SECURITY REQUIREMENTS - FACILITY SECURITY LEVEL II

THESE PARAGRAPHS CONTAIN ADDITIONAL SECURITY REQUIREMENTS, AND, UNLESS INDICATED OTHERWISE, ARE TO BE PRICED AS PART OF THE RENTAL RATE (SHELL) OR THE TENANT IMPROVEMENTS (TI).
NOTE THAT ITEMS IDENTIFIED AS "SHELL" REPRESENT A LESSOR'S OBLIGATIONS OR THE GOVERNMENT'S RIGHTS AND ARE NOT NECESSARILY ITEMS TO BE CONSTRUCTED.

DEFINITIONS:
Definitions are the same as those used in the Lease unless re-defined in these Security Requirements.

CRITICAL AREAS - The areas that house systems that if damaged or compromised could have significant adverse consequences for the facility, operation of the facility, or mission of the agency or its occupants and visitors. These areas may also be referred to as "limited access areas," "restricted areas," or "exclusionary zones." Critical areas do not necessarily have to be within Government-controlled space (e.g., generators, air handlers, electrical feeds which could be located outside Government-controlled space).

SENSITIVE AREAS – Sensitive areas include patient records and data, or any area that houses medical, mental, or other items or services that require patient privacy. Also included are police areas, pharmacy, medication rooms and OI&T spaces. Sensitive areas are primarily housed within Government controlled space.

DESIGN-BASIS THREAT – The Design-Basis Threat (DBT) is the profile and estimate of the threats to a government facility across a range of specific undesirable events and serves as the basis for determining appropriate security standards. The Lessor's technical consultant(s) shall work in conjunction with the VA to apply the DBT to the post-award risk assessment. The risk assessment identifies recommended countermeasures and security design features that achieve the minimum baseline level of protection (LOP) for a particular facility. The baseline level of protection may be further customized to address facility-specific conditions. The Lessor is responsible for providing countermeasure provisions outlined in this FSL document, as well as for additional items identified during the post-award risk assessment. Any additional countermeasures identified during this assessment shall be priced as BSAC.

ADDITIONAL INFORMATION ON THE INTERAGENCY SECURITY COMMITTEE (ISC) RISK MANAGEMENT PROCESS IS AVAILABLE HERE: https://www.dhs.gov/interagency-security-committee

Video Surveillance System (VSS), is widely used throughout industry and the federal government. It covers both analog and digital systems and is referenced in the Department of Homeland Security (DHS) Science and Technology Digital Video Quality Handbook.

1.0 SITE SECURITY CRITERIA

1.1 IDENTIFICATION AS FEDERAL FACILITY: (SHELL)

ISC LOP II: Signage identifying a facility as a federal facility shall be posted clearly and prominently to accommodate patient access in accordance with VA Signage Design Guide.

1.2 LANDSCAPING: (SHELL)

ISC LOP II: Minimize areas of concealment in and around facilities. Establish a clear zone around barriers or fences and restrict landscaping from obstructing views of the security force and VSS; or interfering with lighting or Intrusion Detection System (IDS).

1.3 PEDESTRIAN ACCESS TO SITE: (SHELL)

No special measures required.

1.4 VEHICLE ACCESS POINTS: (SHELL):

No special measures required.

1.5 SITE LIGHTING: (SHELL)

- ISC LOP III: Install exterior lighting at entrances, exits, parking lots, garages, VSS locations, and walkways from parking areas to entrances.
- All lighting design decisions should also support Crime Prevention Through Environmental Design (CPTED) goals and enhance environmental design factors (e.g., post-incident investigation, personnel identification, natural surveillance activities).
- Lighting should be sufficient to:
  - Illuminate potential areas of concealment.
  - Enhance the observation of security force patrols.
  - to ensure VSS video images can be used to identify a clear description of a person and any activity they may be engaged in; and
  - Provide for the safety of personnel moving between adjacent parking areas, streets, alleyways, and around the facility.
- For lighting assessment procedures and minimum lighting levels in other areas, refer to the Illuminating *Engineering Society (IES) Security Lighting Handbook G-1-03.*
- There should be no foliage blocking the light from illuminating the desired area.

