THIS EXHIBIT PROVIDES THE INTERAGENCY SECURITY COMMITTEE (ISC) LEVELS OF PROTECTION (LOP) NECESSARY TO ACHIEVE A **FACILITY SECURITY LEVEL II (FSL II).** *(Note* ISC LOP II = FSL II = SHELL)*

OFFERERS ARE RESPONSIBLE FOR PROVIDING ALL ITEMS DESIGNATED AS "**SHELL**". THESE ITEMS WILL NOT BE PRICED.

ITEMS DESIGNAGED "TI" FOR TENANT IMPROVEMENT, SHALL BE PRICED AND NEGOTIATED AFTER AWARD, USING THE SECURITY UNIT PRICE LIST AND WITH INPUT FROM THE VA POLICE.

PRIOR TO AWARD A RISK ASSESSMENT SHALL BE COMPLETED. IF THE RISK ASSESSMENT DETERMINES THAT A GREATER THAN A LEVEL II LEVEL OF PROTECTION IS REQUIRED FOR SPECIFIC COUNTERMEASURES, THEN THE REQUIREMENTS WILL PRICED AS TENANT IMPROVEMENTS. THESE HIGHER LEVELS OF PROTECTION ARE IDENTIFIED BELOW WITH "(TI)".

THE SECURITY UNIT PRICE LIST WILL BE COMPLETED FOR EACH **TI** COUNTERMEASURE.

ADDITIONAL INFORMATION ON THE INTERAGENCY SECURITY COMMITTEE (ISC) RISK MANAGEMENT PROCESS IS AVAILABLE HERE: https://www.dhs.gov/interagency-security-committee

Must comply with VA Handbook 0730 and all updates:
https://www.va.gov/vapubs/search_action.cfm?formno=730&SortBy=Pub_Type_Desc

DEFINITIONS:
CRITICAL AREAS AND SYSTEMS - 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. 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 (DBT)

SENSITIVE AREAS – Sensitive areas include patient care spaces, or any area that houses medical, mental, or other services that require patient privacy. Sensitive areas are primarily housed within Government-controlled space.

VSS – Video Surveillance Systems 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 QualityHandbook.1

SITE SECURITY CRITERIA

IDENTIFICATION AS FEDERAL FACILITY: (SHELL)

Signage identifying a facility as a Federal facility should only be posted when necessary to achieve the mission of the tenants, or when the facility is readily identified or well-known as a government facility based on the nature of public contact or other operations.

LANDSCAPING: (SHELL)

- Minimize areas of concealment in and around facilities. Establish a clear zone around barriers or fences and restrict landscaping from obstructing views of the security force and VSS; or interfering with lighting or Intrusion Detection System (IDS).

PEDESTRIAN ACCESS TO SITE: (SHELL) No special measures required.

VEHICLE ACCESS POINTS: (SHELL): No special measures required.

SITE LIGHTING: (SHELL)

- 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 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 and VSS; and
    - Provide for the safety of personnel moving between adjacent parking areas, streets, alleyways, and around the facility.
- Sufficient lighting must be provided to ensure VSS video images can be used to identify a clear description of a person and any activity they may be engaged in.
- <u>Maintained Illumination Level (lux).</u>
    - Horizontal Illumination:
        - Covered parking areas – 10
        - Roof and surface parking area – 2.5
        - Stairwells, elevator lobbies – 20
        - Uniformity ratio (average: min) – 4:1
        - Uniformity ratio (maximum: min) – 15:1
    - Vertical Illumination:
        - Covered parking areas – 5
        - Roof and surface parking area – 2.5
        - Stairwells, elevator lobbies – 10
- For lighting assessment procedures and minimum lighting levels in other areas, refer to the *Illuminating Engineering Society (IES) Security Lighting Handbook G-1-03.*

- For prescriptive lighting requirements, please refer to the *GSA PBS-P100, Facilities Standards for the Public Buildings Service, issued April 2017.*

RESTRICTED AREAS OR SIGNIFICANT AREAS AND ASSETS: (SHELL)

- Use trees, hedges, berms, or any combination of these elements to create buffer zones to separate public areas and other functions.
- Restricted areas or significant areas and assets include but are not limited to:
  - Utility connections;
  - Loading docks;
  - Emergency power supplies;
  - Hazardous-materials storage;
  - HVAC; and
  - Exterior access to critical rooms (e.g., telecom and information technology (IT) resources).

