - All work shall comply with local plumbing code, NFPA, and GSA/FPS facility standards.
- Pressure & flow:
  - Static pressure at connection point: 40–80 psi.
  - If building pressure exceeds 80 psi, provide a pressure-reducing valve on the branch serving the refrigerator.
- Connection location:
  - Terminate water line in a recessed wall box or finished wall outlet directly behind or adjacent to the refrigerator niche, at 6"–12" above finished floor, coordinated with appliance depth and clearance.
- Identification & coordination:
  - Clearly label the shutoff valve “REFRIGERATOR WATER – FPS GALLEY.”

    - Coordinate final location and connection type with the refrigerator manufacturer's installation instructions and FPS layout requirements.

Storage and cabinetry

Cabinetry should maximize vertical space while keeping the footprint compact.

- Upper cabinets for cups, plates, and dry goods.
- Lower cabinets for cleaning supplies and small appliance storage.
- Durable, easy-to-clean surfaces suitable for daily use.

Seating and occupant comfort

The seating area must fit comfortably within the 120 sq ft limit without obstructing appliance access.

- Seating for up to four using:
    - A small table with four chairs, or
    - A wall-mounted counter with stools to save space
- Chairs or stools that can be tucked away to maintain circulation.
- Adequate lighting for both food prep and dining.

Safety, code, and accessibility considerations

The break area must comply with building codes and workplace safety requirements.

- Fire-safe materials for counters and cabinetry.
- Proper ventilation for heat-producing appliances.
- Slip-resistant flooring.
- ADA-compliant clearances where applicable.
- Trash and recycling receptacles placed to avoid blocking walkways.

Operational considerations for an FPS office

Because this supports a federal law enforcement workspace, the design should emphasize durability and low maintenance.

- Commercial-grade appliances preferred for reliability.
- Surfaces are resistant to heavy daily use.
- Easy-to-clean finishes to support hygiene in a shared environment.
- This space could operate as flexible multiple purpose area offering the storage of cleaning supplies, emergency response kits, a wall-mounted AED, go bags, and placement of other response equipment such as flashlights, radios, and a portable batteries charging station

K9 Storage
Wall type: SP
Floor: Colored epoxy floor similar to Florock.
https://www.florock.net/polymer-flooring/florochip/

Ceiling: Acoustic tile
Door: Solid core

The storage area must support all equipment required for two operational FPS working dogs and their handlers, including duty gear, training aids, medical supplies, and maintenance items. The space must allow quick access while maintaining strict control over sensitive or high-value items.

Space and layout requirements

The room or designated storage zone must be sized and arranged to accommodate bulky K-9 equipment without obstructing circulation.

- Clear floor area for storing crates, deployment bags, and protective gear.
- Wall space for mounted racks, hooks, or shelving.
- Layout that keeps training aids and operational gear separated to avoid cross-contamination.
- Adequate lighting for safe handling of equipment.

Storage furniture and equipment

Furniture must be durable, easy to clean, and capable of supporting heavy or irregularly shaped items.

- Heavy-duty shelving units for leashes, harnesses, bite sleeves, muzzles, boots, and grooming tools.
- Lockable cabinet for sensitive items such as medical kits, narcotics training aids (if applicable), and high-value gear.
- Ventilated storage bins for wet or odor-producing items.
- Wall-mounted hooks or rails for vests, leads, and deployment belts.
- Space for two portable or collapsible K-9 crates.
- Floor-rated storage for bulk items such as food containers or cleaning supplies.

Security and access control

Because K-9 equipment includes controlled training aids, medical supplies, and operational gear, access must be restricted.

- Room secured by keyed or PACS-controlled access limited to K-9 handlers, supervisors, and designated personnel.
- Lockable cabinet or safe for any sensitive training aids or controlled substances used for detection training.
- Clear accountability for keys, combinations, or access permissions.