1.6 RESTRICTED AREAS OR SIGNIFICANT AREAS AND ASSETS: (SHELL)

- ISC LOP II: Use trees, hedges, berms, or any combination of these elements to create buffer zones to separate public areas and other functions.
- Restricted areas or significant areas and assets include but are not limited to:
  - Utility connections.
  - Loading docks.
  - Emergency power supplies.
  - Hazardous materials storage.
  - HVAC and their intakes; and
  - Exterior access to critical or sensitive rooms (e.g., telecom and information technology (IT) resources).

1.7 SIGNAGE – SENSITIVE AREAS: (SHELL)

ISC LOP II: Lessor shall not post signs that identify sensitive areas, unless required by other standards/codes. Avoid marking outside locations such as air intakes, fuel supply valves, gas or power distribution locations, evacuation assembly areas, etc.

1.8 CONTROL OF PARKING: (SHELL)

Lessor shall designate VA employee and patient/visitor parking areas with signage.

1.9 AUTHORIZED PARKING: (SHELL)

No special measure required

1.10 VEHICLE ACCESS TO CONTROLLED PARKING: (SHELL)

No special measures required

1.11 VEHICLE BARRIERS: (SHELL)

- ISC LOP Level III: Provide vehicle barriers to protect pedestrian entrances from penetration by a vehicle meeting the DBT.
    - The type and size should be utilized to support the kinetic energy calculations < Kinetic Energy (KE) = 0.5 * Mass (m) Velocity (v)2 > necessary to determine the minimum crash rating necessary for protection. Practitioners should utilize locally developed threat information indicating a deviation from the DBT vehicle characteristics.
    - Reduce Straight Avenues of Approach for Vehicle Paths:
        - Use a vehicle velocity that considers the angle of incidence in conjunction with the distance between the perimeter and the point at which a vehicle likely would be able to start a run at the perimeter. Design site circulation to prevent high-speed approaches by vehicles and use barriers or offset vehicle entrances from the direction of a vehicle's approach to force a reduction in speed. Appropriate measures for the barrier system may include walls, fences, trenches, berms, ponds and water basins, boulders, plantings, trees, static barriers, sculptures, and street furniture.
    - Maximum clear spacing between vehicle barriers is four feet. Minimum barrier height is 30 inches. Agency standards may require additional height.
    - Barriers must be certified to meet performance requirements for vehicle size and speed specific to the facility under ASTM F 2656-18, Standard Test Method for Crash Testing of Vehicle Security Barriers,

1.12 VEHICLE SCREEENING:

No special measures required

1.13 PEDESTRIAN ACCESS TO CONTROLLED PARKING AREAS:

ISC LOP III (TI): Monitor pedestrian access to parking areas utilizing VSS.

1.14 HAZARDOUS MATERIALS (HAZMAT) STORAGE:

ISC LOP II (SHELL): Locate HAZMAT storage in a restricted area away from loading docks, entrances, and uncontrolled parking.

1.15 RECEPTACLE AND CONTAINER PLACEMENT:

ISC LOP II (SHELL): Position trash containers, mailboxes, donation/recycle containers, vending machines, etc., 25 feet away from building exterior and entry points, or implement blast containment measures to mitigate an explosion.

2.0 STRUCTURE SECURITY CRITERIA

For new construction projects and major rehabilitation projects over 100,000 GSF, a blast engineer with formal training in structural dynamics and demonstrated experience with accepted design practices for blast resistant design must be included as a member of the design team.