SIGNAGE – SENSITIVE AREAS: (SHELL)

- Prohibit signs that identify sensitive areas, unless required by other standards/codes.
- Avoid marking outside locations such as air intakes, fuel supply valves, gas or power distribution locations, evacuation assembly areas, etc.

CONTROL OF PARKING: No special measures required.

AUTHORIZED PARKING: (SHELL):

- Visitor parking should be located as far from the facility as practical. Assigned employee and government parking may be used to establish a "buffer zone."

VEHICLE ACCESS TO CONTROLLED PARKING:

- LEVEL II (SHELL): Designate employee and visitor parking areas.
- LEVEL III (TI): Install enclosed fence area with vehicle gates to limit access to staff parking and/or GOV parking areas.

VEHICLE BARRIERS:

- ISC LOP Level III (TI): Provide vehicle barriers to protect pedestrian entrances from penetration by a vehicle meeting the Interagency Security Committee Design Based Threat, 2018 Edition.
  - The type and size should be utilized to support the kinetic energy calculations < Kinetic Energy (KE) = 0.5 * Mass (m) Velocity (v)2 > necessary to determine the minimum crash

rating necessary for protection. Practitioners should utilize locally developed threat information indicating a deviation from the DBT vehicle characteristics.

- Reduce Straight Avenues of Approach for Vehicle Paths:
  - Use a vehicle velocity that considers the angle of incidence in conjunction with the distance between the perimeter and the point at which a vehicle likely would be able to start a run at the perimeter. Design site circulation to prevent high-speed approaches by vehicles and use barriers or offset vehicle entrances from the direction of a vehicle's approach to force a reduction in speed. Appropriate measures for the barrier system may include walls, fences, trenches, berms, ponds and water basins, boulders, plantings, trees, static barriers, sculptures, and street furniture.
- Maximum clear spacing between vehicle barriers is four feet. Minimum barrier height is 30 inches. Agency standards may require additional height.
- Barriers must be certified to meet performance requirements for vehicle size and speed specific to the facility under ASTM F 2656-18, Standard Test Method for Crash Testing of Vehicle Security Barriers,

VEHICLE SCREEENING: No special measures required

PEDESTRIAN ACCESS TO CONTROLLED PARKING AREAS:

- LEVEL II (SHELL): Minimize areas of concealment in and around parking areas.
- LEVEL III (TI): Monitor pedestrian access to parking areas utilizing security force and/or VSS.

HAZARDOUS MATERIALS (HAZMAT) STORAGE:

- LEVEL II (SHELL): Locate HAZMAT storage in a restricted area away from loading docks, entrances, and uncontrolled parking.

RECEPTACLE AND CONTAINER PLACEMENT:

- LEVEL II (SHELL): Position trash containers, mailboxes, donation/recycle containers, vending machines, etc., 25 feet away from building exterior and entry points, or implement blast containment measures to mitigate an explosion.

STRUCTURAL SECURITY CRITERIA

BLAST RESISTANCE-WINDOWS:

- LEVEL III (TI): Utilize acceptable fragment retention film or preferred glazing systems to reduce the glass fragmentation hazard.

- Acceptable Fragment Retention Film: In applications requiring retention film, film shall meet or exceed the following physical 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%
  - In most cases, a 7-mil retention film will be sufficient to meet the minimum physical properties
- Preferred glazing systems include: thermally tempered heat-strengthened or annealed glass with a fragment retention film installed on the interior surface and attached to the frame; or laminated thermally tempered, laminated heat-strengthened, or laminated annealed glass.
  - New glazing systems at the Low or higher LOPs shall be designed with a minimum ½-inch bite.
- Unacceptable systems include untreated monolithic annealed or heat-strengthened glass and wire glass.
- For new construction projects, a blast engineer with formal training in structural dynamics and demonstrated experience with accepted design practices for blast resistant design must be included as a member of the design team.