Environmental and hygiene requirements

K-9 equipment must be stored in conditions that preserve safety, cleanliness, and operational readiness.

- Adequate ventilation to prevent odor buildup and moisture retention.
- Temperature-controlled environment to protect food, medical supplies, and electronics.
- Non-porous, easy-to-clean flooring.
- Storage solutions that allow wet gear to dry without mold or odor accumulation.
- Spill-proof containers for food and cleaning chemicals.

Operational considerations for FPS K-9 teams

The storage area must support daily deployment and training cycles.

- Quick-access layout for emergency response or rapid mobilization.
- Dedicated space for replenishing medical kits and maintaining equipment.
- Organization system (labels, bins, or inventory list) to track consumables and replacements.
- Separation of duty gear from training aids to maintain scent integrity for detection dogs.

Indoor K-9 Magazine requirements

1. Purpose

This document defines the minimum requirements for an **indoor explosives storage magazine** to support **FPS and Homeland Security (HDS) K9 operations**. The magazine will store operational explosive training aids in compliance with **ATF**, **DHS**, and **FPS** safety and security standards.

2. Magazine Type

The indoor magazine shall be an ATF-approved Type 2 Cabinet-Style Indoor Magazine, meeting or exceeding the construction and security requirements of 27 CFR Part 555, Subpart K.

The magazine must be:

- Designed for indoor use only
- Constructed for high-security explosives storage
- Equipped with front-opening doors for safe and efficient access
- Manufactured to meet or exceed Armag’s Type 2 cabinet specifications

3. Standard Sizes (Acceptable Options)

The magazine shall be provided in one of the following standard sizes, depending on storage needs and available space:

Model Size (W × D × H)
36 in. × 24 in. × 36 in.
48 in. × 24 in. × 48 in.
36 in. × 36 in. × 72 in.
60 in. × 28 in. × 72 in.

Custom sizes may be used if operational requirements dictate and if they remain compliant with ATF Type 2 construction standards.

4. Construction Requirements

The indoor magazine must meet the following:

4.1 Structural Construction

- Double-wall steel construction
- Minimum 12-gauge outer steel shell
- Minimum 20-gauge inner steel liner
- Insulated with non-spark, non-conductive material
- Welded or continuous-seam construction
- Interior surfaces must be non-sparking

4.2 Door Construction

- Full-height, front-opening doors
- Heavy-duty hinges, welded or securely fastened
- Reinforced locking hasps
- Doors must open fully for safe handling of explosive aids

5. Security Requirements

The magazine must comply with ATF 27 CFR 555.208 for indoor Type 2 magazines:

- Two padlocks, each meeting ATF high-security requirements
- Locks must be:
    - 5-pin or greater
    - Case-hardened
    - Protected from prying, sawing, and cutting
- Magazine must be anchored or secured to prevent unauthorized removal
- Room housing the magazine must be:
    - Access-controlled
    - Under FPS or facility security oversight
    - Equipped with intrusion detection or CCTV coverage

6. Ventilation & Environmental Requirements

- Indoor magazines do not require exterior ventilation but must be stored in a dry, climate-controlled space
- Room must maintain:
  - Stable temperature
  - Low humidity
  - No direct heat sources
- Magazine must be kept away from:
  - Electrical panels
  - Ignition sources
  - Flammable liquids

7. Location & Installation Requirements

- Magazine must be installed **indoors only**
- Must be placed in a **restricted-access room** used exclusively for:
  - K9 explosive training aids
  - Operational storage
- Magazine must be:
  - Level and stable
  - Anchored to floor or wall (unless weight exceeds ATF exemption threshold)
  - Positioned to allow full door swing and safe loading/unloading

8. Operational Requirements

- Only authorized FPS/HDS personnel may access the magazine
- Inventory must be logged per DHS/FPS explosives accountability procedures
- Magazine must remain locked when not in active use
- No ignition sources or prohibited materials may be stored inside

9. Compliance

The indoor K9 magazine must comply with:

- ATF 27 CFR Part 555 (Explosives Storage Regulations)
- DHS/FPS explosives handling protocols
- NFPA 495 – Explosive Materials Code
- Local fire and building codes
- Facility Security Level (FSL) requirements

Tactical Storage
Wall type: SP
Floor: Colored epoxy floor similar to Florock.
https://www.florock.net/polymer-flooring/florochip/
(7) 18 – 36” TA-50 style storage lockers. See attached specifications.
(Construction contractor provided)
Room to be sized to accommodate lockers.