2.1 BLAST RESISTANCE-WINDOWS: (SHELL)

- ISC LOP III: Utilize acceptable fragment retention film or preferred glazing systems to reduce the glass fragmentation hazard for new lease construction. The acceptable fragment retention film is required when existing buildings are offered, and the windows are not replaced using the preferred glazing systems.
    - Acceptable Fragment Retention Film: In applications requiring retention film, film shall meet or exceed the following physical properties:
        - Film composite strength and elongation rate measured at a strain rate not exceeding 50% per minute shall not be less than the following:
        - Yield strength: 12,000 psi
        - Elongation at yield: 3%
        - Longitudinal tensile strength: 22,000 psi
        - Traverse tensile strength: 25,000 psi
        - Longitudinal elongation at break: 90%
        - Traverse elongation at break: 75%
        - Minimum 7-mil retention film
    - Preferred glazing systems include thermally tempered heat-strengthened or annealed glass with a fragment retention film installed on the interior surface and attached to the frame; or laminated thermally tempered, laminated heat-strengthened, or laminated annealed glass.
        - New glazing systems at the Low or higher LOPs shall be designed with a minimum ½-inch bite.
    - Unacceptable systems include untreated monolithic annealed or heat-strengthened glass and wire glass.
    - Reference the current DBT, unless device size is superseded by an agency-specific threat assessment. Device location is the closest possible point to the setback with the DBT device.

2.2 **BLAST RESISTANCE: FAÇADE AND STRUCTURE: (SHELL)**

ISC LOP II (SHELL):

New Lease Construction

Use construction materials which have inherent ductility, and which are better able to respond to load reversals (e.g., cast in place reinforced concrete column and steel construction).

- All building materials and types acceptable under model building codes are allowed. Design detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry to adequately respond to the design loads.
- **Unreinforced masonry is unacceptable**. Pre-stressed concrete is not very ductile and may not be appropriate where load reversals may occur.
- Reference the current ISC DBT, unless device size is superseded by an agency-specific threat assessment. Device location is the closest possible point to the setback with the DBT device.
- All building components requiring blast resistance must be designed using established methods and approaches for determining dynamic loads, structural detailing, and dynamic structural response. The demands on the structure will be equal to the combined effects of dead, live, and blast loads. Blast loads or dynamic rebound may occur in directions opposed to typical gravity loads. Design and analysis approaches should be consistent with Unified Facilities Criteria (UFC) 3-340-02, "Structures to Resist the Effects of Accidental Explosions, with Change 2." Response limits shall follow U.S. Army Corps of Engineers (USACE) PDC-TR 06-08, "Single Degree of Freedom Structural Response Limits for Antiterrorism Design."

Existing Facilities

- **Unreinforced masonry is unacceptable**. Pre-stressed concrete is not very ductile and may not be appropriate where load reversals may occur.

2.3 BLAST RESISTANCE: PROGRESSIVE COLLAPSE: (SHELL) *This section only applies to new lease construction.*

ISC LOP II: Use construction materials for structural framing system, which have inherent ductility and are able to respond to load reversals (e.g. cast-in-place reinforced concrete and steel construction).

2.4 BLAST RESISTANCE – UNDER BUILDING PARKING:

Under building parking is prohibited.

2.5 BURGLARY RESISTANCE OF WINDOWS AND GLASS DOORS: (TI)

ISC LOP II: All operable ground floor windows shall be locked and monitored via IDS.

2.6 WALLS AND NON-WINDOW OPENINGS:

ISC LOP II: Protect non-window openings such as mechanical vents and exposed plenums to resist forcible entry.

- Forced entry resistance will be uniform around the perimeter and the façade of the building.

- Interior walls of secure or restricted areas (IT Closets, Armory, Police Operations and Pharmacy) shall be monitored via IDS.

2.7 WINDOWS IN CTRICIAL AREAS- BALLISTIC PROTECTION:

ISC LOP II: No special measures required.

2.8 PROTECTION OF AIR INTAKES: (SHELL)

ISC LOP II: Provide emergency shutdown, SIP, and evacuation procedures. Secure accessible air intake grilles from tampering or removal.

2.9 ISOLATED VENTILATION SYSTEMS: (SHELL)

ISC LOP II: No special requirements

2.10 HVAC CONTROL: (SHELL)

ISC LOP II: Lessor shall develop written procedures for the emergency shut-down or exhaust of air handling systems.

- A "one-step shutoff" is a mechanism that requires only a single action by an individual (e.g., engineer or security personnel) to initiate the immediate shut down of all air handling equipment in the building.

