SECURITY REQUIREMENTS - FACILITY SECURITY LEVEL III

THESE PARAGRAPHS CONTAIN ADDITIONAL SECURITY REQUIREMENTS THAT MAY BE INSTALLED IN THE LEASED SPACE, AND UNLESS INDICATED OTHERWISE, ARE TO BE PRICED AS PART OF THE BUILDING SPECIFIC AMORTIZED CAPITAL (BSAC). BECAUSE EACH BUILDING IS UNIQUE, THE FINAL LIST OF SECURITY COUNTERMEASURES WILL BE DETERMINED DURING THE DESIGN PHASE AND IDENTIFIED IN THE DESIGN INTENT DRAWINGS AND CONSTRUCTION DOCUMENTS. AFTER COMPLETING THE CONSTRUCTION DOCUMENTS, THE LESSOR SHALL SUBMIT A LIST OF THE ITEMIZED COSTS. SUCH COSTS SHALL BE SUBJECT TO NEGOTIATION.

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 AND SYSTEMS- The areas that house systems that if damaged and/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, utilities, telecom closets or potable water supply that may be located outside 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 Government, including the Federal Protective Service (FPS), 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 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.

I. FACILITY ENTRANCES, LOBBY, COMMON AREAS, NON-PUBLIC, AND UTILITY AREAS

A. FACILITY ENTRANCES AND LOBBY

If the total Space leased by the Government 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 total Space leased by the Government 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.

1. LIMITING LOBBY QUEUING

The Lessor and the Government shall minimize lobby queuing caused by screening, visitor processing, and access control systems.

2. PHYSICAL BOUNDARIES TO CONTROL ACCESS TO PUBLIC AND NON-PUBLIC AREAS

The Government reserves the right to use signage, stanchions, counters, furniture, knee walls, or product-equivalents, as determined by the Government, to establish physical boundaries to control access to non-public areas. The Lessor shall post directional signs as appropriate.

3.. MAGNETOMETERS AND X-RAYS AT PUBLIC ENTRANCES

The Government shall establish a list of prohibited items, including potential weapons, that shall apply to all building tenants and visitors. Magnetometers and X-ray machines will be installed, tested (on a daily basis), and maintained by the Government at the public entrance(s). Armed security guards, provided by the Government, will direct the occupants and visitors through the screening equipment. Appropriate lobby and entrance/exit space shall be made available for this purpose in a manner to minimize queuing. This space shall be considered part of the lease common area and not ABOA square footage. The Government requires visitors to non-public areas to display a visitor's identification badge. If there are other non-Government tenants, the Lessor shall notify them of this requirement and assist those tenants in obtaining ID acceptable to the Government.

B. ADDITIONAL REQUIREMENTS

1. EMPLOYEE AND VISITOR SIGN-IN/OUT AFTER HOURS

The Lessor shall provide a system, acceptable to the Government, that after hour employees, contractors, and visitors to the Building shall be required to sign in and sign out either electronically or on a building register.

2. ACCOMMODATION OF RETAIL/MIX USE SPACE (SHELL)

Lessor shall accommodate publicly accessible retail and mixed uses through such means as separating entryways.

C. COMMON AREAS, NON-PUBLIC, AND UTILITY AREAS

1. PUBLIC RESTROOMS ACCESS (SHELL)

If required by the Government, the Lessor shall provide a means to control access to public restrooms within Government controlled Space.

2. SECURING CRITICAL AREAS

Areas designated as Critical Areas shall be locked using fully HSPD-12 compliant electronic access control equipment (see Intrusion Detection System (IDS) requirements). The Government shall have the right to monitor and limit access to these areas. Access shall be limited to authorized personnel, as determined by the Government.

3. VISITOR ESCORT AND ID REQUIREMENTS

The Government shall require the Lessor to escort contractors, service personnel, and visitors to all non-public areas. The Lessor shall require visitors to non-public areas to display a visitor ID at all times.

4. SECURING COMMON BUILDING UTILITIES, SERVICE ROOMS, AND ACCESS TO ROOF

The Lessor shall secure utility, mechanical, electrical telecommunication rooms, HVAC control panels, roof access points, and access to interior space from the roof with locks or Physical Access Control Systems (PACS), and as part of BSAC, monitor these areas with an Intrusion Detection System (IDS). Roof access should meet the applicable egress requirements in National Fire Protection Association (NFPA) 101, Life Safety Code, or IBC, current as of the award date of the lease.

