SECURITY REQUIREMENTS - FACILITY SECURITY LEVEL II

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

DEFINITIONS:

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 Information Technology rooms and sensitive documents areas. Sensitive areas are primarily housed within Government-controlled space.

REFERENCES:
VA Handbook 0730/4, Security and Law Enforcement, March 29, 2013

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

FACILITY ENTRANCES AND LOBBY

EMPLOYEE ACCESS CONTROL AT ENTRANCES

The Lessor shall provide electronic access control, with access card (HSPD-12 compliant Personal Identity Verification) and pin, for the entrance to this building. All Government employees, under this lease, shall be allowed access to the leased space. After hours is restricted to specific individuals.

COMMON AREAS, NON-PUBLIC, AND UTILITY AREAS.

PUBLIC RESTROOM ACCESS

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

SECURING CRITICAL AREAS

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. 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, telecommunications rooms.

VISITOR ACCESS CONTROL
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
The Government shall have a designated main entrance.

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

FORMAL KEY CONTROL PROGRAM
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

CONCENTRIC LEVELS OF CONTROL AND PROTECTION AS FOLLOWS:

- Fenced property perimeter with limited number of controlled and CCTV ID monitored entry points. **Provide perimeter fencing. The entire building and parking will be enclosed.** For this facility, 8-foot high fencing shall be used. Design fencing with due consideration for character and aesthetics of the building design and surrounding properties.
- Controlled perimeter access/entry points, with CCTV surveillance and intrusion detection
- Building perimeter with limited number of controlled entry points, including control hardware, intrusion detection and CCTV surveillance

    - Building entry will be limited to two locations, production staff entrance and the main public/admin staff entry. Both have controlled access.
- Segregation of authorized and unauthorized staff areas with door access controls.
- Restricted access to restricted areas by access control systems, CCTV surveillance monitors, detection alarms and forced-entry resistant construction. These may include computer server rooms.
    - Computer server room will be located no closer than twenty-five (25) feet in any direction to the main entrance and loading docks.
    - Entry door to server room to be equipped with motion-activated CCTV camera coverage on the egress side of the door.
- For spaces indicated as Sound Insulated and/or Secure Area, partition walls will extend from the floor to the deck above. Where Sound Insulated and/or Secure Area spaces are constructed using pre-fabricated modular construction, the modular construction shall be designed to prevent “up and over” access between adjacent spaces.

SITE CONSIDERATIONS

SITE ACCESS AND PARKING

Separate entrances to the site shall be provided for staff and visitors, emergency and service and delivery vehicles. Access roads for all vehicles shall allow for separate driveways to the building entrance, service yard or parking areas. Access roads from the entrances to parking for each vehicle type shall be separated, but may be connected for maintenance and emergency vehicles through gates controlled by access cards.

Vendors shall use the delivery vehicle entrance and service yard at the loading dock. Parking shall be provided for vendors in the service yard.

Where employees share access with visitors, the entrance to the employee parking shall be controlled by a card-actuated gate. Employee parking areas shall be monitored by CCTV.

When separation of types of traffic is not feasible, card-controlled access gates and other traffic separation measures shall be used.

BUILDING ENTRANCES AND EXITS

CMOP is NOT open to the public. Visitors to the facility should be restricted to a single entrance. The visitor entrance is to the main lobby of the facility. Visitor access shall include a screening vestibule with sufficient space. The production staff entrance shall be located independently of main entrance lobbies and be convenient to staff parking. Design access from drop-off to lobby to prevent a straight line of travel.

Public doors shall be capable of being remotely locked and unlocked from the reception desk in the main lobby. Secondary public entrance doors shall prevent unauthorized access. Staff entrance door hardware shall include either mechanical or electronic locks.

Means of egress doors that do not also function as entrances shall be provided with delayed action and alarmed emergency egress hardware. Delayed egress and alarmed exits shall comply with applicable codes and regulations. Means of egress shall not be obstructed by installation of security devices such as guard stations, screening equipment, or other security devices.

Access for Emergency Responders: The Fire Command Center (FCC) and secure house key knox box for emergency responders shall be located near an entrance door. The entrance shall be controlled and monitored by Security Surveillance Television (SSTV).

