INSTRUCTIONS TO LEASING SPECIALISTS: THE FOLLOWING BASELINE SPECIFICATIONS REPRESENT THE FULL EXTENT OF SECURITY SPECIFICATIONS AVAILABLE TO LEVEL II REQUIREMENTS UNDER THE ISC.

these are the minimum baseline requirements (mandatory). the LCO may include additional requirements, identified through programmatic or risk-based assessment.

The Listed level of protection (LOP) requirements may show lop of i-v, these LOPs have been designated by VA physical security specialist as the minimum lops they shall not be reduced without a wavier request approved by the national physical security committee.

|  |
| --- |
| **VA Security Requirements - Facility Security Level I** |

**THESE PARAGRAPHS CONTAIN ADDITIONAL SECURITY REQUIREMENTS, AND, UNLESS INDICATED OTHERWISE, ARE TO BE PRICED AS PART OF THE RENTAL RATE (SHELL) OR THE TENANT IMPROVEMENTS (TI). 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).

**SENSITIVE AREAS** – Sensitive areas include patient records and data, or any area that houses medical, mental, or other items or services that require patient privacy. Also included are police areas, pharmacy, medication rooms and OI&T spaces. Sensitive areas are primarily housed within 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 Department of Veterans Affairs (VA) 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 (LOP) 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 TI.

ADDITIONAL INFORMATION ON THE INTERAGENCY SECURITY COMMITTEE (ISC) RISK MANAGEMENT PROCESS IS AVAILABLE [HERE](https://www.cisa.gov/resources-tools/resources/isc-standard-risk-management-process).

Video Surveillance System (VSS) is widely used throughout industry and the federal government. It covers both analog and digital systems and is referenced in the Department of Homeland Security (DHS) Science and Technology Digital Video Quality Handbook.

**1.0 SITE SECURITY CRITERIA**

1. **IDENTIFICATION AS FEDERAL FACILITY: (SHELL)**

ISC LOP I: Signage identifying a facility as a federal facility shall be posted clearly and prominently to accommodate patient access in accordance with VA Signage Design Guide.

1. **LANDSCAPING: (SHELL)**

ISC LOP I: Minimize areas of concealment in and around facilities.

1. **PEDESTRIAN ACCESS TO SITE: (SHELL)**

ISC LOP I: No special measures required.

1. **VEHICLE ACCESS POINTS: (SHELL)**

ISC LOP I: No special measures required.

1. **SITE LIGHTING: (SHELL)**
   * + - ISC LOP III: Install exterior lighting at entrances, exits, parking lots, garages, VSS locations, and walkways from parking areas to entrances.

* All lighting design decisions should also support Crime Prevention Through Environmental Design (CPTED) goals and enhance environmental design factors (e.g., post-incident investigation, personnel identification, natural surveillance activities).
* Lighting should be sufficient to:
  + Illuminate potential areas of concealment.
  + Enhance the observation of security force patrols.
  + to ensure VSS video images can be used to identify a clear description of a person and any activity they may be engaged in; and
  + Provide for the safety of personnel moving between adjacent parking areas, streets, alleyways, and around the facility.
* For lighting assessment procedures and minimum lighting levels in other areas, refer to the Illuminating *Engineering Society (IES) Security Lighting Handbook G-1-03.*
* There should be no foliage blocking the light from illuminating the desired area.

1. **RESTRICTED AREAS OR SIGNIFICANT AREAS AND ASSETS: (SHELL)**

ISC LOP I: No special measures required.

The following three sections need to detail the parking requirements for the lease facility. The leasing specialist will have to work with the security specialist and tenant to establish requirements based on risk. Under Control of Parking a requirement to separate patient/visitor and staff parking areas should be added if desired. Under Authorized Parking a requirement to limit parking to authorized vehicles only should be added if desired. Under Vehicle Access to controlled parking a requirement to include gates to control parking can be added if necessary.

1. **SIGNAGE – SENSITIVE AREAS: (SHELL)**

ISC LOP I: No special measures required.

The following three sections need to detail the parking requirements for the lease facility. The leasing specialist will have to work with the security specialist and tenant to establish requirements based on risk. Under Control of Parking a requirement to separate patient/visitor and staff parking areas should be added if desired. Under Authorized Parking a requirement to limit parking to authorized vehicles only should be added if desired. Under Vehicle Access to controlled parking a requirement to include gates to control parking can be added if necessary.

1. **CONTROL OF PARKING: (SHELL)**

ISC LOP I: No special measures required.

1. **AUTHORIZED PARKING: (SHELL)**

ISC LOP I: No special measures required.