5. CRITICAL SYSTEM LOCATION

Critical Systems (e.g., mechanical, electrical, utility rooms; HVAC vents; emergency generator) shall be located at least 25 feet from the Building loading docks, entrances, mailrooms, personnel and package screening locations, and uncontrolled parking areas, or, alternatively, as part of BSAC, Lessor shall protect critical Building system areas in accordance with the post-award DBT analysis by implementing sufficient standoff, hardening, and venting methods.

6. RESTRICT CONTACT FROM PUBLIC AREAS WITH PRIMARY VERTICAL LOAD MEMBERS

The Lessor shall implement architectural or structural features, or other positive countermeasures that deny contact with exposed primary vertical load members in the public areas. A minimum standoff of at least 100 mm (4 inches) is required. For measurement purposes, standoff shall be considered building support space and not ABOA.

7. RESTRICT CONTACT FROM MAIL AREA WITH PRIMARY VERTICAL LOAD MEMBERS

The Lessor shall implement architectural or structural features, or other positive countermeasures in the mail screening and receiving areas that deny contact with exposed primary vertical load members. A minimum standoff of at least 150 mm (6 inches) is required. For measurement purposes, standoff shall be considered building support space and not ABOA.

II. INTERIOR (GOVERNMENT SPACE)

A. WEARING PHOTO ID IN GOVERNMENT SPACE

The Lessor and his/her contractors shall be required to wear a photo ID to be visible at all times when in Government- controlled Space.

B. SECURE EMPLOYEE ENTRANCE DOORS

The Lessor shall provide a means to secure doors identified by Government as employee entrance doors. The Government may elect to post guards to verify ID badges via visual and physical inspection or electronic means before entry to Government occupied Space.

C. LIMIT ON ENTRY POINTS (SHELL)
The Government may elect to limit the number of entry points to the Building or to the Government occupied Space to the fewest number practicable.

D. FORMAL KEY CONTROL PROGRAM (SHELL)
The Government reserves the right to implement a formal key control program. The Lessor shall have a means of allowing the electronic disabling of lost or stolen access media if electronic media is used.

E. ELECTRONIC ACCESS FOR EMPLOYEES
The Lessor shall provide a PACS card reader for employee entry doors without a guard post (including after-hours access) in conjunction with Video Surveillance System (VSS) coverage.

F. 552.270-34 ACCESS LIMITATIONS FOR HIGH-SECURITY LEASED SPACE (JUN 2021) (SHELL *)
(a) The Lessor, including representatives of the Lessor's property management company responsible for operation and maintenance of the leased space, shall not—

(1) Maintain access to the leased space; or

(2) Have access to the leased space without prior approval of the authorized Government representative.

(b) Access to the leased space or any property or information located within that Space will only be granted by the Government upon determining that such access is consistent with the Government's mission and responsibilities.

(c) Written procedures governing access to the leased space in the event of emergencies shall be documented as part of the Government's Occupant Emergency Plan, to be signed by both the Government and the Lessor.

III. SITE AND EXTERIOR OF THE BUILDING

A. SIGNAGE

1. POSTING OF SIGNAGE IDENTIFYING THE SPACE AS GOVERNMENTAL (SHELL)
The Lessor shall not post sign(s) or otherwise identify the facility and parking areas as a Government, or specific Government tenant, occupied facility, including during construction, without written Government approval.

2. POSTING OF REGULATORY SIGNAGE (SHELL)
The Government may post or request the Lessor to post regulatory, statutory, sensitive areas, and site-specific signage.

B. LANDSCAPING AND ENTRANCES

1. CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (SHELL)

a. The Lessor shall separate from public access, restricted areas as designated by the Government, through the application of Crime Prevention Through Environmental Design (CPTED) principles by using trees, hedges, berms, or a combination of these or similar features, and by fences, walls, gates, and other barriers, where feasible and acceptable to the Government.

b. Landscaping shall be neatly trimmed in order to minimize the opportunity for concealment of individuals, packages/containers, and parking areas. Lessor shall provide trees, hedges, berms, or any combination of these to create buffer zones to separate public areas and other functions. Landscaping shall not obstruct the views of security guards and VSS cameras or interfere with lighting or IDS equipment.

2. HAZMAT STORAGE

Where applicable, Lessor shall locate HAZMAT storage in a restricted area or storage container away from loading docks, entrances, and uncontrolled parking. As part of BSAC, Lessor shall monitor the HAZMAT storage area using IDS and/or VSS, and control access to these areas.

3. PLACEMENT OF RECEPTACLES, CONTAINERS, AND MAILBOXES

Lessor shall position trash containers, mailboxes, FedEx-UPS boxes, donation/recycle containers, vending machines, or other fixtures and features that could conceal packages, briefcases, or other portable containers away from building exterior and entry points. Alternatively, as part of BSAC, the Lessor shall implement blast containment measures to mitigate an explosion in these areas. If blast containment measures are proposed, certification by a registered professional engineer is required that the equivalent mitigation capability is present.