2.11 CBR DETECTION TECHNOLOGY: (SHELL)

ISC LOP II: No special measures required.

2.12 BIOLOGICAL FILTRATION – GENERAL BUILDING: (SHELL)

ISC LOP II: No special measures required

2.13 BIOLOGICAL FILTRATION – LOBBIES AND MAILROOMS: (SHELL)

ISC LOP II: No special measures required.

2.14 CHEMICAL FILTRATION: (SHELL)

ISC LOP II: No special measures required.

2.15 SECURITY OF VENTILATION EQUIPMENT AND CONTROLS: (SHELL)

ISC LOP II: The lessor shall protect the system controls from unauthorized access.

- Access to government space shall be managed by installing compliant Physical Access Control in compliance with OMB policy M-05-24, NIST SP-800-116-1, and all other applicable standards established by OMB, NIST, and the OCIO Council.
- To ensure HVAC system operation cannot be disrupted by someone physically accessing the controls, HVAC equipment shall be located in a secure area with access limited to authorized staff.

2.16 LOCATION OF UTILITIES AND FEEDERS: (SHELL)

ISC LOP II: No special measures required.

2.17 SEPARATION OF EMERGENCY AND NORMAL POWER DISTRIBUTION: (SHELL)

ISC LOP II: No special measures required.

2.18 EMERGENCY GENERATOR PROTECTION: (SHELL)

ISC LOP III: New Construction: Generator shall be secured against unauthorized access and locate the emergency generator and fuel tank at least 25 feet away from loading docks, entrances, and parking, or implement standoff, hardening, and venting methods to protect utilities from the DBT at these locations.

- The generator shall not be located in any areas that are prone to flooding.

- More secure locations include the roof, protected grade level, and protected interior areas. VSS, electronic Physical Access Control, and IDS coverage shall be utilized (TI).
- Provisions for securing any refueling and shutoff valves in fuel lines within or in close proximity to the building must be addressed.

2.19 PROTECTION OF WATER SUPPLY: (SHELL)

ISC LOP III: Secure handles, control mechanisms, and service connections at onsite publicly accessible locations with locks or other anti-tamper devices.

2.20 BLAST RESISTANCE – INTERIOR PUBLIC SPACES:

Existing Construction: ISC LOP I: No special measures required.

New Construction: ISC LOP II: Use construction materials which have inherent ductility, and which are able to respond to load reversals.

2.21 BLAST RESISTANCE – MAIL SCREENING AND RECEIVING LOCATIONS:

Existing Construction: ISC LOP I: No special measures required.

New Construction: ISC LOP II: Use construction materials which have inherent ductility, and which are able to respond to load reversals.

3.0 FACILITY ENTRANCE SECURITY CRITERIA

If the leased Space is greater than 75% of the space in the building (based upon ABOA measurement), the requirements of FACILITY ENTRANCES AND LOBBY Section below shall apply to the entrance of the building. If the leased Space is less than or equal to 75% of the space in the building (based upon ABOA measurement), then the requirements of FACILITY ENTRANCES AND LOBBY Section below shall apply to the entrance of the leased Space.

3.1 BADGE IDENTIFICATION (ID) SYSTEM:

No special measures required of Lessor.

3.2 REGULATORY SIGNAGE:

ISC LOP II: Lessor shall post necessary regulatory, statutory, and/or site-specific signage per the VA Signage Design Guide.

3.3 EMPLOYEE ACCESS CONTROL: (SHELL)

ISC LOP II: Provide a means to secure employee entrance doors and to verify the identity of persons requesting access prior to allowing entry in the facility by physical or electronic means.

- When it is determined an electronic Physical Access Control System (ePACS) is to be installed, procurement and installation must comply with OMB policy M-05-24, NIST SP-800-116-1, and all other applicable standards established by OMB, NIST, and the OCIO Council.

3.4 VISITOR ACCESS CONTROL: (SHELL)

ISC LOP II: Always require visitors (Lessor contracted maintenance personnel) to nonpublic areas be sponsored by a tenant and either approved for unescorted access or escorted at all times.