1. **VEHICLE ACCESS TO CONTROLLED PARKING: (SHELL)**

ISC LOP I: No special measures required.

1. **VEHICLE BARRIERS: (SHELL)**

ISC LOP I: No special measures required.

1. **VEHICLE SCREENING: (SHELL)**

ISC LOP I: No special measures required.

1. **PEDESTRIAN ACCESS TO CONTROLLED PARKING AREAS: (SHELL)**

ISC LOP I: No special measures required.

1. **HAZARDOUS MATERIALS (HAZMAT) STORAGE: (SHELL)**

ISC LOP I: No special measures required.

1. **RECEPTACLE AND CONTAINER PLACEMENT: (SHELL)**

ISC LOP I: No special measures required.

**2.0 STRUCTURE SECURITY CRITERIA**

1. **BLAST RESISTANCE-WINDOWS: (SHELL)**

ISC LOP I: No special measures required.

1. **BLAST RESISTANCE: FAÇADE AND STRUCTURE: (SHELL)**

ISC LOP II (SHELL):

**New Lease Construction**

Use construction materials which have inherent ductility, and which are better able to respond to load reversals (e.g., cast in place reinforced concrete column and steel construction).

* + All building materials and types acceptable under model building codes are allowed. Design detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry to adequately respond to the design loads.
  + **Unreinforced masonry is unacceptable**. Pre-stressed concrete is not very ductile and may not be appropriate where load reversals may occur.
  + Reference the current ISC DBT unless device size is superseded by an agency-specific threat assessment. Device location is the closest possible point to the setback with the DBT device.
  + All building components requiring blast resistance must be designed using established methods and approaches for determining dynamic loads, structural detailing, and dynamic structural response. The demands on the structure will be equal to the combined effects of dead, live, and blast loads. Blast loads or dynamic rebound may occur in directions opposed to typical gravity loads. Design and analysis approaches should be consistent with Unified Facilities Criteria (UFC) 3-340-02, “Structures to Resist the Effects of Accidental Explosions, with Change 2.” Response limits shall follow U.S. Army Corps of Engineers (USACE) PDC-TR 06-08, “Single Degree of Freedom Structural Response Limits for Antiterrorism Design.”

**Existing Facilities**

* **Unreinforced masonry is unacceptable**. Pre-stressed concrete is not very ductile and may not be appropriate where load reversals may occur.

1. **BLAST RESISTANCE: PROGRESSIVE COLLAPSE: (SHELL)**

ISC LOP I: No special measures required.

1. **BLAST RESISTANCE – UNDER BUILDING PARKING: (SHELL)**

ISC LOP I: No special measures required.

1. **BURGLARY RESISTANCE OF WINDOWS AND GLASS DOORS: (TI)**

ISC LOP II: All operable ground floor windows shall be locked and monitored via IDS.

1. **WALLS AND NON-WINDOW OPENINGS: (SHELL)**

ISC LOP I: Protect non-window openings such as mechanical vents and exposed plenums to resist forcible entry.

* + Forced entry resistance will be uniform around the perimeter and the façade of the building.
  + Interior walls of secure or restricted areas (IT Closets, Armory, Police Operations and Pharmacy) shall be monitored via IDS.

1. **WINDOWS IN CRITICAL AREAS- BALLISTIC PROTECTION: (SHELL)**

ISC LOP I: No special measures required.

1. **PROTECTION OF AIR INTAKES: (SHELL)**

ISC LOP I: Provide emergency shutdown, SIP, and evacuation procedures.

1. **ISOLATED VENTILATION SYSTEMS: (SHELL)**

ISC LOP I: No special requirements.

1. **HVAC CONTROL: (SHELL)**

ISC LOP I: Lessor shall develop written procedures for the emergency shutdown or exhaust of air handling systems.

* + A “one-step shutoff” is a mechanism that requires only a single action by an individual (e.g., engineer or security personnel) to initiate the immediate shut down of all air handling equipment in the building.

1. **CBR DETECTION TECHNOLOGY: (SHELL)**

ISC LOP I: No special measures required.

1. **BIOLOGICAL FILTRATION – GENERAL BUILDING: (SHELL)**

ISC LOP I: No special measures required.

1. **BIOLOGICAL FILTRATION – LOBBIES AND MAILROOMS: (SHELL)**

ISC LOP I: No special measures required.

1. **CHEMICAL FILTRATION: (SHELL)**

ISC LOP I: No special measures required.