4. VEHICLE BARRIERS

In accordance with the post-award DBT analysis, the Lessor shall provide vehicle barriers to protect pedestrian entrances from penetration by a vehicle (e.g., concrete bollards, concrete planters, concrete retention walls).

Minimum barrier height is 30 inches, and maximum clear spacing between vehicle barriers is 4 feet. The Lessor shall use barriers to ensure that vehicles cannot pass beyond the screening check point until cleared.

C. PARKING

1. NUMBER OF PARKING ENTRANCES

The number of parking entrances shall be limited to the minimum required for efficient operations or local code, (giving consideration to minimizing queuing). Entrances to parking areas shall be equipped with vehicle gates to control access to authorized vehicles (employee, screened visitor and approved Government vehicle). Gates controlling vehicles may include, but are not limited to, barriers (drop arm/wedge), garage style doors, and traditional chain link fences.

2. AUTHORIZED ACCESS TO PARKING (SHELL)
Lessor shall limit parking and access to parking to employee vehicles, authorized visitor vehicles, approved government vehicles, and other authorized vehicles.

3. VEHICLE SCREENING
The Government may elect to screen all visitor vehicles (before entry into the controlled parking area) as prescribed by the Government. This screening shall include ID verification and visual inspection of the vehicle, including undercarriage. The Lessor shall provide adequate lighting in screening area to illuminate the vehicle exterior and undercarriage. VSS coverage of the screening area shall be provided by the Lessor (see VSS requirements).

4. PUBLIC ACCESS TO GOVERNMENT PARKING AREAS
Where there is Government controlled parking the area shall be controlled by limiting pedestrian access to the controlled parking areas. Pedestrian and vehicle access points to all parking areas shall be monitored by VSS camera(s) at all times

IV. SECURITY SYSTEMS

A. SECURITY SYSTEM TESTING AND MAINTENANCE CRITERIA:

The Lessor in consultation and coordination with a security provider, either internal or external, as determined by the Lease Contracting Officer, and the Government security representative shall implement a testing and preventive maintenance program for all security systems the Lessor has installed. Testing must be based on established, consistent, agency-specific protocols, to be determined at the time of design. All testing shall be documented. Operational performance testing shall be conducted annually and functional testing shall be conducted more frequently, as determined by the Government. Components which fail, either during testing or throughout the life of this lease shall be repaired or replaced by the Lessor within a reasonable timeframe as determined by the Government. Any critical component that becomes inoperable must be replaced or repaired by the Lessor within 72 hours. Critical components are those required to provide security (IDS, VSS, PACS, etc.) for a perimeter access point or critical area. "Replacement" may include implementing other temporary measures in instances where the replacement or repair is not achievable within the specified time frame (e.g. a temporary barrier to replace an inoperable pop-up vehicle barrier, etc.). Failure by the Lessor to provide sufficient replacement measures within the timeframe identified above may result in the Government providing guard service, the cost of which must be reimbursed by the Lessor.

B. VIDEO SURVEILLANCE SYSTEM

GOVERNMENT PROVIDED PRODUCT, INSTALLATION, AND MAINTENANCE
The Government may provide and install an entry control system, with time lapse video recording and digital image storage, that will allow Government employees to view and communicate remotely with visitors before allowing access. This Video Surveillance System (VSS) shall provide the Government with unobstructed coverage, as determined by the Government, of designated pedestrian entrances and exits. The Lessor shall permit twenty-four-hour VSS coverage and recording, provided and operated by the Government. The

Government will centrally monitor the VSS surveillance. Government specifications are available from the Contracting Officer.

After notice to proceed, the Lessor shall advise the Government of the appropriate time to install the equipment during the construction of the Space and shall facilitate the installation, including access to electrical panels and other areas of the building, as necessary. The Lessor's construction schedule shall reflect the installation of this equipment.

C. INTRUSION DETECTION SYSTEM

GOVERNMENT PROVIDED SCOPE AND PRODUCT, INSTALLATION, AND MAINTENANCE The Lessor shall permit installation of a perimeter Intrusion Detection System (IDS) to be operated by the Government. The Government shall provide and install an IDS on perimeter entry and exit doors, and all ground-floor windows. Basic Security-in-Depth IDS— include: magnetic door switch(s), alarm system keypad, passive infrared sensor(s) (PIR), an alarm panel (to designated monitoring center) and appropriate communication method i.e. telephone and/or Internet connection, glass-break detector, magnetic window switches or shock sensors.

