

APPENDIX C.2

SECURITY REQUIREMENTS

SECURITY REQUIREMENTS –

FACILITY SECURITY LEVEL II

THESE PARAGRAPHS CONTAIN ADDITIONAL SECURITY REQUIREMENTS AND UNLESS INDICATED OTHERWISE AS (SHELL), ARE TO BE PRICED AS PART OF THE BUILDING TENANT IMPROVEMENTS (TI)/AGENCY SPECIFIC REQUIREMENTS (ASR). WHERE THEY ARE IN CONFLICT WITH ANY OTHER REQUIREMENTS ON THIS LEASE, THE STRICTEST SHALL APPLY.

DEFINITIONS:

CRITICAL AREAS – These areas that house systems that if damaged or compromised could have significant adverse consequences for the facility, operations of the facility, or mission of the agent 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 Governmental-controlled space).

SENSITIVE AREAS – Sensitive areas include vaults, SCIFs, evidence rooms, war rooms, and sensitive documents areas. Sensitive areas are primary housed within Government-controlled space.

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

FACILITY ENTRANCES AND LOBBY

EMPLOYEE ACCESS CONTROL AT ENTRANCES (SHELL)

The Lessor shall provide key or electronic access control for all Government under this Lease employees to the entrance to the building (including after-hours access).

COMMON AREAS, NON-PUBLIC AND UTILITY AREAS

PUBLIC RESTROOM ACCESS (SHELL)

The Government reserves the right to control access to public restrooms, VA Police Operations, and OIT Communications (Main Server Room) located within the Space.

SECURITY CRITICAL AREAS (SHELL)

The Lessor shall secure areas designated as Critical Areas to restrict access:

- A. Keyed locks, keycards, or similar security measures shall strictly control access to mechanical areas. Additional controls for access to keys, keycards and key codes shall be strictly maintained. The Lessor shall develop and maintain accurate HVAC diagrams and HVAC system labeling within mechanical areas.
- B. Roofs with HVAC systems shall also be secured. Fencing or other barriers may be required to restrict access from adjacent roofs based on a Government Building Security Assessment.

APPENDIX C.2

Roof access shall be strictly controlled through keyed locks, keycards, or similar measures. Fire and life safety egress shall be carefully reviewed when restricting roof access.

- C. At a minimum, Lessor shall secure building common areas including sprinkler rooms, electrical closets, and telecommunications rooms.

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 Space.

INTERIOR (GOVERNMENT SPACE)

DESIGNATED ENTRANCES (SHELL)

The Government shall have a designated main entrance.

IDENTITY VERIFICATION (SHELL)

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

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.

SITES AND EXTERIOR OF THE BUILDING

SIGNAGE

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.

POSTING OF REGULATORY SIGNAGE (SHELL)

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

LANDSCAPING

LANDSCAPING REQUIREMENTS (SHELL)

Lessor shall maintain landscaping (trees, bushes, hedges, land contour, etc) around the facility. Landscaping shall be neatly trimmed in order to minimize the opportunity of concealment of

APPENDIX C.2

individuals and packages/containers. Landscaping shall not obstruct the views of security guards and CCTV cameras, or interfere with lighting or IDS equipment.

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (SHELL)

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.

LIGHTING

Install exterior lights at entrances, exits, parking lots, garages, and CCTV locations.

**** Illumination Level will comply with assisting patrolling of the facility after-darkness.**

PARKING

Designate Employee and Visitor parking areas.

**** Separate & Controlled.**

HAZMAT STORAGE

If there is HAZMAT storage, Lessor shall locate it in a restricted area or storage container way from loading docks, entrances and uncontrolled parking.

PLACEMENT OF RECEPTACLES, CONTAINERS AND MAILBOXES

Trash receptacles, containers, mailboxes, vending machines, or other fixtures and/or features that could conceal packages, brief cases, or other portable containers shall be located 10 feet away from building. All mail and packages shall be visually inspected prior to distribution through the facility.

EMERGENCY GENERATOR

Secure against unauthorized access and locate the emergency generator at least 25 feet from Loading Docks, Entrances, and Parking.