- Entrances are open to the public during business hours.

- The Government reserves the right to verify the identity of persons requesting access to the Government-controlled Space prior to allowing entry.

3.5 OCCUPANT SCREENING:

No special measures required.

3.6 VISITOR SCREENING:

No special measures required.

3.7 BALLISTIC PROTECTION AT SCREENING LOCATIONS:

No special measures required.

3.8 LOBBY QUEUING:

No special measures required.

3.9 AFTER-HOURS ACCESS CONTROL (SHELL)

ISC LOP II: All employees, contractors, and visitors shall sign in and sign out electronically or on a building register after-hours.

- All Government employees, under this lease, shall be allowed access to the leased space (including after-hours access).

3.10 LIMIT BUILDING ENTRY POINTS:

No special measures required

3.11 ENTRANCE CO-LOCATION: (SHELL):

No special measures required.

3.12 PERIMETER DOORS AND DOOR LOCKS: (SHELL)

ISC LOP II: Secure government space perimeter doors with non-removable hinges and high-security mechanical or electronic locks.

- Access to government space shall be managed by installing compliant Physical Access Control in compliance with OMB policy M-05-24, NIST SP-800-116-1, and all other applicable standards established by OMB, NIST, and the OCIO Council.
- Hinge pins located on the unsecured side of perimeter and critical interior doors must be designed to preclude door removal.
- Ensure magnetic locks have at least 1,200 pounds of shear holding power.
- Electric strikes must meet all specifications of UL Standard 1034, Burglary-Resistant Electric Locking Mechanisms. For more information on electric strikes, refer to American National Standards Institute (ANSI) A156.25.
- Door strikes should not allow the dead latch to be in the fully extended position when the door is closed.
- Entrance Doors shall be capable of being remotely locked and unlocked from the reception desk or other designated position

3.13 CONTROL OF KEYS AND ACCESS MEDIA: (SHELL):

The Government reserves the right to implement a formal key control program. The Lessor shall have a means of electronically disabling lost or stolen access media.

3.14 EMPLOYEE CONVENIENCE DOOR: (SHELL)

ISC LOP III: The Lessor shall ensure staff entrances are located independently of main entrance lobbies and be convenient to staff parking.

- Provide electronic access control for employee entry doors without a security force post (including after-hours access) in conjunction with VSS coverage.

3.15 EMERGENCY EXIT DOORS: (SHELL):

ISC LOP II: Secure emergency exit doors using an automatic door closer and exit hardware that are compliant with NFPA Life Safety Code and applicable standards. Monitor all emergency exits via visual, electronic, or audible means.

3.16 DELAYED EGRESS: (SHELL):

No special measures required.

4.0 INTERIOR SECURITY CRITERIA

2.22 SPACE PLANNING:

No special measures required

2.23 ACCESS TO NON-PUBLIC AREAS (PROVIDER AREAS): (TI)

ISC LOP IV: Use signage, walls, and electronic access control to establish physical boundaries to control access to non-public areas such as exam rooms and provider offices.

- The Lessor will create a protected partition between the leased space lobby and the non-public provider area.
- The doors leading to the non-public area will meet the same specifications as the perimeter. The doors will have electronic locks to allow escorted visitors into the non-public space.

2.24 SECURITY OF CRITICAL AREAS (i.e. PHARMACY or TELECOM ROOMS): (TI)

ISC LOP III: Install electronic access control, VSS and IDS to control and monitor access into critical areas such as pharmacy, Network Rooms/IT Closets, etc.

- Access to government space shall be managed by installing compliant Physical Access Control in compliance with OMB policy M-05-24, NIST SP-800-116-1, and all other applicable standards established by OMB, NIST, and the OCIO Council.
- For Pharmacy: Interior wall separating pharmacy from public area must meet 15-minute forced entry resistant construction and extend from slab to slap.

2.25 BUILDING SYSTEMS AND ROOF ACCESS: (SHELL)

ISC LOP II: Secure utility, mechanical, electrical, and telecom rooms, and access to interior space from the roof with high-security locks.