Basic Security-in-Depth IDS shall be connected and monitored at a central station. Emergency notification lists shall be coordinated with the monitoring station to include all applicable Government and Lessor points of contact, including law enforcement (Federal Protective Service and facility security force). Monitoring shall be designed to facilitate a real-time detection of an incident, and to coordinate an active response to an incident.

After notice to proceed, the Lessor shall advise the Government of the appropriate time to install the equipment during the construction of the Space and shall facilitate the installation, including access to electrical panels and other areas of the building, as necessary. The Lessor's construction schedule shall reflect the installation of this equipment.

D. DURESS ALARM

GOVERNMENT PROVIDED SCOPE, PRODUCT, INSTALLATION, AND MAINTENANCE
The Lessor shall permit installation of a duress alarm system to be provided and operated by the Government. The Government, in coordination with a security provider, either internal or external, as determined by the Lease Contracting Officer, shall document and implement duress procedures for emergency situations.

After notice to proceed, the Lessor shall advise the Government of the appropriate time to install the equipment during the construction of the Space and shall facilitate the installation, including access to electrical panels and other areas of the building, as necessary.
The Lessor's construction schedule shall reflect the installation of this equipment.

E. SECURITY SYSTEMS DESIGN

The Lessor, in consultation and coordination with security providers (internal or external) and the agency designated security representative, shall ensure at the time of system design, system construction, and throughout the term of the Lease, that alarm and Physical Access Control Panel, VSS components, controllers, and cabling shall be secured from unauthorized physical and logical access.

F. CENTRAL SECURITY CONTROL CENTER

1. CENTRALIZED COMMUNICATIONS SYSTEM

The Lessor, in consultation and coordination with security providers (internal or external) and the agency designated security representative, shall provide and maintain a communication system for security and emergency announcements. Communication may be achieved through public address systems, specially-designed phone systems, and computer-based mass delivery. This communication system should be utilized to provide emergency announcements, alerts and instructions to occupants. On site communication with guards (if applicable), designated response personnel and Occupant Emergency Plan (OEP) support employees is essential during an incident. Procedures for standard announcements and drills shall be developed. Standard announcements may be prerecorded into the Building communication system for immediate notification.

2. EMERGENCY POWER TO SECURITY SYSTEMS

The Lessor, in consultation and coordination with a security provider (internal or external) and the agency designated security representative, shall provide uninterruptible emergency power to essential electronic security systems for a minimum of 4 hours. Uninterruptable power can be provided through the use of batteries, emergency generators, UPS, or a combination thereof to meet the requirements.

V. STRUCTURE

NOTE: FOR ADDITIONAL BLAST RESISTANT MEASURES REQUIRED IN NEW LEASE CONSTRUCTION PROJECTS, REFER TO LEASE PARAGRAPH “SECURITY FOR NEW CONSTRUCTION”.

A. WINDOWS

1. SHATTER-RESISTANT WINDOW PROTECTION

The Lessor shall use either (1) preferred or acceptable glazing systems or (2) acceptable fragment retention film to reduce the glass fragmentation hazard. 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.

Acceptable glazing systems include thermally tempered glass and thermally tempered, heat strengthened, or annealed glass with fragment retention film installed on the interior surface. Acceptable fragment retention film must meet or exceed the following physical properties:

- Shatter-resistant material shall not be less than 0.18 millimeters (7 mil) thick on all exterior windows in Government-occupied Space meeting the following 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%

2. LOCK GROUND FLOOR WINDOWS
If a Government tenant occupies ground floor space in the Building, there shall be no operable windows. As part of BSAC, the Lessor shall monitor any operable windows via IDS.

3. SECURE NON-WINDOW OPENINGS (SHELL)
The Lessor shall secure all non-window openings, such as, mechanical vents, utility entries, and exposed plenums to prevent forcible entry.

4. PREVENT VISUAL OBSERVATION INTO EXTERIOR OFFICES (T.I.)
The Lessor shall provide blinds, curtains, or other window treatments in critical areas acceptable to the Government, that can be employed to prevent visual observation of that area when temporary conditions warrant.

B. BUILDING SYSTEMS

1. EMERGENCY GENERATOR PROTECTION (T.I.)
If an emergency generator is required by the Government, the Lessor shall locate it in a secure area, protected from unauthorized access, and vehicle ramming, if outdoors. The emergency generator and its fuel tank must be located at least 25 feet from loading docks, entrances, and parking areas. Alternatively, if the 25 foot distance cannot be achieved, Lessor shall protect utilities in accordance with the post-award DBT analysis, through a combination of standoff, hardening, and venting methods.

