U.S. Citizenship and Immigration Services

Facility Security Specific Requirements

Office of Security and Integrity

in collaboration with

Office of Facilities Project Management Branch

November 2017

Version 4.0

Table of Contents

1.0 Purpose 3

2.0 Site Security 3

- **2.1 Illumination of Entrances, Exits, Parking Lots, and Garage Security:** 3
- **2.2 Visitor Access Control Parking:** 3
- **2.3 Application of Barriers:** 3
- **2.4 Authorized GOV Parking:** 3

3.0 Structure Security 4

- **3.1 Blast Resistance Windows:** 4
- **3.2 Security of Ventilation Equipment and Controls:** 4
- **3.3 Emergency Generators:** 4

4.0 Facility Entrance Security 4

- **4.1 Employee/Visitor Access Control** 4
- **4.2 Perimeter Doors and Door Locks** 4
- **4.3 Hydraulic Door Closers (HDC):** 5
- **4.4 Electric Door Strike (ES) Specifications:** 5
- **4.5 High Security Magnetic Locksets** 5
- **4.6 Emergency Exit Doors/Delayed Egress:** 6
- **4.7 Door Hardware Schedule:** 6

5.0 Security Systems 6

- **5.1 ESS Network Infrastructure Requirements** 6
- **5.2 Access Control Systems (ACS)** 12
- **5.3 Intrusion Detection Systems (IDS)** 16
- **5.4 Internet Protocol Video Surveillance Systems (IPVSS):** 18

1.0 Purpose

The purpose of this document is to provide the Lessor with the USCIS Security Requirements for hardware, software, devices, components and related items that are expected by the U.S. Citizenship and Immigration Services (USCIS).

This document includes general descriptions and specifications for security requirements for USCIS space. In conjunction with the GSA's Request for Lease Proposal (RLP), this document will assist the Lessor in understanding and developing the site specific security requirements and detailed costing required for the offered space.

The intentions of this document are the following:

- Accommodate the functional requirements of present and future security systems.
- Support a multi-product and multi-vendor environment
- Facilitate the planning and installation of security systems that will support the diverse needs of various building locations.
- Ensure uniformity and consistency in the security measures provided in all USCIS facilities.

2.0 Site Security

2.1 Illumination of Entrances, Exits, Parking Lots, and Garage Security:

The type of lighting and positioning selected will not impede the visibility/quality of video surveillance cameras.

2.2 Visitor Access Control Parking:

Visitor parking will be clearly defined using visitor signs. If adjacent building parking is provided, it will be reserved for disabled parking and Government parking. (See 2.4).

2.3 Application of Barriers:

If applicable, barriers will be required as part of the Preliminary Facility Security Level (FSL) determination by USCIS Office of Security and Integrity. Barriers used will be K-4 rated or higher. Barriers can be bollards, planters, drop arm gates or combination thereof. Barrier installation will be in accordance with manufacturer's specification. Decorative sleeves, soil, plants etc. will be included to maintain aesthetics and as to not detract from neighboring areas.

2.4 Authorized GOV Parking:

If adjacent building parking is provided, a section of this area will be reserved for Government Official Vehicles (GOV) parking only. GOV areas will be clearly defined using "Reserved" signs. GOV's parking will be well illuminated and covered by video surveillance.

3.0 Structure Security

3.1 Blast Resistance Windows:

All USCIS space exterior windows will have fragmentation film applied in accordance the GSA RLP.

3.2 Security of Ventilation Equipment and Controls:

All access to HVAC equipment that provides fresh air to USCIS spaces is to be secured from unauthorized access.

3.3 Emergency Generators:

If generator is required, emergency generators will be fenced within a secured access gate. Bollards will be positioned to reduce damage from vehicles. Electronic Security Systems shall be tied to generator for continued power.

4.0 Facility Entrance Security

4.1 Employee/Visitor Access Control

Magnetometers and X-rays - The government will procure and maintain magnetometers and X-rays.

Guards - The government will procure and post armed guards. The number of guards will depend on a guard survey conducted by local the Field Security Manager.

4.2 Perimeter Doors and Door Locks

Key Controls and Access Media - The lessor will use construction cores to secure required space during construction. Construction cores are required on exterior doors to secure the site until acceptance of the facility. Upon substantial completion and acceptance of the space, the locksmith (under supervision of a designated USCIS representative) will change out construction cores and install all permanent cores. At no time will the locksmith be in possession of the keys for the permanent cores. GSA will receive, sign for and turn over to USCIS the permanent core keys.

Mechanical Lock Specifications - Locksets will be installed on all non-passage set doors as follows:

- Storeroom function locks and hardware are required for all doors receiving card readers. These locksets/hardware have a lever on both sides, but the outside is stationary and cannot be moved. From the outside, the door latch is operated with a key. On the inside, simply engaging the lever will retract the latch. (For doors with panic hardware and/or magnetic locksets, see section 4.5 of this document.)
- Lockset will be high security, tamper resistant, commercial grade mortise lockset with storeroom function lock.
- Lockset will be on master key system.