A tactical storage room for seven FPS law enforcement officers needs to support secure, organized, and mission-ready storage of operational gear while fitting within FPS facility and security expectations. The requirements

below outline the **space, security, furniture, environmental, and operational standards** appropriate for an FPS tactical equipment room.

Tactical storage purpose and operational expectations

The room must support daily deployment and training needs by providing secure storage for tactical gear such as body armor, helmets, shields, breaching tools, PPE, radios, and specialty equipment. The layout must allow quick retrieval and safe handling of heavy or bulky items.

- Designed exclusively for tactical and operational equipment, not weapons, ammunition, or evidence.
- Must support rapid access, organized storage, and accountability for shared gear.
- Must accommodate equipment for seven FPS law enforcement officers.

Space and physical layout

The room must be sized and arranged to safely store bulky tactical items while maintaining clear circulation.

- Sufficient square footage to allow 36 inches of clear aisle space between shelving or storage units.
- Full-height walls from floor slab to structural ceiling to prevent overhead access.
- Solid-core or steel door with commercial-grade hardware.
- Lighting adequate for identifying and retrieving equipment.
- Slip-resistant, durable flooring suitable for heavy gear.

Access control and security

Because tactical gear is mission-critical and high-value, access must be restricted and controlled.

- Door secured by PIV-enabled PACS or a high-security keyed lock, depending on facility standards.
- Access limited to authorized FPS officers, supervisors, and designated personnel.
- Door position switch recommended if located within a restricted suite.
- No public or visitor access.

Storage furniture and equipment

Furniture must be durable, load-rated, and configured to support a variety of tactical gear types.

- Heavy-duty metal shelving units capable of supporting helmets, armor plates, shields, and equipment bags.
- Lockable storage cabinet for sensitive or high-value items such as radios, optics, or specialty tools.

- Individual cubbies or gear lockers for each of the seven officers, sized for vests, belts, boots, and duty bags.
- Wall-mounted hooks or rails for helmets, vests, and frequently accessed gear.
- Open bins or totes for PPE, gloves, and consumables.
- Floor-rated storage space for large items such as breaching tools or protective shields.
- Clear labeling on all shelves, lockers, and bins to support organization and accountability.

Environmental and safety requirements

The room must maintain conditions that preserve the integrity and readiness of tactical equipment.

- Adequate ventilation to prevent moisture buildup and odor retention.
- Temperature-controlled environment to protect electronics, radios, and PPE.
- Non-porous, easy-to-clean surfaces.
- Fire-safe shelving and cabinetry.
- No storage of flammable or hazardous materials unless the room is specifically rated for such items.

Operational considerations for FPS tactical teams

The room must support efficient deployment and sustainment of tactical operations.

- Layout must allow quick access to gear during emergency response.
- Space for staging or temporarily placing equipment during inspections or maintenance.
- Organization system (labels, inventory lists, or digital tracking) to maintain accountability.
- Separation of training gear from operational gear to prevent cross-use or confusion.
- Storage solutions that prevent damage to radios, optics, and protective equipment.

Integration with FPS facility standards

The tactical storage room must align with FPS and ISC facility security requirements.

- Located within a restricted-access FPS suite or controlled operational area.
- Designed to support FPS risk-based facility security posture.
- Compliant with DHS privacy and property accountability requirements for government-issued equipment.