1. **SECURITY OF VENTILATION EQUIPMENT AND CONTROLS: (SHELL)**

ISC LOP I: The lessor shall protect the system controls from unauthorized access.

* + Access to government space shall be managed by installing compliant Physical Access Control in compliance with OMB policy M-05-24, NIST SP-800-116-1, and all other applicable standards established by OMB, NIST, and the OCIO Council.
  + To ensure HVAC system operation cannot be disrupted by someone physically accessing the controls, HVAC equipment shall be located in a secure area with access limited to authorized staff.

1. **LOCATION OF UTILITIES AND FEEDERS: (SHELL)**

ISC LOP I: No special measures required.

1. **SEPARATION OF EMERGENCY AND NORMAL POWER DISTRIBUTION: (SHELL)**

ISC LOP I: No special measures required.

1. **EMERGENCY GENERATOR PROTECTION: (SHELL)**

ISC LOP I: If an emergency generator is used, secure against unauthorized access.

1. **PROTECTION OF WATER SUPPLY: (SHELL)**

ISC LOP I: No special measures required.

1. **BLAST RESISTANCE – INTERIOR PUBLIC SPACES: (SHELL)**

ISC LOP I: No special measures required.

1. **BLAST RESISTANCE – MAIL SCREENING AND RECEIVING LOCATIONS: (SHELL)**

ISC LOP I: No special measures required.

**3.0 FACILITY ENTRANCE SECURITY CRITERIA**

If the leased Space 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 leased Space 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. **BADGE IDENTIFICATION (ID) SYSTEM: (SHELL)**

ISC LOP I: No special measures required.

1. **REGULATORY SIGNAGE: (SHELL)**

ISC LOP II: Lessor shall post necessary regulatory, statutory, and/or site-specific signage per the VA Signage Design Guide.

1. **EMPLOYEE ACCESS CONTROL: (SHELL)**

ISC LOP II: Provide a means to secure employee entrance doors and to verify the identity of persons requesting access prior to allowing entry in the facility by physical or electronic means.

* + When it is determined an electronic Physical Access Control System (ePACS) is to be installed, procurement and installation must comply with OMB policy M-05-24, NIST SP-800-116-1, and all other applicable standards established by OMB, NIST, and the OCIO Council.

1. **VISITOR ACCESS CONTROL: (SHELL)**

ISC LOP II: Always require visitors (Lessor contracted maintenance personnel) to nonpublic areas be sponsored by a tenant and either approved for unescorted access or escorted at all times.

* + Entrances are open to the public during business hours.
  + The Government reserves the right to verify the identity of persons requesting access to the Government-controlled Space prior to allowing entry.

1. **OCCUPANT SCREENING: (SHELL)**

ISC LOP I: No special measures required.

1. **VISITOR SCREENING: (SHELL)**

ISC LOP I: No special measures required.

1. **BALLISTIC PROTECTION AT SCREENING LOCATIONS: (SHELL)**

ISC LOP I: No special measures required.

1. **LOBBY QUEUING: (SHELL)**

ISC LOP I: No special measures required.

1. **AFTER-HOURS ACCESS CONTROL: (SHELL)**

ISC LOP I: All employees, contractors, and visitors shall sign in and sign out electronically or on a building register after-hours.

* + All Government employees, under this lease, shall be allowed access to the leased space (including after-hours access).

1. **LIMIT BUILDING ENTRY POINTS: (SHELL)**

ISC LOP I: No special measures required.

1. **ENTRANCE CO-LOCATION: (SHELL)**

ISC LOP I: No special measures required.

1. **PERIMETER DOORS AND DOOR LOCKS: (SHELL)**

ISC LOP I: Secure perimeter doors with high-security mechanical locks.

1. **CONTROL OF KEYS AND ACCESS MEDIA: (SHELL)**

ISC LOP I: The Government reserves the right to implement a formal key control program. The Lessor shall have a means of electronically disabling lost or stolen access media.

1. **EMPLOYEE CONVENIENCE DOOR: (SHELL)**

ISC LOP I: No special measures required.

1. **EMERGENCY EXIT DOORS: (SHELL):**

ISC LOP I: Secure emergency exit doors using an automatic door closer and exit hardware that are compliant with NFPA Life Safety Code and applicable standards.

1. **DELAYED EGRESS: (SHELL)**

ISC LOP I: No special measures required.

**4.0 INTERIOR SECURITY CRITERIA**

1. **SPACE PLANNING: (SHELL)**

ISC LOP I: No special measures required.

1. **ACCESS TO NON-PUBLIC AREAS (PROVIDER AREAS): (TI)**

LOP I: Use signage to designate nonpublic areas and establish procedures to prevent unauthorized access.