2.26 PUBLICLY ACCESSBILE RESTROOMS:

Patients and Visitors shall have access to public restrooms in the facility.

2.27 PUBLICLY ACCESSIBLE RETAIL AND MIXED-USE SPACE: (SHELL)

ISC LOP II: Accommodate publicly accessible retail and mixed uses through such means as separating entryways.

2.28 INTERIOR WINDOWS: (TI)

No special measures required.

5.0 SECURITY SYSTEMS CRITERIA

5.1 VSS COVERAGE: (SHELL)

ISC LOP III: Provide VSS coverage of personnel entrances and exits, parking lots, loading docks, lobbies and other areas as required by other paragraphs.

- VA Police will designate a purpose and goal for each security camera installed and verify/test that the VSS is designed to meet the physical security needs of the space and occupants.
- The lessor shall design, install and maintain the VSS.
- Technical review of the proposed system shall be coordinated with the VA security representative, and the direction of the Contracting Officer, prior to completion of the CD's, as well as prior to installation. VSS system testing, and acceptance shall be conducted by the VA prior to occupancy.
- The Lessor shall comply with FAR52.204-25: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services of Equipment (NOV 2021). See https://www.acquisition.gov/far/part-52#FARD_52_204_25

5.2 VSS MONITORING AND RECORDING: (SHELL)

ISC LOP II: Record CCTV views using a digital medium.

- Firmware and software updates from the manufacturer should be installed as soon as possible to prevent any breach.
  - A chain of custody and written procedures for evidence retrieval must be developed (contact isfubgroup@tswg.gov for a publication on Best Practices for the Retrieval of Video Evidence from Digital VMS Systems or visit www.tswg.gov).
  - The need for disaster recovery and remote operational capability, including offsite storage of data, should be considered when designing the VSS.
- The images shall be recorded at a minimum rate of 15 frames per second on digital media.
  - Motion recording with conditional refresh is recommended to reduce bandwidth and storage challenges. External entrance/exit cameras and any cameras covering significant areas or assets (identified during the risk assessment) should record at all times. Recorded images should be at the camera's maximum resolution.
- Edge recording capabilities should be considered when network bandwidth or network outages are a concern.
- Storage:

- Surveillance video must be stored for 90 days.

5.3 SECURITY CONTROL CENTER:

No special measures required

5.4 VSS SURVEILLANCE ADVISORY: (SHELL)

ISC LOP II: When VSS is utilized, post signage at the entrance of the location.

- Post signs at entrances to the site, facility, parking garages, etc., where VSS coverage exists.
- Signs should be large enough to be noticed, placed in an easily seen location, and have both words and pictures indicating video surveillance is being conducted at the location.

5.5 INTRUSTION DETECTION SYSTEM (IDS) COVERAGE: (TI)

ISC LOP II: Provide IDS on perimeter entry and exit doors and all ground-floor windows. Provide a separate IDS partition for all rooms where VA IT network equipment is kept. Provide a separate IDS partition for the police operations area when included in the program. Provide a separate IDS partition for the Armory when included in the program. Provide a separate IDS partition for the Pharmacy when included in the program. Provide a separate IDS partition for the Pharmacy Vault when included in the program.

- The Lessor shall design, install, and maintain the IDS system. Technical review of the proposed system shall be coordinated with the VA security representative, at the direction of the Lease Contracting Officer, prior to completion of the CDs, and prior to installation. System testing and acceptance shall be conducted by the VA prior to occupancy.
- UL 2050 Listed intrusion detection equipment is required. Initial installation should include validation (testing) of the entire system, including monitoring center notification and connected equipment.
- The following descriptions are provided as benchmarks in considering the appropriate system technologies. An access control system can serve as an IDS as long as it meets the IDS details listed here and has provisions for monitoring (see IDS Monitoring).
  - Entry Doors will have:
    - Magnetic switch;
    - Alarm system keypad (at main employee entrance); and
    - Motion Sensor coverage (passive infrared sensor (PIR), microwave, ultrasonic, or similar device).
  - Windows and other openings greater than 96 square inches:
    - Glass-break detector; and
    - Magnetic switches or shock sensors.
    - Non-opening windows should utilize glass break detectors and/or motion sensor coverage.
  - Installation Practices: No matter the system type listed above the following installation practices should be used:
    - All IDS devices should be on a supervised circuit.