Detainee/Handcuff Bench/Processing Room

This document defines the minimum requirements for the design and construction of an FPS Detainee Hold Room, Handcuff Bench Area, and Processing Room within a federally controlled facility. The space must support short-term detention, safe processing, and secure monitoring of detainees in accordance with FPS operational procedures and DHS standards.

General Requirements

- All spaces must be located within a secure, access-controlled area.
- Materials, fixtures, and hardware must be tamper-resistant, vandal-resistant, and suitable for detention environments.
- All systems must comply with DHS, FPS, GSA PBS P-100, ADA, NFPA, and local building codes.
- Design must support officer safety, detainee safety, and efficient workflow.

3. Detainee Hold Room Requirements

3.1 Room Size & Layout

- Minimum 37 sq ft for a single-occupant hold room.
- Additional 7 sq ft of unencumbered space per additional detainee for multi-occupant rooms.
- Clear sightlines from the officer monitoring position.
- No blind corners or obstructions.

3.2 Construction & Finishes

- Walls: reinforced, tamper-resistant, durable finishes.
- Floor: slip-resistant, seamless, and easy to sanitize.
- Ceiling: secure, non-removable panels or hard lid.

3.3 Fixtures

- Stainless-steel combination toilet/lavatory unit.
- Minimum fixture count per DHS standards:
    - 1 unit for ≤14 detainees
    - 2 units for 15–49 detainees
- Drinking water access integrated into the fixture.

3.4 Environmental Controls

- Adequate ventilation and temperature control.
- Lighting must be:
    - Vandal-resistant
    - Evenly distributed
    - Controlled externally

3.5 Security Features

- Detention-grade door and frame.

- Exterior-controlled door hardware.
- CCTV coverage with no blind spots.
- Duress alarm accessible to FPS officers.

4. Handcuff Bench Requirements

4.1 Bench Construction

- Bench must be fixed to the floor or wall.
- Must withstand 250 lbs horizontal force on all components.
- Constructed of durable, non-removable, tamper-resistant materials.

4.2 Restraint Features

- Integrated handcuff bar or restraint rings spaced appropriately for multiple detainees.
- Hardware must be detention-grade and securely anchored.

4.3 ADA Requirements

- At least one bench must meet ADA standards:
    - Minimum 42" length
    - 20"–24" depth
    - 17"–19" seat height
    - Back support required

5. Processing Room Requirements

5.1 Functional Layout

- Space must support:
    - Intake
    - Identification
    - Documentation
    - Property handling
- Clear separation of:
    - Public circulation
    - Staff circulation
    - Detainee movement

5.2 Workstation Requirements

- Secure FPS officer workstation with:
    - Power and data
    - Access to FPS systems
    - Lockable storage for equipment and documents

5.3 Security Systems

- CCTV coverage of all processing activities.
- Duress alarm system integrated with facility security.

- Access control for all entry/exit points.

5.4 Materials & Durability

- All surfaces must be:
  - Easy to sanitize
  - Resistant to impact and tampering
  - Suitable for high-security environments

6. Accessibility Requirements

- At least 3% of holding cells must be ADA-accessible (minimum one).
- Accessible rooms must include:
  - Required clearances
  - Accessible fixtures
  - ADA-compliant bench (if applicable)

7. Deliverables (for A&E or Contractor Use)

- Floor plans, elevations, and sections
- Mechanical, electrical, plumbing, and security system drawings
- Material and fixture specifications
- Code compliance analysis
- Construction phasing plan (if required)

Office/Workstation Furniture Requirements

Untethered Electric Adjustable-Height Desk Workstations Department of Homeland Security – Federal Law Enforcement Operations

1.0 Purpose

The purpose of this Performance Work Statement (PWS) is to define the requirements for the acquisition, delivery, and installation of multiple untethered electric adjustable-height desk workstations to support DHS federal law enforcement personnel. These workstations must provide ergonomic flexibility, operational reliability, and the capability to support dual-monitor configurations, multiple low-voltage devices, and secure cable-management solutions consistent with DHS mission needs and facility standards.