2. SECURING ON-SITE PUBLICLY ACCESSIBLE UTILITIES
The Lessor shall secure the water supply handles, control mechanisms, and service connections at on-site publicly accessible locations with locks and anti-tamper devices.

3. SECURING AIR INTAKE GRILLES
The Lessor shall secure accessible air intakes with fencing. Air intake grilles shall be secured with tamper switches connected to a central alarm monitoring station and monitored by VSS or other security force patrols.

4. HVAC SYSTEM FOR CHEMICAL, BIOLOGICAL AND RADIOLOGICAL (CBR) ATTACK-SUSCEPTIBLE AREAS

The Lessor shall provide separate isolated HVAC systems in lobbies, loading docks, mail rooms and other locations as identified by a risk assessment as susceptible to CBR attack, to protect other building areas from possible contamination.

All exterior air handling units (AHUs), including the supply air for re-circulating AHUs, shall be equipped with Minimum Efficiency Reporting Value (MERV) 10 particulate filters. AHUs serving lobbies and mailroom, including the supply air stream for re-circulating AHUs, shall be equipped with Minimum Efficiency Reporting Value (MERV) 13 filters.

5. HVAC CONTROL

As part of operating rates, all air handlers must be equipped with an emergency shut-off and exhaust system. Lessor must provide for controlling the movement of elevators, and the closing of applicable doors and dampers to seal the Building. Where shut-off is via a Building Automation System (BAS), the system configurations must be properly programmed, tested, and accessible at all necessary times.

VI. OPERATIONS AND ADMINISTRATION

A. FACILITY SECURITY COMMITTEE (SHELL *)

The Lessor shall cooperate and work with the buildings Facility Security Committee (FSC) throughout the term of the Lease. The FSC is responsible for addressing facility-specific security issues and approving the implementation of security measures and practices. The FSC consists of representatives of all Federal tenants in the facility, the security organization, and the leasing department or agency.

B. ACCESS TO BUILDING INFORMATION (SHELL *)

Building Information—including mechanical, electrical, vertical transport, fire and life safety, security system plans and schematics, computer automation systems, and emergency operations procedures—shall be strictly controlled. Such information shall be released to authorized personnel only, approved by the Government, by the development of an access list and controlled copy numbering. The Lease Contracting Officer may direct that the names and locations of Government tenants not be disclosed in any publicly accessed document or record. If that is the case, the Government may request that such information not be posted in the building directory.

Lessor shall have emergency plans and associated documents readily available to the Government in the event of an emergency.

C. SECURITY PLANS AND LAYOUTS

The Lessor shall secure and keep safe any security plans, construction and alteration plans and layouts. This shall be addressed in the construction security plan. The Lessor shall treat and safe keep any plans and specifications related to security measures as For Official Use Only (FOUO).

D. CONSTRUCTION SECURITY PLAN (SHELL)

The Lessor shall develop and implement a construction security plan. The plan should specify who is responsible for the security of the site during each phase of the project until final completion. The construction

security plan shall describe in detail, how the Government's information, assets, equipment, and personnel will be protected during the construction process. (This shall include background checks, restrictions on accessibility, and escorts for the construction personnel). The required security measures will vary with the risk presented during the project. The Lessor shall also submit a security plan for all post-occupancy construction and alterations projects in the leased Space, throughout the term of this Lease.

E. SCREENING OF MAIL AND PACKAGES

Lessor shall provide space suitable for the Government to inspect and screen all mail and packages using X-ray at a loading dock, if present. If there is no loading dock, Lessor shall provide space at an existing screening location or at an alternative location in the Building acceptable to the Government. The screeners shall physically inspect items that cannot be passed through screening equipment before distribution to the Government agencies throughout the facility. This space shall be considered part of the lease common area and not ABOA square footage.

F. SECURITY GUARD POSTINGS

The Government may elect to post armed security guards at all screening checkpoints and at the entrances to Government-occupied Space.

G. SECURITY GUARD PATROLS

The Government may elect to provide interior and exterior roving guard patrols which may be conducted four times each day during normal business hours. The security guard force, provided by the U.S. Department of Homeland Security Federal Protection Service, will be armed and equipped with a centralized radio network with incident response dispatch capability from the on-site central security control center. The Lessor and the Government shall develop in coordination with the Government's Designated (security) Official, the security guard response SOPs to alarms and incidents to ensure full coordination and cooperation between the on-site Lessor representative and the Government tenant(s).

VII. CYBERSECURITY (SHELL *)

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 in order 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/.