- The contractor will provide and install a wall mounted organized lockable key box to accommodate all required keys to USCIS space.
- Lockset will be 6 pin cores.
- Locksets will be interchangeable cores and contractor will provide core removal key.
- A key plan developed with coordination from USCIS displaying key cut codes, pin codes, key numbers and their corresponding door access will be provided by the contractor. (The number of keys required will be determined during the key plan development.)
- A knox box may be required by local code or by USCIS guidance to secure an access device, i.e., key or access card, to expedite Fire Department entry. If required, a tamper switch alarm will be installed.

4.3 Hydraulic Door Closers (HDC):

Door closer will be commercial/industrial grade.

Door closing hardware is required for all doors with card reader equipment installed.

4.4 Electric Door Strike (ES) Specifications:

Commercial grade strikes are required.

Electric Door Strikes will be installed on doors with card readers.

Electric Door Strikes will be set at Fail Secure.

Electric door strikes will be powered by dedicated DC power in accordance with manufacturer's specifications.

4.5 High Security Magnetic Locksets

Only use magnetic locksets on double doors that are glass, with or without framing, and do not have astragal (center piece). The use of electrified vertical rods is not acceptable.

Locks will be mounted/installed in accordance with security industry standard as well as federal, state, local, and ADA laws.

Locks will be powered with dedicated DC power.

A push button request to exit button or touch sensitive panic bar with built-in request to exit will be installed on the egress side to deactivate the magnetic field for exit. Request to Exit (REX) device will be dependent on the door type and location.

Magnetic locking devices without built-in suppression and/or magnetic locking devices that draw large amounts of current (typically older models or defective devices) shall be installed utilizing external isolation relay(s) to protect the system from the transients these magnetic locking devices can generate, to ensure reliable operation.

Battery uninterrupted power supply will be supplied and support 4 hours.

For Main Entrance visitor doors, a toggle switch accessible on interior above door will be provided to disable magnetic locks during business hours.

Doors equipped with magnetic locksets will also have mechanical vertical locksets that can be actuated with panic hardware, locked in open position by locking down panic bar with hex key and either secured or unlocked using a mechanical lockset and key from exterior. (See mechanical lockset requirements)

4.6 Emergency Exit Doors/Delayed Egress:

Delayed egress will function in accordance with local fire and safety codes. The delay will be set on a timer, time determined by local fire codes. The panic hardware will prevent exit until the timer releases the lockset. The opening of the door will annunciate an audible local alarm that can only be reset by key. Key for alarm will be provided to USCIS.

High Rise Specific Requirements

International Building Code 2014 requires that all emergency egress doors to stairwells require that the doors fail safe in the event of a fire alarm activation or power outage. If this requirement applies, additional alarm points (motion sensors, glass break detectors, and door contact points) will be required to protect sensitive areas.

4.7 Door Hardware Schedule:

Door hardware for all doors will be listed in the USCIS Specific Requirements.

5.0 Security Systems

The Lessor will furnish and install an operational Electronic Security System (ESS). This requires the three (3) components of the ESS: Access Control System (ACS), Intrusion Detection System (IDS), Internet Protocol Video Surveillance System (IPVSS) that will be capable of operating on an integrated standalone platform which can provide USCIS with the ability access, monitor, administer and control of all three systems through a single client.

5.1 ESS Network Infrastructure Requirements

Server/Rack/KMM/Power:

Lessor shall supply system server which exceeds minimum server build specs of USCIS standard. The servers shall be a Dell PowerEdge R730. Servers will be rack mountable and located in LAN room. Server shall be provided by Lessor according to the model number and build specifications contained in Attachment 2.The servers will come preconfigured with Gallagher software for operating and managing the ACS as required; including Gallagher Command Center software, Credential Registration Engine, and certification validation software for ACS as required.

a. The specifications include the following:
   i. Redundant power supply.
   ii. Independent remote management processor.
   iii. Rails for rack installation.
   iv. Hard drives replaced under warranty will not be returned to the vendor; the Government will destroy or dispose of these based on the sensitivity level of the system which they are removed.
   v. Operating Systems shall be Windows Server 2012 R2.

KMM Switch:

A Dell™ 1U rackmount LED console model number: FPM185 is required and will be mounted in the rack.

Rack Specifications:

The rack will be a full 4 post APC NetShelter, 42U cabinet or equivalent with lockable doors for the security equipment along with grounding to meet manufacturer's requirements.

Workstations (WS):

Security Installer shall supply system workstations which exceed minimum server build Specs of USCIS standard, and Workstation OS shall be Windows 7 Enterprise.