- End-of-line resistors for supervision must be placed in the individual sensor and not in the alarm panel.
- Alarm panels should be in a locked tamper-proof container with a tamper switch.
- Alarm panels should be located in a locked area that is only assessable to authorized individuals. Area should be protected by IDS.
- External facility entrances and high-security applications should be designed in a multi-layered approach (e.g., doors that have magnetic or balanced magnetic switches should also be protected with a motion sensor).
- Zoning – Each alarm sensor or alarm point should have its own zone. This will help with troubleshooting alarm points and response to alarms.
- Double doors – Double doors or split doors should be zoned on each leaf, not both doors on one zone.
- Cross zoning (the requirement of two or more sensors to be activated in a specific amount of time before activating an alarm) should be avoided.
- Garage doors – Garage doors should have a sensor on each side to prevent the lifting on one side without an alarm.
- Accessible external facility openings that are 96 square inches or more should be alarmed.
- Door contacts should be installed on the opening side of the door and should not allow the door to open far enough to provide the ability to tamper with the contact inside the door without going into alarm.

5.6 INTRUSTION DETECTION SYSTEM (IDS) MONITORING: (SHELL)

ISC LOP II: Lessor shall monitor at a central station with notification to law enforcement or security responders.

5.7 DURESS ALARMS OR ASSISTANCE STATIONS: (TI)

ISC LOP III: Provide duress buttons or call buttons at security force posts and sensitive public contact areas.

Locations: All reception/transaction counters and windows, shared medical appointments rooms, group therapy rooms and large multi-purpose rooms.

- Duress devices shall be concealed from the public and shall annunciate for an immediate response.
- System owner will perform monthly testing of duress buttons and perform required maintenance; system owner will provide documentation at the request of the VA.
- If batteries are utilized to power the alarm, the batteries should be replaced yearly or as required and documented.
- Duress Alarm system and design will be approved by VA Police during design or prior to installation.

5.8 SECURITY SYSEM INTEGRITY:

ISC LOP II: Secure alarm and physical access control panels, VSS components, controllers, and cabling against unauthorized access.

5.9 SECURITY COMMUNICATIONS:

No special measure required.

5.10 BUILDING COMMUNICATON SYSTEM:

ISC LOP III (TI): Provide a communication system for security and emergency announcements.

5.11 EMERGENCY POWER FOR SECURITY SYSTEMS:

ISC LOP III (TI): Provide uninterruptible emergency power to essential electronic security systems for a minimum of four hours.

5.12 SECURITY SYSTEM TESTING:

ISC LOP II (SHELL): Lessor shall conduct security system performance testing annually and provide documentation to VA.

5.13 SECURITY SYSTEM MAINTENANCE:

ISC LOP II (SHELL): Lessor shall implement a maintenance program for all security systems. Any critical component that becomes inoperable must be replaced or repaired within five business days.

- Failure by the Lessor to provide sufficient replacement measures within the timeframe identified may result in the VA providing guard service, the cost of which must be reimbursed by the Lessor.

6.0 SECURITY OPERATIONS AND ADMINISTRATION

6.1 FACILITY SECURITY PLAN: (SHELL):

Lessor shall develop a written Facility Security Plan in conjunction with VA that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades in accordance with the National Terrorism Advisory System. Plan shall be submitted to VA for review and approval prior to lease acceptance.

6.2 SECURITY DURIGN CONSTRUCTION AND RENOVATION (SHELL):

Develop and implement a Construction Security Plan.

6.3 PROTECTION OF CONSTRUCTION INFORMATION: (SHELL):

Limit access to construction documents to those persons with an established need-to- know.