BLAST RESISTANCE: FAÇADE AND STRUCTURE:

- LEVEL II (SHELL): **EXISTING BUILDING**: Ensure building constructed with materials which have inherent ductility and which are better able to respond to load reversals (e.g., cast in place reinforced concrete column 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.

- ISC LOP Level IV: (TI): **NEW CONSTRUCTION**: Use a combination of setback, site planning, façade hardening, and structural measures to provide a medium level of façade protection.
  - Medium Façade Protection: Moderate damage, repairable. The facility will sustain a significant degree of damage, but the structure should be reusable. Assets may be damaged. Building elements other than major structural members may require replacement.

- For new construction projects a blast engineer with formal training in structural dynamics and demonstrated experience with accepted design practices for blast-resistant design must be included as a member of the design team.
- 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."

BLAST RESISTANCE: PROGRESSIVE COLLAPSE:

- LEVEL II: (SHELL) Given the low occupancy and risk level associated with these types of facilities, progressive collapse design is not required for FSL I and II, regardless of the number of floors.

BLAST RESISTANCE – UNDER BUILDING PARKING: Under building parking is highly discouraged. However, if under building parking is required; the Lessor will ensure access to under building parking is limited with the Lessors guarantee that all parking under the structure will be controlled through active screening or another access control method to ensure only authorized, vetted personnel may park under the building. No unscreened public parking access will be allowed under VA leased space.

- LEVEL II (SHELL): 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 construction).

BURGLARY RESISTANCE OF WINDOWS AND GLASS DOORS:

- ISC LOP Level II (SHELL): All operable ground floor windows shall be locked and monitored via IDS.
  - The degree of penetration resistance should be commensurate with the delay necessary to protect assets while security and law enforcement personnel are notified and respond. Additional solutions may include burglary-resistant bars, wire mesh window systems, pin, epoxy, film, laminate, etc.

WALLS AND NON-WINDOW OPENINGS:

- ISC LOP Level III (TI): 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.
- Exterior non-window openings (e.g., vents) greater than 96 square inches in perimeter walls should be secured with grills, bars, and IDS.
- Interior walls of secure or restricted areas (IT Closets, Pharmacy) should be checked for penetration via the plenum and secured via grills, bars, mesh etc., and monitored via IDS when necessary.

WINDOWS IN CTRICIAL AREAS- BALLISTIC PROTECTION:

- LEVEL II (SHELL): No special measures required.

PROTECTION OF AIR INTAKES:

- LEVEL II (SHELL): Secure accessible air intake grilles from tampering or removal.

ISOLATED VENTILATION SYSTEMS:

- LEVEL II (SHELL): No special requirements

HVAC CONTROL:

- LEVEL II (SHELL): 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.

CBR DETECTION TECHNOLOGY:

- LEVEL II: (SHELL): No special measures required.

BIOLOGICAL FILTRATION – GENERAL BUILDING:

- LEVEL II (SHELL): No special measures required

BIOLOGICAL FILTRATION – LOBBIES AND MAILROOMS:

- LEVEL II (SHELL): No special measures required.

CHEMICAL FILTRATION:

- LEVEL II: (SHELL): No special measures required.

SECURITY OF VENTILATION EQUIPMENT AND CONTROLS:

- LEVEL II: (SHELL): 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.

LOCATION OF UTILITIES AND FEEDERS:

- LEVEL II: (SHELL): No special measures required.

SEPARATION OF EMERGENCY AND NORMAL POWER DISTRIBUTION:

- LEVEL II: (SHELL): No special measures required.