The Security Installer shall provide two workstations used for this project as follows:

a. One workstation (PIV Provisioning WS) will be installed in the security office for administrative management of the systems. Manufacturer part number 50-1302 Dell Optiplex 7040 with Morpho USB Enrolment Reader, Cherry keyboard/reader, Gallagher native Credential Registration Engine Client software installed, 240-watt power supply, 128-GB Sata class 20 SSD hard drive, Windows 7 Pro, and one USB mouse. Provide a Dell U2412M HD 30" Monitor; manufacturer part number 415-40-U2412M for PIV Provisioning WS. This Workstation shall be able to view camera video and burn video to a DVD Disk.

b. One workstation (Guard WS) will be located at the guard station for camera and visitor management. Manufacturer part number 50-40-Optiplus Dell Precision Tower, 256-GB Sata class 20 SSD, Dual AMD Fire Pro W5100 4-GB video cards, Windows 7 Pro, and one USB mouse. Provide two (2) Dell U2412M HD 30-inch monitors; manufacturer part number 415-40-U2913WM for the Guard WS.

c. General Equipment Specifications purchased separately from Workstations:

   i. An 8 outlet Surge Protector and battery backup workstation unit for each workstation.

   ii. One video joystick controller (Guard WS only) for controlling Pan Tilt Zoom camera functions and other viewing functions.

Cabling:

a. Each Gallagher 6000 HI SPEC PIV Controller shall receive two CAT6A network cables to be terminated between the onboard dual Ethernet ports of the 6000 and the network switch for redundancy.
b. Install and terminate the required Category 6A horizontal plenum cables (gray color) on a 24- or 48-port performance-compliant Cat 6A – 1U or 2U patch panel in each USCIS Main Distribution Frame (MDF) / Computer Room in the designated cabinet provided by the security vendor. Coordinate with IT on the designated location within the MDF / Computer Room as noted on the provided layout drawing within the space.
c. Provided manufacturer specific Category 6A patch cables that shall be used for cross-connect from network switch to the 24- or 48-port patch panel ports and at the device location with the required lengths.

d. All plenum horizontal cabling routed through ceiling space that are not supported in wire mesh, basket style tray will be supported by J-hooks staggered approximately within 4 feet on center (maximum distance of 5-foot spacing).
e. Category 6A horizontal cables shall be labeled with the designated cable number at the termination points at the backside of patch panel in the corresponding closet and the surface box at the drop location (mounted inside the provided lockable security enclosure).
f. Machine-printed labels are mandatory, and hand written or permanent marker is not acceptable. Labeling is also required for the front of the patch panels and 1-port surface boxes with identification.
g. Tie wraps shall not be used. USCIS will only accept Velcro.
h. Terminate Category 6A horizontal cables on patch panels and modular connectors/jacks in surface mount housings to meet manufacturer's requirements. (Do NOT allow pairs to untwist, and outer jacket should only be ½ inch from termination point).
i. Route cables from both sides of equipment rack when terminating on patch panels with separation down center of rack, and use wire management, supporting bars, etc.
j. (Category 6A plenum CMP, cable specification or equivalent: Berk-Tek LANMARK 10G2 part # 10137183 or equiv. (gray color), Cat 6A Leviton patch panels # 6A586-U24 or equiv. or # 6A586-U48 or equiv., Cat 6A gray jacks with shutter – Leviton # 6AUJK-SG6 or equiv., surface mounting housing, 2-port box assembly Leviton # 4S089-1IP or equiv., and 3-foot gray Leviton # 6AS10-03S patch cables or equiv.)
k. A composite plenum-CMP rated access control cable is required for each door location. Cable shall be Belden Part Number 638AFS composite for lock power, card reader, door contact, and request to exit. Cable will consist of banana peel plenum with the following conductors: 4-16 AWG stranded conductors, 3-18 AWG pairs, 4-18 AWG stranded conductors, and 2-18 AWG stranded conductors.
l. Security Installer shall provide and install to provide necessary connections and power sources to the reader, lock, door position switch, and request to exit throughout the facility.
m. Power sources to the reader, lock, and other door devices throughout the facility will originate from the MDF / Computer Room where the security cabinet and components will reside. Power supplies or 120-volt (V) electrical outlets shall NOT be located above door locations for design.
***NOTE** : All cabling shall be installed according to the Gallagher Technical Reference Manual and shall follow all USCIS cabling standards as defined herein. Any conflict between Gallagher TRM and USCIS standards shall be brought to the attention of COTR for final determination prior to installation. Power requirements must be calculated by Security Installer. Proper cable gauge shall be selected based on reader distance from 6000 controller and must be calculated using appropriate load calculations provided by the PACS*

manufacturer. Discrepancies between specified cable and power requirements shall be brought to the attention of USCIS PM.

n. Separation must be maintained with a minimum of 2 inches between the IT cable plant installation (All Cat 6A and Cat 6 cables) and the security multi-conductor cabling (for power, signal, etc. (e.g., AWG 18/6, 22/2) throughout the facility. The Cat 6A cable for security may route with IT cable plant, which is Cat 6 – gray color, within the basket tray system.

o. The security multi-conductor cables may be routed within the same basket tray if the sizing accommodates, but must maintain the minimum of 2 inches of separation and be coordinated with the IT cabling contractor, with the IT cable plant installation taking precedence.

p. All multi-conductor security cables for the system must also be installed in separate supporting hardware (j-hooks) and upon exiting the basket tray system as well. All security cabling shall be CMP plenum-rated for all applications with the exception of cabling completely routed in rigid metallic raceway, EMT.

q. The Cat 6A – IT cabling shall NOT be routed within the same conduit as multi-conductor security cables used for power, signal, etc. If shielded, multi-conductor security cables and bundled assemblies must be bonded to meet NEC requirements accordingly. Refer to the USCIS Structured Cable Plant Standard, V2.2, March 2016 to meet the requirements for the IT and security cable installation.