1. **SECURITY OF CRITICAL AREAS (i.e., PHARMACY or TELECOM ROOMS): (TI)**

ISC LOP III: Install electronic access control, VSS and IDS to control and monitor access into critical areas such as pharmacy, Network Rooms/IT Closets, etc.

* + Access to government space shall be managed by installing compliant Physical Access Control in compliance with OMB policy M-05-24, NIST SP-800-116-1, and all other applicable standards established by OMB, NIST, and the OCIO Council.
  + For Pharmacy: Interior wall separating pharmacy from public area must meet 15-minute forced entry resistant construction and extend from slab to slap.

1. **BUILDING SYSTEMS AND ROOF ACCESS: (SHELL)**

ISC LOP II: Secure utility, mechanical, electrical, and telecom rooms, and access to interior space from the roof with high-security locks.

1. **PUBLICLY ACCESSIBLE RESTROOMS: (SHELL)**

ISC LOP I: Control access to public restrooms.

1. **PUBLICLY ACCESSIBLE RETAIL AND MIXED-USE SPACE: (SHELL)**

ISC LOP II: Accommodate publicly accessible retail and mixed uses through such means as separating entryways.

1. **INTERIOR WINDOWS: (TI)**

ISC LOP I: No special measures required.

**5.0 SECURITY SYSTEMS CRITERIA**

1. **VSS COVERAGE: (TI)**

ISC LOP II: Provide VSS coverage of personnel entrances and exits.

1. **VSS MONITORING AND RECORDING: (TI)**

ISC LOP II: Record CCTV views using a digital medium.

* + Firmware and software updates from the manufacturer should be installed as soon as possible to prevent any breach.
    - A chain of custody and written procedures for evidence retrieval must be developed (contact isfubgroup@tswg.gov for a publication on Best Practices for the Retrieval of Video Evidence from Digital VMS Systems or visit www.tswg.gov).
    - The need for disaster recovery and remote operational capability, including offsite storage of data, should be considered when designing the VSS.
  + The images shall be recorded at a minimum rate of 15 frames per second on digital media.
    - Motion recording with conditional refresh is recommended to reduce bandwidth and storage challenges. External entrance/exit cameras and any cameras covering significant areas or assets (identified during the risk assessment) should record at all times. Recorded images should be at the camera’s maximum resolution.
  + Edge recording capabilities should be considered when network bandwidth or network outages are a concern.
  + Storage:
    - Surveillance video must be stored for 90 days.

1. **SECURITY CONTROL CENTER: (SHELL)**

ISC LOP I: No special measures required.

1. **VSS SURVEILLANCE ADVISORY: (SHELL)**

ISC LOP I: When VSS is utilized, post signage at the entrance of the location.

* + Post signs at entrances to the site, facility, parking garages, etc., where VSS coverage exists.
  + Signs should be large enough to be noticed, placed in an easily seen location, and have both words and pictures indicating video surveillance is being conducted at the location.

1. **INTRUSION DETECTION SYSTEM (IDS) COVERAGE: (TI)**

ISC LOP II: Provide IDS on perimeter entry and exit doors and all ground-floor windows. Provide a separate IDS partition for all rooms where VA IT network equipment is kept. Provide a separate IDS partition for the police operations area when included in the program. Provide a separate IDS partition for the Armory when included in the program. Provide a separate IDS partition for the Pharmacy when included in the program. Provide a separate IDS partition for the Pharmacy Vault when included in the program.