EMERGENCY GENERATOR PROTECTION:

- LEVEL II: (SHELL): If an emergency generator is used, secure against unauthorized access and locate the emergency generator and fuel tank at least 25 feet away from loading docks, entrances, and parking, or implement standoff, hardening, and venting methods to protect utilities from the DBT at these locations.
    - If the emergency generator is installed outdoors at grade, it should be protected by perimeter walls and locked entrances. The generator should not be located in any areas that are prone to flooding.
    - More secure locations include the roof, protected grade level, and protected interior areas. VSS, electronic Physical Access Control, and IDS coverage should be utilized.
    - Provisions for securing any refueling and shutoff valves in fuel lines within or in close proximity to the building must be addressed.

PROTECTION OF WATER SUPPLY:

- LEVEL II (SHELL): Secure handles, control mechanisms, and service connections at onsite publicly accessible locations with locks or other anti-tamper devices.

FACILITY ENTRANCE 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**.

REGULATORY SIGNAGE:

- LEVEL II: (SHELL): Post necessary regulatory, statutory, and/or site-specific signage.

EMPLOYEE ACCESS CONTROL:

- LEVEL II (SHELL): Provide a means to secure employee entrance doors 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.

VISITOR ACCESS CONTROL:

- LEVEL II (SHELL): Always require visitors to nonpublic areas be sponsored by a tenant and either approved for unescorted access or always escorted.

LIMIT BUILDING ENTRY POINTS:

- LEVEL II (SHELL): No special measures required

ENTRANCE CO-LOCATION: (SHELL):

- No special measures required.

PERIMETER DOORS AND DOOR LOCKS:

- LEVEL II: (SHELL): Secure government space perimeter doors with non-removable hinges and high-security mechanical or electronic locks.
    - 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.
    - Hinge pins located on the unsecured side of perimeter and critical interior doors must be designed to preclude door removal. Ensure magnetic locks have at least 1,200 pounds of shear holding power.
    - Electric strikes must meet all specifications of UL Standard 1034, Burglary-Resistant Electric Locking Mechanisms. For more information on electric strikes, refer to American National Standards Institute (ANSI) A156.25.
    - Door strikes should not allow the dead latch to be in the fully extended position when the door is closed.
    - Entrance Doors shall be capable of being remotely locked and unlocked from the reception desk or other designated position

- Glass for entrance and egress doors shall have shatter-resistant material not less than 0.18 millimeters (7 mil) thick– 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%

CONTROL OF KEYS AND ACCESS MEDIA: (SHELL):

- Implement a formal key control program and electronically disable lost or stolen access media.

EMPLOYEE CONVIENANCE DOOR:

- LEVEL III (TI): The Lessor shall ensure staff entrances are located independently of main entrance lobbies and be convenient to staff parking.
    - Provide electronic access control for employee entry doors without a security force post (including after-hours access) in conjunction with VSS coverage.

EMERGENCY EXIT DOORS: (SHELL):

- Secure emergency exit doors using an automatic door closer and exit hardware that are compliant with applicable life safety codes and standards. Monitor all emergency exits via visual, electronic, or audible means.

DELAYED EGRESS: (SHELL):

- No special measures required.

INTERIOR SECURITY CRITERIA

SPACE PLANNING:

- LEVEL II (SHELL): No special measures required

ACCESS TO NON-PUBLIC/PROVIDER AREAS:

- Level IV: (TI): Use signage, walls, IDS, and electronic access control force to establish physical boundaries to control access to non-public areas such as exam rooms and provider offices.
    - The Lessor will create a protected partition between the leased space lobby and the non-public provider area. A combination of walls and doors will be used.

- The doors leading to the non-public area will meet the same specifications as the perimeter. The doors will have electronic locks to allow escorted visitors into the non-public space.

SECURITY OF CRITICAL AREAS SUCH AS PHARMACY OR NETWORK ROOMS:

- LEVEL III (TI): 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.
  - Validate additional requirements with VA Police during design.

BUILDING SYSTEMS AND ROOF ACCESS:

- LEVEL II (SHELL): Secure utility, mechanical, electrical, and telecom rooms, and access to interior space from the roof with high-security locks.