USCIS Cable and Labeling Standards, Requirements, and Guidelines:

a. USCIS strictly adheres to the following standards. No deviations will be accepted.

b. Cat 6A shielded cable will not be accepted.

c. A Fluke Level 5 or higher cable tester must be used to certify the complete cable plant installation. Permanent Link Test required for Category 6A certification. Fluke Linkware format (.flw) required for technical deliverables package.

d. The manufacturer of the conductivity/termination hardware is responsible for supporting the single-source warranty of the complete cable plant installation. The selected contractor is required to be a certified installer with trained technicians of the proposedmanufacturer's product. The proposed cable plant solution must meet the minimum 15-year application assurance warranty to include product, cable, etc. and labor for the provided installation.

e. Each of the Category 6A horizontal cables shall be labeled with the designated cable number at the termination points located at the backside of patch panel in thecorresponding closet and at the drop location on the single port box. Machine-printed labels are mandatory, and hand-written or permanent marker is not acceptable. Labeling is also required for the front of the patch panels and faceplates, which will also be provided for identification.

f. Terminate Category 6 horizontal cables on patch panels and modular outlets to meet manufacturer's requirements. (Do NOT allow pairs to untwist, and outer jacket should only be a ½ inch from termination point). Route cables from both sides of equipment rack when terminating on patch panels with separation down center of rack, and use wire management, supporting bars, etc.

Cable labeling requirements:

a. All cables must be machine labeled; no hand-written labels will be accepted.
b. USCIS naming conventions shall be followed. Alternative naming conventions will not be accepted.
c. These naming conventions shall be used throughout the system architecture, reflected on submittals and as-built documentation, and when programming or configuring Gallagher Command Center database objects.
d. Security Installer is required to label each cable at the back of the patch panel and as close as possible to the terminating point in the controller. Labels shall also be placed at each end of each device. Additionally, all controller Ethernet connection are required to be labeled at each end of the device location and at the front of patch cable. All Cat6A cables shall meet the following standards and naming conventions:

i. Controller to Network

- Cat 6A cable-Patch Panel to Gallagher 6000-PIV controller: Each 6000 controller shall have two Ethernet cables terminated between controller and the patch panel to provide redundant communications between the controller and the production network. The following naming convention shall be used for all controller-to-network or controller-to-patch-panel connections.
- Three-letter building identification-the floor number that the wire closet is located on- the wire closet and type (MDF, TR1,TR2) – security panel number – Ethernet connection A (primary), B (secondary).

  ❖ Examples:
    - Panel 1 cable A Example: COH-2-MDF-1A
    - Panel 1 cable B Example: COH-2-MDF-1B
    - Panel 2 cable A Example: COH-2-MDF-2A
    - Panel 2 Cable B example: COH-2-MDF-2B

ii. Patch Panel to PTZ Camera (PTZ)

- Mounted in single port box- Cat 6A cable.
- Three-letter building identification-the floor number that the wire closet is located on- the wire closet and type (MDF, TR1,TR2) – PTZ camera number.

  ❖ Examples:
    - PTZ camera #1, wired to TR1 closet, 4th floor example: COH-4-TR1-PTZ1.
    - PTZ camera #3, wired to MDF closet, 2nd floor example: COH-2-MDF-PTZ3.

iii. Patch Panel to Fixed Camera (FC)

- Mounted in single port box – Cat 6A cable.
- Three-letter building identification-the floor number that the wire closet is located on – the wire closet and type (MDF, TR1,TR2) – FC Camera number.

  - Examples:
    - FC camera #1, wired to TR1 closet, 4th floor example: COH-4-TR1-FC1.
    - FC camera #3, wired to MDF closet, 2nd floor example: COH-2-MDF-FC3

iv. Security Controller to Each Door

- Specialty cable (as specified in technical requirements)
- Three-letter building identification-floor the wire closet is located on – the wire closet and type (MDF, TR1,TR2) – security panel# –cable number.

  - Examples:
    - Door #1, wired to security controller #1, located in MDF
    - closet, 4th floor example: COH-4-MDF-SC1-1.
    - Door #9, wired to security controller #2, located in MDF
    - closet, 4th floor example: COH-4-MDF-SC2-9.

v. Patch panel to Aiphone (AP)

- Mounted in single port box – Cat 6A cable.
- Three-letter building identification – floor the wire closet is located on-the wire closet and type (MDF, TR1,TR2) – AP camera number.

