SECURITY REQUIREMENTS - FACILITY SECURITY LEVEL II

THESE PARAGRAPHS CONTAIN ADDITIONAL SECURITY REQUIREMENTS, AND, UNLESS INDICATED OTHERWISE, ARE TO BE PRICED AS PART OF THE BUILDING SPECIFIC AMORTIZED CAPITAL (BSAC). MAINTENANCE COSTS ARE TO BE INCLUDED IN THE OPERATING RENT.

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).

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

1. EMPLOYEE ACCESS CONTROL AT ENTRANCES (SHELL)
The Lessor shall provide key or Physical Access Control System (PACS) for the entrance to this building and to doors identified by the Government as employee entrance doors. All Government employees, under this lease, shall be allowed access to the leased space (including after-hours access).

B. SCREENING REQUIREMENTS

1. ACCOMODATION OF RETAIL/MIXED USE SPACE (SHELL)

The 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 RESTROOM ACCESS (SHELL)

The Government reserves the right to control access to public restrooms within Government controlled Space.

2. SECURING CRITICAL AREAS (SHELL)

The Lessor shall secure areas designated as Critical Areas to restrict access to authorized personnel only, and post signage accordingly:

a. At a minimum, the Lessor shall secure building common areas such as mechanical and janitorial areas, sprinkler rooms, electrical closets, telecommunications rooms, and janitor closets. Utility, mechanical, electrical, and telecom rooms shall be secured with high-security (UL437) locks. Keyed locks, PACS card reader, or similar security measures shall strictly control access to Critical Areas. Additional controls for access to keys, PACS, and key codes shall be strictly maintained.

b. Roofs with HVAC systems and access to interior space from the roof shall also be secured with high-security (UL437) locks. Roof access shall be strictly controlled through keyed locks, PACS card reader, or similar measures. Fire and life safety egress shall be carefully reviewed when restricting roof access.

c. In addition, Lessor shall protect the ventilation equipment and system controls from unauthorized access.

3. VISITOR ACCESS CONTROL (SHELL)

Entrances are open to the public during business hours. After hours, visitor entrances are secured, and have a means to verify the identity of persons requesting access prior to allowing entry into the Premises.

4. PUBLIC SPACE RESTRICTIONS WITH PRIMARY VERTICAL LOAD MEMBERS

The Government reserves the right to remove this countermeasure requirement, post-award, based on building-specific conditions. For measurement purposes, standoff shall be considered building support space and not ABOA.

a. **RESTRICT CONTACT FROM PUBLIC AREAS WITH PRIMARY VERTICAL LOAD MEMBERS**: For partitions separating public space from federal space, the Lessor shall use construction materials which have inherent ductility, and which are able to respond to load reversals. Alternatively, the Lessor can use a minimum standoff of at least 100 mm (4 inches).

b. **RESTRICT CONTACT FROM MAIL AREA WITH PRIMARY VERTICAL LOAD MEMBERS:** In the partitions that separate public mail screening and receiving areas from federal tenants, the Lessor

shall use construction materials which have inherent ductility, and which are able to respond to load reversals. Alternatively, the Lessor can use a minimum standoff of at least 150 mm (6 inches).

II. INTERIOR (GOVERNMENT SPACE)

A. IDENTITY VERIFICATION (SHELL)

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

B. 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.

III. SITES 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. LANDSCAPING REQUIREMENTS (SHELL)

Landscaping shall be neatly trimmed to minimize the opportunity for concealment of individuals, packages/containers, and parking areas. If Landscaping exists, the 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 Video Surveillance System (VSS) cameras or interfere with lighting or Intrusion Detection System (IDS) equipment.

2. HAZMAT STORAGE (SHELL)

Where applicable, Lessor shall locate HAZMAT storage in a restricted area or storage container away from loading docks, entrances, and uncontrolled parking.

3. PLACEMENT OF RECEPTACLES, CONTAINERS, AND MAILBOXES (SHELL)

Trash receptacles, containers, mailboxes, FedEx-UPS boxes, vending machines, or other fixtures and/or features that could conceal packages, briefcases, or other portable containers shall be located away from building exterior and entry points.

C. PARKING

1. PUBLIC ACCESS TO GOVERNMENT PARKING AREAS (SHELL)

Lessor shall designate Government employee and visitor parking areas.

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 five business days. 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 SCOPE AND 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. The Lessor shall facilitate the installation by allowing 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 operable 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. The Lessor shall facilitate the installation by allowing 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 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 PACS panel, VSS components, controllers, and cabling shall be secured from unauthorized physical and logical access.

V. STRUCTURE

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

A. WINDOWS

LOCK GROUND FLOOR WINDOWS
If a Government tenant occupies ground floor space in the Building, the Lessor shall provide a means to lock all operable, ground floor windows with secure latches. As part of BSAC, any operable, ground floor windows shall be monitored via IDS.

B. BUILDING SYSTEMS

1. EMERGENCY GENERATOR PROTECTION (T.I.)

If an emergency generator is required by the Government, the Lessor shall locate it, either pre-existing or installed as part of Tenant Improvements, 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 AIR INTAKE GRILLES

Lessor shall secure all accessible air intake grills from tampering or removal. Whenever possible, locate outdoor air intakes at least 30 feet above grade, and preferably at roof level.

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 in the event of an emergency.

C. 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.

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 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/.