2.0 Background

DHS federal law enforcement personnel require modern, adaptable workstations that support high-intensity operational environments, including investigative, intelligence, and command-and-control functions. Workstations must accommodate multiple electronic devices, ensure safe use, provide cable management solutions, and operate independently through the continuous power connection-supply (wall, floor, or a ceiling power pole) to support flexible workspace layouts and continuity of operations.

3.0 Scope

The Contractor shall provide all labor, materials, equipment, tools, transportation, and supervision necessary to deliver and install fully functional untethered electric adjustable-height workstations that meet the specifications outlined in this PWS. All work shall comply with DHS facility standards, federal ergonomic guidelines, and applicable safety and electrical codes.

4.0 Requirements

4.1 Workstation Functional Requirements

- Electric height-adjustable desk with smooth, quiet operation suitable for seated and standing use.
- Untethered power capability (battery or equivalent integrated system) capable of supporting a full duty day under typical load.
- Load capacity sufficient for:
  - Two monitors (up to 27” each or as specified by DHS)
  - Six low-voltage devices (e.g., docking station, keyboard, mouse, VoIP phone, headset base, mobile device charger)
  - One task light
- Stable frame construction that prevents wobbling at full height extension.

4.2 Power and Electrical Requirements

- Integrated power system capable of supporting all connected devices without continuous wall power.
- Rechargeable power module with safety certifications (UL, FCC, or equivalent).
- Surge protection or power-conditioning features.
- Minimum of:
  - Four AC outlets
  - Two USB-A ports
  - One USB-C port (preferred)
- Power system must not interfere with DHS low-voltage or secure communications equipment.

4.3 Monitor Support Requirements

- Dual-monitor arms or mounting system compliant with VESA standards.
- Full adjustability including height, tilt, swivel, and depth.
- Integrated cable routing within the monitor arm assembly.

4.4 Cable Management Requirements

- Built-in cable-management channels, trays, or raceways.
- Ability to conceal and secure all power and data cables.
- Cable-management system must remain functional throughout full height-adjustment range.
- No exposed wiring that could create safety hazards or compromise operational security.

4.5 Desk Surface and Construction

- Durable, scratch-resistant work surface suitable for daily law enforcement use.
- Surface area adequate for monitors, peripherals, and operational materials.
- Rounded or ergonomic front edge preferred.
- Frame and components constructed of high-quality materials designed for long-term use.

5.0 Installation Requirements

- Delivery and installation at DHS-designated secure facilities.
- Assembly of all workstation components, including monitor arms and cable-management systems.
- Functional testing of:
    - Height-adjustment mechanism
    - Power system
    - Device support capability
- Removal and disposal of all packaging materials in accordance with DHS facility procedures.
- Contractor personnel must comply with DHS security and access requirements.

6.0 Security Requirements

- Contractor personnel must undergo DHS visitor screening and comply with escort requirements.
- No contractor equipment may connect to DHS networks.
- All materials must be inspected upon delivery for compliance with DHS facility security protocols.

7.0 Warranty and Support

- Manufacturer’s warranty covering mechanical, electrical, and structural components.
- Contractor shall provide warranty documentation and user manuals.
- Contractor shall provide support for troubleshooting, replacement parts, and repairs.
- Optional extended warranty or service plan information shall be included.

8.0 Deliverables

- Fully assembled and operational adjustable-height workstations meeting all specifications.
- Documentation including:
    - User manuals
    - Warranty information
    - Power system specifications
    - Maintenance and safety guidance
- Final installation report confirming completion and functionality.

9.0 Performance Standards

- Workstations must meet all functional and safety requirements outlined in this PWS.
- Installation must be completed within the agreed performance period.
- All equipment must be free of defects and fully operational upon acceptance.