PUBLICALLY ACCESSIBLE RESTROOMS:

- LEVEL II (SHELL): Control access to public restrooms

PUBLICLY ACCESSIBLE RETAIL AND MIXED-USE SPACE:

- LEVEL II (SHELL): Accommodate publicly accessible retail and mixed-use space through such means as separating entryways.

BLAST RESISTANCE – INTERIOR PUBLIC SPACES

- LEVEL II (SHELL): Certify that construction materials were or will be used which have inherent ductility and which are better able to respond to load reversals (e.g., cast in place reinforced concrete column construction).

BLAST RESISTANCE – MAIL SCREENING AND RECEIVING LOCATION:

- LEVEL II (SHELL): Certify that construction materials were or will be used which have inherent ductility and which are better able to respond to load reversals (e.g., cast in place reinforced concrete column construction).

INTERIOR WINDOWS:

- LEVEL II: (SHELL): No special measures required.

SECURITY SYSTEMS CRITERIA

VSS COVERAGE:

- LEVEL III(TI): Provide VSS coverage of personnel entrances and exits, parking lots, loading docks, and lobbies and other areas designed by VA Police.
    - VA Police will designate a purpose and goal for each security camera installed and verify/test that the VSS is designed to meet the physical security needs of the space and occupants.

VSS MONITORING AND RECORDING:

- LEVEL II (SHELL): 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.
    - When possible, 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:
        - According to the NARA General Records Schedule (GRS) 5.6: Security Records, surveillance video must be stored for 30 days (https://www.archives.gov/files/records-mgmt/grs/grs05-6.pdf).
        - Longer retention is authorized if required for business use. If less than 30 days of video images are to be kept, then a waiver should be granted from NARA utilizing SF 115.

SECURITY CONTROL CENTER:

- LEVEL II (SHELL): No special measures required

VSS SURVEILLANCE ADVISORY:

- LEVEL II: (SHELL): 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.

INTRUSTION DETECTION SYSTEM (IDS) COVERAGE:

- LEVEL II (SHELL): Provide IDS on perimeter entry and exit doors and all ground-floor windows.
- UL 2050 Listed intrusion detection equipment is strongly recommended. 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;
        - Alarm system keypad (at main employee entrance); and
        - 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.

INTRUSTION DETECTION SYSTEM (IDS) MONITORING:

- LEVEL II (SHELL): Monitor at a central station with notification to law enforcement or security responders.

DURESS ALARMS OR ASSISTANCE STATIONS:

- LEVEL III (TI): Provide duress buttons or call buttons at security force posts and sensitive public contact areas.
  - Duress devices shall be concealed from the public and shall annunciate for an immediate response.
  - Duress buttons should be tested monthly by the occupants of the facility. If batteries are utilized to power the alarm, the batteries should be replaced yearly and documented.
  - Duress Alarm system and design will be approved by VA Police during design or prior to installation.

BUILDING COMMUNICATON SYSTEM:

- LEVEL II (SHELL): No special measures required.

EMERGENCY POWER FOR SECURITY SYSTEMS:

- LEVEL II (SHELL): No special measures required.

SECURITY SYSTEM TESTING: (SHELL):

- Conduct security system performance testing annually and provide documentation.

SECURITY SYSTEM MAINTENANCE:

- LEVEL II (SHELL): Implement a maintenance program for all security systems. Any critical component that becomes inoperable must be replaced or repaired within five business days.

SECURITY OPERATIONS AND ADMINISTRATION

FACILITY SECURITY PLAN: (SHELL):

- Develop a written Facility Security Plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades in accordance with the National Terrorism Advisory System.

SECURITY DURIGN CONSTRUCTION AND RENOVATION (SHELL):

- Develop and implement a Construction Security Plan.

PROTECTION OF CONSTRUCTION INFORMATION: (SHELL):

- Limit access to construction documents to those persons with an established need-to- know.