SECURITY REQUIREMENTS - FACILITY SECURITY LEVEL I

THESE PARAGRAPHS CONTAIN SECURITY REQUIREMENTS, ALL OF WHICH ARE TO BE PRICED AS PART OF THE BUILDING SHELL.

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).

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

A. FACILITY ENTRANCES AND LOBBY

1. EMPLOYEE ACCESS CONTROL AT ENTRANCES

The Lessor shall provide a key or a physical access control system (PACS) for the entrance to this building, and to doors identified by the Government as employee entrance doors. The Lessor shall consult and coordinate with the Federal Protective Service (FPS) on the installation, maintenance, and repair of PACS. All Government employees, under this lease, shall be allowed access to the leased space (including after-hours access).

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

1. PUBLIC RESTROOM ACCESS

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

2. SECURING CRITICAL AREAS

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. Keyed locks, PACS, 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. The Lessor shall consult and coordinate with FPS on the installation, maintenance, and repair of PACS.

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

3. VISITOR ACCESS CONTROL

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.

II. INTERIOR (GOVERNMENT SPACE)

A. IDENTITY VERIFICATION

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

B. FORMAL KEY CONTROL PROGRAM

The Government reserves the right to implement a formal key control program.

III. SITES AND EXTERIOR OF THE BUILDING

A. SIGNAGE

1. POSTING OF REGULATORY SIGNAGE

The Government may post or request the Lessor to post regulatory, statutory, and site-specific signage.

B. LANDSCAPING AND ENTRANCES

1. LANDSCAPING REQUIREMENTS

Landscaping shall be neatly trimmed to minimize the opportunity for concealment of individuals and packages/containers.

IV. SECURITY SYSTEMS

The Lessor, in consultation with FPS, shall secure any installed alarm and PACS, Video Surveillance System (VSS) components, controllers, and cabling in government- controlled Space against unauthorized access. Lessor shall conduct annual testing of any security systems and daily testing of any active screening equipment.

A. VIDEO SURVEILLANCE SYSTEM

If Video Surveillance System (VSS) is in use, the Lessor shall post signage at the entrance of the building.

The Lessor shall comply with FAR 52.204-25: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2020). See https://www.acquisition.gov/far/part-52#FAR_52_204_25.

B. INTRUSION DETECTION SYSTEM

If Intrusion Detection System (IDS) is in use, the Lessor shall install local annunciation, consisting of an interior alarm within the facility.

C. DURESS ALARM

Lessor shall implement duress procedures for emergency situations.

V. STRUCTURE

A. 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, the Lessor shall protect utilities through a combination of standoff, hardening, and venting methods.

VI. OPERATIONS AND ADMINISTRATION

A. FACILITY SECURITY COMMITTEE (FSC)

The Lessor shall cooperate and work with the buildings Facility Security Committee (FSC) throughout the term of the Lease. The Facility Security Committee (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

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 are not 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.

VII. CYBERSECURITY

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 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/.