SECURITY SYSTEMS

**** CCTV INSTALLED BY LESSOR BUT APPROVED BY THE GOVERNMENT**

CLOSED CIRCUIT TELEVISION SYSTEMS (CCTV)

LESSOR PROVIDED DESIGN, INSTALLATION AND MAINTENANCE

The lessor shall design, install and maintain a Closed Circuit Television (CCTV) system as described in this section. The CCTV system will support the entry control system (at entrances and exits to the space), with time lapse video records that will allow Government employees to view and communicate remotely with visitors before allowing access to the Space. As determined by the Government the CCTV system shall provide unobstructed coverage of designated pedestrian entrances and exits. Technical review of the proposed system shall be coordinated with the Government security representative to the direction of the Contracting Officer, prior to installation. CCTV system testing and acceptance shall be conducted by the Government prior to occupancy.

APPENDIX C.2

The CCTV system shall comply with the Architectural Barriers Act, section F230.0. The Government will centrally monitor the CCTV system. Government specifications are available from the Lease Contracting Officer. CCTV system components which fail or require maintenance or which fail during testing should be serviced in accordance with the Security System Maintenance Criteria listed below.

Security System 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 preventive maintenance program for all security systems the Lessor has installed. Any critical component that becomes inoperable must be replaced or repaired by the Lessor within 5 business days. Critical components are those required to provide security (IDS, CCTV, access control, 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's providing guard service, the cost of which must be reimbursed by the Lessor.

INTRUSION DETECTION SYSTEMS (IDS)

**** IDS (LENEL/ACCESS CONTROL) INSTALLED BY THE LESSOR, MONITORED BY GOVERNMENT**

LESSOR PROVIDED DESIGN, INSTALLATION AND MAINTENANCE

The Lessor shall design, install and maintain an Intrusion Detection System (IDS) as described in this section. The Government requires an IDS, which will cover perimeter entry and exit doors, and operable ground-floor windows. Basic Security-in-Depth IDS components 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. Technical review of the proposed system shall be coordinated with the Government security representative, at the direction of the lease Contracting Officer, prior to installation. System testing and acceptance shall be conducted by the Government prior to occupancy.

Base Security-in-Depth IDS shall be connected to and monitored at a central station operated by the Department of Homeland Security Megacenter. Emergency notification lists shall be coordinated with the monitoring station to include all applicable Government and lessor points of contact. Monitoring shall be designed to facilitate a real-time detection of an incident and to coordinate an active response to an incident. The Lessor must complete the Megacenter Alarm Requirements (MAR) application process specified by the Government to meet the monitoring requirements for a functional IDS. Components which fail or require maintenance or which fail during testing shall be serviced in accordance with the Security System Maintenance Criteria listed below.

Security System 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 preventative maintenance program for all security systems the Lessor has installed. Any critical component that becomes inoperable must be replaced or repaired by the Lessor within 5 business days. Critical components are those required to provide security (IDS, CCV, access control, 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 specific time frame (e.g. temporary barrier to

APPENDIX C.2

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's providing guard service, the cost of which must be reimbursed by the Lessor.

DURESS ALARM

**** DURESS ALARMS (Computer base LynxKeyPro) Procurement of license Seats required, INSTALLED BY THE GOVERNMENT.**

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.

The Lessor, at the notice to proceed stage of the procurement, 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.

STRUCTURE

WINDOWS

SHATTER-RESISTANT WINDOW PROTECTION

The Lessor shall provide and install shatter-resistant material not 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%

THE ALTERNATIVE METHOD is for the Lessor to provide a window system that conforms to a minimum glazing performance condition of "3b" for a high protection level and a low hazard level. Window systems shall be certified as prescribed by WINARD PE 4.3 or later to GSA performance condition 3b (in accordance with the GSA Standard Test Method for Glazing and Window Systems Subject to Dynamic Loadings or Very Low Hazard (in accordance with ASTM F 1642, Standard Test Method for Glazing or Glazing Systems Subject to Air Blast Loading)) in response to air blast load of 4 psi/28 psi-msec.

If the Lessor chooses the Alternative Method, they shall provide a description of the shatter-resistant window system and provide certification from a licensed professional engineer that the system has offered meets the above standard. Prior to installation, this will be provided for evaluation by the Government, whose approval shall not be unreasonably withheld.

APPENDIX C.2

LOUVERS

Secure Accessible air intakes from tampering.

OPERATIONS AND ADMINISTRATION

LESSOR TO WORK WITH FACILITY SECURITY COMMITTEE (FSC) (SHELL)

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

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 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.

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:

APPENDIX C.2

- 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/>.