7.0 CYBERSECURITY

7.1 FACILITY CYBERSECURITY REQUIREMENTS

A. Lessors are prohibited from connecting any portion of their building and access control systems (BACS) to any federally owned or operated IT network. BACS include systems providing fire and life safety control, physical access control, building power and energy control, electronic

surveillance, and automated HVAC, elevator, or building monitoring and control services (including IP addressable devices, application servers, or network switches).

B. In the event of a cybersecurity incident related to BACS, the Lessor shall initially assess the cyber incident, identify the impacts and risks to the building and its occupants, and follow their organization's cyber and IT procedures and protocols related to containing and handling a cybersecurity incident. In addition, the Lessor shall immediately inform the Lease Contracting Officer's (LCO's) designated representative, i.e., the Lease Administration Manager (LAM), about cybersecurity incidents that impact a federal tenant's safety, security, or proper functioning.

C. Lessors are encouraged to put into place the following cyber protection measures to safeguard facilities and occupants:

1. Engineer and install BACS to comply with the Department of Homeland Security Industrial Control Systems Computer Emergency Response Team (DHS ICS-CERT) cyber security guidance and recommendations (https://ics-cert.us-cert.gov/Recommended-Practices).
2. Refer to the National Institute of Standards and Technology Cyber Security Framework (NIST-CSF) (https://www.nist.gov/cyberframework) and cybersecurity guidance in the DHS Commercial Facilities Sector-Specific Plan (https://www.dhs.gov/publication/nipp-ssp-commercial-facilities-2015) for best practices to manage cyber risks.
3. Encourage vendors of BACS to secure these devices and software through the following:
   a. Develop and institute a proper Configuration Management Plan for the BACS devices and applications, so that the system can be supported.
   b. Safeguard sensitive data and/or login credentials through the use of strong encryption on devices and applications. This means using NIST- approved encryption algorithms, secure protocols (i.e., Transport Layer Security (TLS) 1.1, TLS 1.2, TLS 1.3) and Federal Information Processing Standard (FIPS) 140-2 validated modules.
   c. Disable unnecessary services in order to protect the system from unnecessary access and a potential exposure point by a malicious attacker. Examples include File Transfer Protocol-FTP (a protocol used for transferring files to a remote location) and Telnet (allowing a user to issue commands remotely). Additionally, use of protocols that transmit data in the clear (such as default ZigBee) should be avoided, in favor of protocols that are encrypted.
   d. Close unnecessary open ports to secure against unprivileged access.
   e. Monitor and free web applications and supporting servers of common vulnerabilities in web applications, such as those identified by the (Open Web Application Security Project (OWASP) Top 10 Project (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).
   f. Enforce Least Privilege, where proper permissions are enforced on a device or application so that a malicious attacker cannot gain access to all data. Enforcing Least Privilege will only allow users to access data they are allowed to see. Additional information can be found at https://www.beyondtrust.com/blog/what-is-least-privilege/.
   g. Protect against Insufficient User Access Auditing, where device or application does not have a mechanism to log/track activity by user. Enforce changing of factory default Username and Password to prevent unauthorized entry into the BACS system.
   h. Use updated antivirus software subscription at all times. Kaspersky-branded products or services, prohibited from use by the Federal Government, are not to be utilized.
   i. Conduct antivirus and spyware scans on a regular basis. Patching for workstations and server Operating System (OS), as well as vulnerability patching should follow standard industry best practices for software development life cycle (SDLC).

j. Discontinue the use of end of life (EOL) systems and use only applications/systems that are supported by the manufacturer.
k. Operating Systems must be supported by the vendor for security updates (e.g., do not use Windows Server 2003).
l. Proposed standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved United States Government Configuration Baseline (USGCB) or tenant agency guidance (if applicable).
m. Disallow the use of commercially provided circuits to manage building systems and install building systems on a protected network, safeguarded by the enterprise firewalls in place. Workstations or servers running building monitor and control systems are not connected and visible on the public internet.
n. Systems should have proper system configuration hardening and align with Center for Internet Security (CIS) benchmarks or other industry recognized benchmarks. Additional information can be found at https://www.cisecurity.org/cis-benchmarks/.