  - Examples:
    - Aiphone #1, wired to TR1 closet, 4th floor example: COH-4-TR1-AI1.
    - Aiphone #3, wired to MDF closet, 2nd floor example: COH-2-MDF-AI3

vi. Remaining Cables All remaining cables that are not required to be punched down to the patch panel (e.g., those terminating at a field sensor or device such as motion detectors, request to exit, keypads, glass breaks, door contacts, etc.) require the use of a combination of an agreed-upon abbreviation and the number the cable. USCIS will require machine-generated labeling on both ends of the cable.

  - Examples:
    - Glass Break: GB1,GB2,GB3,GB4,GB5
    - Key Pad: KP1,KP2,KP3,

- Door Contact: DC1,DC2,DC3,DC4
- Motion Detector: MD1,MD2,MD3,MD4

Network Switches:

1. The ESS infrastructure requires Cisco Catalyst 3850-X Series Power over Ethernet (PoE) switches.
2. The port security on the Cisco switches and those they interconnect with cannot be extended to other vendor switches.
3. Contractor will configure devices using USCIS provided IP addresses.
4. Switches will be mounted in security rack located in the USCIS LAN room and wire closets.
5. Contractor will supply enough switches to provide ports for all cameras, panels, intercom devices, servers and workstations. Note: Switches will be required on each floor for vertical connectivity to head end.

Battery Backup/Power Supplies:

1. Controller and UPS enclosures shall be ordered from Gallagher, referencing the acceptable part numbers listed below. Enclosure shall include power supply and UPS battery backup system which shall be wall mountable Life Safety Power units able to monitor the health status of power supply and batteries.

    a. C305720, LSP E2 Cabinet, 6A PSU (Third-Party Product)
    b. C305721, LSP E4 Cabinet, 12A PSU (Third-Party Product)
    c. C305740, LSP B100 Secondary Voltage Module
    d. C305741, LSP C8 Lock Controller Module, 8 Output
    e. C305742, LSP NL2 Power Netlink Module

2. Battery backup shall support all devices connected for the times noted below for each system.
3. The system shall include UPS backup power with low-voltage power supply monitoring and alarm notification for the following.

    a. Monitor health and status of host power supply and battery set
    b. Auto-schedule or manual test and report battery standby time
    c. Remote supervision of battery's state of charge
    d. Remote monitoring and alert of external temperature fluctuations
    e. Monitoring of internal cabinet temperature Remote power cycling control of external equipment
    f. Time / date stamp system log reports of last 1,000 events
    g. Security Installer shall supply power, UPS, and load calculations to the USCIS PM prior to commencing installation.

5.2 Physical Access Control Systems (PACS)

PACS Specifications:

The following specifications provide functional, technical, and operational requirements for the Gallagher Command Center PIV PACS.

1. The ACS system will be Gallagher PIV ACS. The system will have GSA E-PACS certification using 13.01 topology.

    a. PIV Command Centre (APL Listing 10019)
    b. PIV PACS Validation (APL Listing 10020)
    c. T10 PIV Reader (APL Listing 10021)
    d. T11 PIV Reader (APL Listing 10022)
    e. T11 PIV Reader MultiTech (APL Listing 10023)
    f. T15 PIV Reader (APL Listing 10101)
    g. T15 PIV Reader MultiTech (APL Listing 10102)
    h. T20 PIV Reader (APL Listing 10038)
    i. T20 PIV Reader MultiTech(APL Listing 10039)
    j. T21 PIV Reader (APL Listing 10099)
    k. T21 PIV Reader MultiTech(APL Listing 10100)

2. The Security Installer must be certified by the manufacturer for the security system and will provide the certification to USCIS. GSA will ensure that the Security Installer selected is an HSPD-12 certified provider.
3. Standardized naming conventions: Security Installer shall follow all government provided naming conventions and standardized nomenclature when performing system configuration and database programming. Naming conventions will be provided to Security Installer by the Government prior to Security Installer commencing these activities.
4. Database and event storage capacities may vary based upon the system configuration. The ACS shall be capable of storing a minimum of one million records of system activity.
5. Records management on the ACS database shall automatically truncate or “roll-over” when the maximum record capacity has been reached so that space is always available to save the most recent transaction data in the system.
6. Security Installer is to install in accordance with ALL manufacturer's current specifications for installations, along with having all up-to-date manufactures installations guides and specifications prior to install.
7. The Security Installer will provide to GSA/USCIS shop drawings, product data, material list, and/or cut sheets on all devices, systems, and/or components that are to be provided under these requirements. USCIS will review and provide comments on provided information.
8. The Security Installer will pay close attention to the USCIS specific requirements for each room and/or space within the USCIS-controlled space.
9. If applicable, intercoms for remote access into parking areas and/or common entrances not staffed by USCIS guards will be required.
10. The Lessor is responsible for the required coordination between the installer of the ACS system, all door hardware, electrical power requirements, and all other trades involved in the project.

11. The Security Installer will provide enough battery backup power to support 90 minutes of continuous power to ACS in case of power loss.
12. All wiring, terminations, power, and grounding installations must be performed in accordance with and consistent with current manufacturer component installation diagrams and recommendations.
13. PoE will NOT be utilized as a power source for the access control system.