* The Lessor shall design, install, and maintain the IDS system. Technical review of the proposed system shall be coordinated with the VA security representative, at the direction of the Lease Contracting Officer, prior to completion of the CDs, and prior to installation. System testing and acceptance shall be conducted by the VA prior to occupancy.
* UL 2050 Listed intrusion detection equipment is required. Initial installation should include validation (testing) of the entire system, including monitoring center notification and connected equipment.
* The following descriptions are provided as benchmarks in considering the appropriate system technologies. An access control system can serve as an IDS as long as it meets the IDS details listed here and has provisions for monitoring (see IDS Monitoring).
  + Entry Doors will have:
    - Magnetic switch; and
    - Alarm system keypad (at main employee entrance).
    - Motion Sensor coverage (passive infrared sensor (PIR), microwave, ultrasonic, or similar device).
  + Windows and other openings greater than 96 square inches:
    - Glass-break detector; and
    - Magnetic switches or shock sensors.
    - Non-opening windows should utilize glass break detectors and/or motion sensor coverage.
  + Installation Practices: No matter the system type listed above the following installation practices should be used:
    - All IDS devices should be on a supervised circuit.
    - End-of-line resistors for supervision must be placed in the individual sensor and not in the alarm panel.
    - Alarm panels should be in a locked tamper-proof container with a tamper switch.
    - Alarm panels should be located in a locked area that is only assessable to authorized individuals. Area should be protected by IDS.
    - External facility entrances and high-security applications should be designed in a multi-layered approach (e.g., doors that have magnetic or balanced magnetic switches should also be protected with a motion sensor).
    - Zoning – Each alarm sensor or alarm point should have its own zone. This will help with troubleshooting alarm points and response to alarms.
    - Double doors – Double doors or split doors should be zoned on each leaf, not both doors on one zone.
    - Cross zoning (the requirement of two or more sensors to be activated in a specific amount of time before activating an alarm) should be avoided.
    - Garage doors – Garage doors should have a sensor on each side to prevent the lifting on one side without an alarm.
    - Accessible external facility openings that are 96 square inches or more should be alarmed.
    - Door contacts should be installed on the opening side of the door and should not allow the door to open far enough to provide the ability to tamper with the contact inside the door without going into alarm.

1. **INTRUSION DETECTION SYSTEM (IDS) MONITORING:** **(SHELL)**

ISC LOP II: Lessor shall monitor at a central station with notification to law enforcement or security responders.

1. **DURESS ALARMS OR ASSISTANCE STATIONS: (TI)**

ISC LOP I, II: Implement duress procedures for emergency situations.

ISC LOP

* + required and documented.
  + Duress Alarm system and design will be approved by VA Police during design or prior to installation.

1. **SECURITY SYSTEM INTEGRITY: (SHELL)**

ISC LOP I: Secure alarm and physical access control panels, VSS components, controllers, and cabling against unauthorized access.

1. **SECURITY COMMUNICATIONS: (SHELL)**

ISC LOP I: No special measure required.

1. **BUILDING COMMUNICATION SYSTEM: (TI)**

ISC LOP I: Provide a communication system for security and emergency announcements.

1. **EMERGENCY POWER FOR SECURITY SYSTEMS: (SHELL)**

ISC LOP I: No special measures required.

1. **SECURITY SYSTEM TESTING: (SHELL)**

ISC LOP I: Lessor shall conduct security system performance testing annually and provide documentation to VA.

1. **SECURITY SYSTEM MAINTENANCE: (SHELL)**

ISC LOP I: Lessor shall implement a maintenance program for all security systems. Any critical component that becomes inoperable must be replaced or repaired within five business days.

* Failure by the Lessor to provide sufficient replacement measures within the timeframe identified may result in the VA providing guard service, the cost of which must be reimbursed by the Lessor.

**6.0 SECURITY OPERATIONS AND ADMINISTRATION**

1. **FACILITY SECURITY PLAN: (SHELL)**

Lessor shall develop a written Facility Security Plan in conjunction with VA that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades in accordance with the National Terrorism Advisory System. Plan shall be submitted to VA for review and approval prior to lease acceptance.

1. **PROTECTION OF CONSTRUCTION INFORMATION: (SHELL)**

ISC LOP I and II: No Special Measures Required

1. **SECURITY DURING CONSTRUCTION AND RENOVATION: (SHELL)**

ISC LOP II: Develop and implement a Construction Security Plan.

**7.0 CYBERSECURITY**

1. **FACILITY CYBERSECURITY REQUIREMENTS: (SHELL)**
2. 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).
3. 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.
4. Lessors are encouraged to put into place the following cyber protection measures to safeguard facilities and occupants:
5. 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>).
6. 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.
7. Encourage vendors of BACS to secure these devices and software through the following:
   * + 1. Develop and institute a proper Configuration Management Plan for the BACS devices and applications, so that the system can be supported.
       2. 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.
       3. 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.
       4. Close unnecessary open ports to secure against unprivileged access.
       5. 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>).

* + - 1. 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/entry/what-is-least-privilege>.
      2. 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.
      3. 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.
      4. 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).
      5. Discontinue the use of end of life (EOL) systems and use only applications/systems that are supported by the manufacturer.
      6. Operating Systems must be supported by the vendor for security updates (e.g., do not use Windows Server 2003).
      7. 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).
      8. 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.
      9. Systems should have proper system configuration hardening and align with Center for Internet Security [(CIS) benchmarks](https://www.cisecurity.org/cis-benchmarks/) or other industry recognized benchmarks. Additional information can be found at https://www.cisecurity.org/cis-benchmarks/.