BUILDING SYSTEMS

HVAC systems: locate major mechanical equipment above the ground floor in an area not subject to flooding. All air intakes shall be located so that they are protected from external sources of contamination.

- Locate all outdoor air intakes a minimum of 100 feet [30.48 m] from areas where vehicles may be stopped with their engines running.
- Locate all outdoor air intakes a minimum of 30 feet [9.14 m] above finish grade or on roof away from the roof line. Provide protection, with bars or grills, for accessible vents greater than 96 square inches.

Emergency Generators: locate in a structure separate from the main building. The generator room shall not be located at an elevation subject to flooding at any time. The generator room shall not be located closer than 25 feet of a loading dock/receiving area or mailroom, and shall not be located beneath such facilities. Areaways and louver openings serving the generator shall not open to the service yard for the loading dock. Entrances from the exterior shall not open to the loading dock service yard.

SIGNAGE

POSTING OF SIGNAGE IDENTIFYING THE SPACE AS GOVERNMENTAL

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

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

LANDSCAPING

LANDSCAPING REQUIREMENTS

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

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.

HAZMAT STORAGE

If there is HAZMAT storage, Lessor shall locate it in a restricted area or storage container away 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.

SECURITY SYSTEMS

System design shall be capable of integrating with the existing VA CMOP Enterprise system with components that are compliant with HSPD-12. CMOP utilizes the Department of Homeland Security, Federal Protective Service MegaCenter, for third party system monitoring. CMOP will supply the cameras, video encoders, network switches, PoE injectors, and workstations as GFE. The Lessor is responsible for working with CMOP to develop the design as well as to provide pathways and cabling.

CLOSED CIRCUIT TELEVISION SYSTEM (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 recording, 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, at the direction of the Contracting Officer, prior to installation. CCTV system testing and acceptance shall be conducted by the Government prior to occupancy. 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 SYSTEM (IDS)

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.

The Lessor must provide an intrusion detection system (IDS)/burglar alarm system that is equivalent to the nationally standardized system implemented across the CMOP organization: Bosch/Radionics. The following are specific model numbers for the Bosch/Radionics control panels that are acceptable for use: Bosch/Radionics D1260 or better. The specific control panel model numbers that are acceptable for use are D9412GV4 or better and shall include: panel tamper switch, minimum 12 hour battery backup, communication module capable of interfacing with the Federal Protective Service MegaCenter monitoring services (reference current version of FPS Alarm Design and Installation Standards) and a cellular backup.

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 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.

PHYSICAL ACCESS CONTROL SYSTEM (PACS)

The Lessor shall include, but not be limited to: card readers, keypads, biometrics, electromagnetic locks and strikes, and electronic security management system (SMS). PACS devices shall be used for the purpose of controlling access and monitoring building entrances, sensitive areas, mission critical asset areas, and alarm conditions from an access control perspective. This includes maintaining control over defined areas such as site access points, parking lot areas, building perimeter, and interior areas that are monitored from a centralized SCC. PACS shall be able to be fully integrated with other security subsystems using direct hardwire or computer interface.

DURESS, SECURITY PHONES, AND INTERCOM SYSTEM (DSPI)

The DSPI system is used to provide security intercommunications for access control, emergency assistance, and identification of locations where persons under duress request a security response. All components of the DSPI shall be fully compatible and shall not require the addition of interface equipment or software upgrades to ensure a fully operational system. DSPI shall be fully integrated with other security subsystems.

STRUCTURE

WINDOWS

No windows are permitted below 40 feet on any exterior walls directly to rooms where pharmaceuticals are stored. Does not apply to administrative areas.

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 WINGARD 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 as offered meets the above standard. Prior to installation, this will be provided for evaluation by the Government, whose approval shall not be unreasonably withheld.

OPERATIONS AND ADMINISTRATION

LESSOR TO WORK WITH FACILITY SECURITY COMMITTEE (FSC)
The Lessor shall cooperate and work with the VA's Safety Committee throughout the term of the lease.

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 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.