PACS Summary:

1. The PACS shall provide FIPS 201-2 – compliant access control functionality and shall have the capability of being integrated with video surveillance (i.e., IPVSS requirements below), intrusion detection, building automation systems, fire alarm system, lighting controls, elevators, and other perimeter security countermeasures and systems where applicable.
2. The PACS shall consist of an end-to-end solution listed on the FIPS 201-2 / FICAM Testing Program Approved Products List.
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. Installers/integrators shall use existing PACS cabling infrastructure where such cabling conforms to current Institute of Electrical and Electronics Engineers / Building Component Safety Information standards, passes current applicable industry standard testing, and sufficiently supports the needs of the system.

    a. Monitoring: The solution shall provide uninterrupted (24x7x365) monitoring of the PACS devices.
    b. Availability: The solution must have a demonstrated availability of 99%, over the past three years of service from the date of submission of the proposal.
    c. The primary system must be internally redundant so that there is no single point of failure within the system.
    d. The primary system shall remain fully functional while being upgraded or backed up.
    e. Disaster Recovery: The architecture must 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 must occur immediately and seamlessly for either manmade or natural disaster. Should the events be precipitated by technical issues, a decision to failover and recommence synchronization must be made and implemented within 90 minutes from the time of the occurrence.
    f. Open Architecture: The central PACS applications shall be capable of supporting multiple security manufacturers' on-premise control panels, edge devices, cameras, sensors, etc. through a published API.
    g. Must appear on the FIPS 201-2 / FICAM Testing Program APL as an end-to end PACS solution. Security Installer's solution may be in testing by

the Program. Security Installer shall not be allowed to install the system until it is approved and listed on the APL.

5.2.1 General Description of Installation and Capabilites

All perimeter doors will use the Gallagher HBUS Terminal series keypad readers for the ability of dual-factor authentication after hours. Secondary doors (interior) will be installed with HBUS series PIV readers. Electronic locking hardware will be installed on all pedestrian door entrances with a card reader. All locking arrangements installed on any means of egress (i.e., the exit access, the exit, and exit discharge) door assembly or fire-rated door assembly must meet the requirements of the NFPA Life Safety Code and NFPA 80, Standard for Fire Doors and Other Opening Protectives (if applicable). In addition, preparation of fire door assemblies for locks, latches, hinges, remotely operated or remotely monitored hardware, etc. must be performed in accordance with the manufacturer's inspection service procedure and under label service (Annex E and Annex F of NFPA 80, Standard for Fire Doors and Other Opening Protectives).

Card Readers (CR):

1. CR with pin pads and LCD display will be installed on all USCIS doors as depicted on floor plans.
2. Gallagher T Series (T-21 PIV Multi-Tech) readers are required and will use FICAM and FIPS-201-2–compliant firmware able to read all federally issued PIV, CAC, FRAC, PIV-I, TWIC and CIV cards. Readers for project shall be all by one manufacturer or the other, not a mixed batch at a single site. Configuration will allow for the cards to be read contactless at 13.56 MHZ or using the contact card read interface.
3. Card readers shall be surface mounted near door located in a position to meet federal,state, local and Americans with Disabilities Act (ACT) laws.
4. CR will indicate access granted when the access control system has released an electricstrike or magnetic locking device as applicable to allow access into the secured space.

Request to Exit Sensors (REX):

1. The ACS will utilize Passive Infrared (PIR) Request to Exit (REX) sensors to indicate an authorized exiting/opening of doors from egress side. REX devices are required on all doors receiving card readers.
2. These devices will provide notification of an authorized exit locally to the access control log and will not tie into the IDS.
3. Bosch DS160, Honeywell IS310, or equal required.
4. The sensor will be located on the egress side of the doors to detect an occupant approaching the door.
5. REX devices will not release electric strikes. Electric door strikes will solely be controlled by the access control system relays when an authorized card read is granted.
6. Push button REX devices or pressure sensitive REX panic hardware devices are required for doors with Magnetic locksets.

Door Position Switches (DPS):

1. The vendor will provide and install magnetic mounted door position switches to monitor all card reader controlled doors. (Exception: Doors required to have a high security Balanced Magnetic Switch (BMS) that are equipped with two outputs.)
2. Sentrol 1078 or equal is required.
3. Door position switches will monitor for door propping, forced door alarms, and open or closed status. This monitoring is to be leveraged locally using the ACS client workstation.

5.3 Intrusion Detection Systems (IDS)

IDS Requirements:

1. IDS is required for all perimeter access, ground floor windows , and any other windows with direct access from adjacent rooftops, and roof hatches into USCIS space. IDS will include Federal Protective Services (FPS) Mega-Center approved alarm panels, passive infrared (PIR) dual technology sensors, balance magnetic switches, duress alarms, glass break sensors, dual technology motion detection sensors and tamper alarms (panel and sensors). The IDS keypad(s) (arm/disarm control) must also be located near the entrance employees utilize.

2. All sensors will be individually zoned in such a way that the alarm location can be easily located through the use of simple zone maps by responding forces. The daisy chaining of sensors, alarms or zones is prohibited for this reason.

3. Zoning needs to be established that allows individual areas to be disarmed for afterhours use, i.e. the interior alarms could be disarmed for afterhours use but the perimeter alarms would remain armed. Zoning requirements will be determined by FPS Mega-Center.

4. Alarm messaging language will meet the FPS Mega-Center Monitoring Station requirements.

5. Lessor will provide enough battery backup power to support 4 hours of continuous power to intrusion detection equipment in the event of power loss.

IDS Panel (IDSP):

1. The IDS Panel will be connected to the FPS Mega-Center servicing the area for alarm monitoring **via an analog "POTS" (Plain Old Telephone System) land line**. The Lessor will be responsible for providing the analog telephone line (POTS) for the required communication to the Government's alarm answering service. The Lessor will pay for and maintain this line for the term of the lease.
2. Connection to the Mega-Center requires the use of panels from the following manufacturers; Bosch (Model: D9412G-V4) or Digital Monitoring Products (DMP) XR500 Alarm Panel. Models need to be verified with the Mega-Center due changes in technology.

3. Mega-Center Alarm Requirements (MAR) Request Form is required to be completed and approved by FPS prior to connecting. Portions of the MAR are required to be completed by the lessor, security vendor and will be coordinated with USCIS.
4. Alarm systems will be configured for manual arming/disarming unless otherwise specified by USCIS.

High Security Balanced Magnetic Switches (BMS):

1. To be installed on all doors leading into USCIS space from outside or doors leading from common shared tenant space areas.
2. Harco Magnasphere HSS L2C or equal required.
3. BMS will act as an alarm to the IDS when armed and provide door status notifications to ACS.
4. Switches will be housed in weatherproof enclosures when exposed to outside elements.
5. Switches will have a tamper alarm notification.
6. Surface mounted switches may be used at the approval of USCIS.

Acoustic Glass Break (GB) Sensors:

1. All glass on the ground floor will be in the coverage area of a glass break sensor. All sensors will be acoustic detection devices). Once the glass break detects the acoustic activity, it will send a signal to the alarm panel.
2. Glass break sensors will be commercial grade and be equipped false alarm reduction technology.
3. Glass break sensors will be ceiling mounted devices.
4. Contractor will provide a glass break testing device matching devices installed.
5. Glass break sensors will provide detection of plate, safety, laminated, and tempered glass breakage.

Dual Technology Motion Sensors (MS):

1. Motion sensors will cover main hallways leading to exterior exits. Dual technology consists of PIR and microwave detection technology integrated into a single enclosure.
2. The Rokonet directional and 360 series or equal required.
3. Motion sensor will be on different microwave frequencies when positioned in same area.
4. Motion sensors will not be mounted on or near pipes, steel girders, or HVAC systems as doing so may result in nuisance alarms. Fans, venetian blinds, open windows may also produce false alarms.
5. Optional: 360 degree ceiling mounted dual technology motion sensors may be used for large areas or where the use of directional sensors are not feasible.

Hardwire Duress Alarm Button (DB):

1. Duress alarms are for use in public facing facilities at guard stations, Field Office Director (FOD) Office, District Director (DD) Office, and information counters. Information counters, FOD and DD duress alarms will annunciate to the USCIS guard visitor screening station. Duress alarms shall annunciate at the guards desk via

audible and visual notification. The guard visitor screening station duress button will annunciate to the Mega-Center. If the facility does not have guard service, all duress alarms will annunciate to the Mega-Center. All other offices have the ability to call guard desk through 911 services and speed dial.

2. Duress alarms will be desk mounted, recessed, and out of sight from the general public, visitors, and customers. The duress alarm will be positioned within arm's reach of the user when seated at their respective desk/stations.
3. Duress alarms will lock-in alarm mode until manually reset by key or similar device.
4. Duress alarm annunciations will be distinguishable from other alarm sensors.

Alarm Keypad (KP):

1. A Bosch D1260B keypad or equivalent shall be used. Keypads will be mounted inside secured space near main entrances, employee entrances and guards desk. Keypads are to be located in a position to meet federal, state, local, and ADA laws. The alarm delay will be set at minimum 30 seconds and maximum of 60 seconds. Keypad alarms locations will be clearly indicated on construction documents. Quantity of keypads will depend on number of partitions, floors, zones, etc.

5.4 Internet Protocol Video Surveillance Systems (IPVSS):

IPVSS Requirements:

1. Video system shall be based on Milestone Video System with Axis cameras. Lessor shall verify that all video components are compatible with current version of Gallagher Command Center and shall provide all necessary integration licenses to provide full interoperability between PACS and IPVSS.
2. The IPVSS system coverage is required to provide complete 360 degree coverage and quality video coverage of all exterior perimeters controlled by USCIS, visitor and employee entrances into USCIS space, security screening areas, waiting areas, naturalization ceremony rooms and information counters.
3. Lessor will provide enough battery backup power to support 90 minutes of continuous power to IPVSS in the event of power loss.
4. The determination of fixed cameras, pan/tilt/zoom (PTZ) cameras, wall and ceiling, and how many cameras are adequate will be determined in coordination with representatives of the Office of Security and Integrity (OSI), Physical Security Section (FSS).

Fixed Wall Mounted IP Cameras (FC):

1. Fixed cameras will be positioned to view activities at the loading dock, guard screening areas, lobbies, waiting room information counters, entrance doors, and coverage of the exterior of the building/parking areas.
2. Exposed camera wires should be covered by flex conduit or installed in a neck mount system to deter tampering.
3. All exterior camera housings must be weather resistant and capable of operating in extreme hot/cold environments as well as high and low humidity environments.
4. Cameras will be pointed at an angle pointed downward providing a field of vision to satisfy the area to be protected.
5. Camera will be equipped with Infrared Illuminators allowing viewing out to a minimum 35 feet with built in light sensor.

6. Camera will be true day/night utilizing an automatic infrared (IR) cut filter to switch between color and black/white modes when environmental lighting conditions change and the need for infrared sensitivity is required.
7. Optical lens must be varifocal with auto iris for focusing. (Coordinate with the USCIS to determine the appropriate varifocal lens for each camera.)
8. Cameras will be high definition at 1080P.
9. Camera will be Microsoft Windows compatible.
10. Camera will be powered by Power over Ethernet (PoE).
11. Camera will be equipped with motion detection for motion detected recording.

Pan/Tilt/Zoom (PTZ) Cameras:

1. For use as corner roof mounted. These cameras are used to supplement fixed cameras.
2. All exterior camera housings must be weather resistant and capable of operating in extreme hot/cold environments as well as high and low humidity environments. Cameras will be mounted parapet style mounts with swing-in arms for maintenance/repairs to camera from roof access. Cameras will hang out and above corner of facility to allow an unimpeded 360 degree view.
3. Camera will be equipped with Infrared Illuminators that allow viewing out to the maximum optical zoom capability of the camera. Note: Optical zoom distances will be based on the distance needed to accurately identify the size, and shape of an object, as well as general facial features of an intruder on the premises covered by the camera.
4. Camera will be true day/night utilizing an automatic infrared (IR) cut filter to switch between color and black/white modes when environmental lighting conditions change and the need for infrared sensitivity is required.
5. Cameras will be high definition 1080P.
6. Camera will be high resolution up to maximum effective optical zoom range.
7. Camera will be Microsoft Windows compatible.
8. Camera will be powered by dedicated AC/DC.
9. Camera will be equipped with motion detection for motion detected recording.

Network Video Recorder (NVR):

1. The NVR is for local IP IPVSS recording. NVR will be rack mountable and located in LAN room.
2. NVR will have the capacity to record at high quality for 60 days of recording of all cameras with a minimum of 10 Terabytes of storage capacity. The use of motion activated recording is required to reduce storage capacity while still meeting the 60 day requirement. Note: NVR will overwrite video stored by oldest date automatically once it has reached capacity.
3. NVR will allow playback by choosing date and time and must auto adjust for daylight savings time changes.
4. NVR will support the amount of cameras on the system using IP based Ethernet (RJ45) connections.
5. NVR will be Microsoft Windows compatible.
6. NVR will be capable of recording up to 1920x1080 resolutions with a 1280x720 resolution at 30 frames per second.
7. NVR video compression will be MPEG-4.
8. NVR will be capable of alarm triggered camera action.
9. NVR will allow for export to DVD.
10. NVR will support remote management and configuration.

11. NVR will support activity log.
12. Functions will include alarm outputs, time/date stamps, motion detection, management software, manage color/black and white cameras, and allow operation in duplex mode.
13. NVR will produce footage copies with watermarks or security stamps to prevent tampering and/or manipulation.

IP Audio/Video Intercoms:

1. Audio/visual intercom transmitters (AVT) will be located at mail rooms and loading dock area and capable of remote door release. Audio/visual receivers (AVR) will be located at guard station and/or the mission support area.
2. Intercoms will allow for electric remote door release controlled at receiver station.
3. Aiphone IS Series or equal required.
4. Intercoms will be a single integrated component consisting of a camera, speaker, and microphone on the transmitter end (customer side). It will also be equipped with hands-free and push-to-talk functions.
5. Camera will be a 170 degree wide angle field of vision.
6. Intercom transmitters exposed to outside elements will be in weather and tamper resistant housings.
7. Intercom transmitter will be positioned to allow for clear facial recognition.
8. Intercom receiver (monitoring end) component will be a standalone device system with viewing screen, remote door release function, hands-free and push-to-talk functions.
9. Intercom will integrate with electric strikes for remote release of doors it communicates with.
10. Intercom transmitter buttons will be labeled.
11. Intercom receiver buttons will be labeled to identify which transmitter it is communicating with and which door it is releasing.