7 Structural System

7.0 SCOPE

This chapter provides requirements for blast resistant structures and includes requirements for the prevention of progressive collapse and the hardening of critical columns. All building components requiring blast resistance must be designed using established methods and approaches for determining dynamic loads, structural detailing, and dynamic structural response. Alternative analysis and mitigation methods are permitted, provided that the performance level is attained.

While structural hardening makes the structure resistant to a specific threat, design to resist progressive collapse increases the robustness of the structure to an undefined event. This threat independent approach provides redundant load paths, ductility, and continuity. Designers may apply static and/or dynamic methods of analysis to demonstrate compliance with this requirement.

These requirements are in addition to the requirements for conventional structural design, including the provisions for hurricane, earthquake, and any other extreme loading condition required by code. The magnitude of GP1, GP2, W1, and W2 are defined in the *Physical Security Design Standards Data Definitions* that shall be stored separate from this document.

The minimum physical requirements for the construction of active and passive vehicle barriers are also included in this chapter.

Connecting corridor concourse and bridges and freestanding greenhouses shall be exempt from the requirements of Chapters 6 and 7. Physical security requirements for temporary buildings shall be determined on a case by case basis by the security staff having cognizance.

7.1 BLAST RESISTANCE

Structures shall be constructed to withstand the actual pressures and corresponding impulses produced by the design level vehicle threat (W2) located at the stand-off distance and the design level satchel threat (W1) that may be delivered to loading docks, mailrooms, lobbies, and below grade parking garages prior to screening. The design shall provide a level of protection for which progressive collapse will not occur; the building damage will be economically repairable and the space in and around damaged area can be used and will be fully functional after cleanup and repairs.

7.1.1 Priority for Protection

The priority for blast resistance shall be given to critical elements that are essential to mitigating progressive collapse. Designs of secondary structural elements, primary non-structural elements, and secondary non-structural elements shall minimize injury and damage. The priority depends on the relative importance of structural or non-structural elements in the following order.

7.1.1.1 Primary structure: Primary structural elements are the essential parts of the building's resistance to catastrophic failure, including columns, girders, roof beams, and the main lateral resistance system.

7.1.1.2 Secondary structure: Secondary structural elements are all other load bearing members, such as floor beams and slabs.

7.1.1.3 Primary non-structural: Primary non-structural elements and their attachments are essential for life safety systems or elements that can cause substantial injury if failure occurs, including ceilings or heavy suspended mechanical units.

7.1.1.4 Secondary non-structural: Secondary non-structural elements are all elements not covered in primary non-structural elements, such as partitions, furniture, and light fixtures.

7.1.2 Existing Facility – Blast Resistance

No additional physical security requirements.

7.2 PROGRESSIVE COLLAPSE

Structures shall be designed to minimize the potential for progressive collapse using the Alternate Path Method, which requires the structure to withstand the threat independent

removal of any exterior column, one at a time, without precipitating a disproportionate extent of damage. Structures shall develop peripheral, internal, and vertical tie forces by providing continuous reinforcement and ductile detailing. Consideration shall be given to ductile moment resisting frame lateral systems at the exterior of the building. Analytical methods for demonstrating a structure's resistance to progressive collapse shall conform to U.S. Government (USG) guidelines, specifically, *Design of Buildings to Resist Progressive Collapse*, UFC 4-023-03. All exterior columns shall be designed to prevent progressive collapse.

7.2.1 Existing Facility – Progressive Collapse

No additional physical security requirements.

7.3 COLUMN PROTECTION

Columns exposed to blast loading shall be hardened or isolated to resist the effects of the design level vehicle threat (W2) located at the stand-off distance and the design level satchel threat (W1) that may be delivered to loading docks, mailrooms, lobbies, and below grade parking prior to screening. The design shall provide a level of protection for which progressive collapse will not occur; the building damage will be economically repairable and the space in and around damaged area can be used and will be fully functional after cleanup and repairs.

7.3.1 Existing Facility – Column Protection

No additional physical security requirements.

7.4 ANTI-RAM RESISTANCE

7.4.1 Vehicle Barriers

Both active and passive barriers shall provide an anti-ram resistance capable of stopping a 4,000 pound (1,800 Kg) vehicle at the speed to be interdicted. The speed determining the appropriate kinetic energy resistance shall be 30 miles per hour (48 Km/Hr). (See also Chapter 3, Section 3.4 Vehicle Barriers.)

7.4.1.1 Testing: Performance of anti-ram element shall be demonstrated by means of impact testing or detailed finite element analysis of the vehicle impact.

7.4.1.2 Active barriers: Active barriers shall be hydraulic wedges, bollards, beams, drop arms, or sliding gates.

7.4.1.3 Passive barriers: Passive barriers shall be walls, stationary bollards, cables, or combination of landscape and hardscape that achieves the required anti-ram resistance.

7.4.2 Existing Facility – Anti-ram Resistance

The requirements of section 7.4.1 shall apply.

7.5 CALCULATION METHODS

All blast design and analysis, whether for new or existing construction, shall be performed in accordance with accepted methods of structural dynamics.

7.5.1 Design and Detailing

The performance of structures in response to blast loading is highly dynamic and often inelastic. Design and detailing of these structures shall therefore be based on analytical methods that accurately represent the loads and response. Explosive test data, developed by an experienced testing facility approved by the USG, may be used to supplement the analytical methods where a direct analytical representation is not feasible.

7.5.2 Blast Loading

Blast loads shall typically be developed using the semi-empirical relations of TM5-855 (CONWEP); however, where near contact detonations are considered, Computational Fluid Dynamics (CFD) methods may be required.

7.5.3 Dynamic Response

Dynamic structural response analyses shall be performed using either empirical data developed by an approved USG testing laboratory, simplified Single-Degree-of-Freedom (SDOF) analytical methods, or advanced Finite Element Methods (FEM). Where simplified SDOF methods are used, the performance criteria shall be in accordance with established standards of practice developed by the USG. Where advanced FEM methods are used, the performance shall be demonstrated through interpretation of the calculated results.

8 Utilities and Building Services

8.0 SCOPE

This chapter describes criteria for site utility entrances (services), on-site utility distribution, and building services. Utility systems include but are not limited to, potable and industrial water, fire protection water, sanitary sewer, fuels, steam, chilled water, electrical power, and telecommunications. Site utility entrances may include utility-owned service and metering equipment. Utility services shall be designed in accordance with VA Design Manuals including the Electrical, HVAC, Plumbing, Fire Protection, Outside Steam Distribution, and Sanitary Design Manuals. In addition, utilities, equipment, and services required to keep a mission critical facility in operation shall not be located at an elevation subject to flooding at any time. Throughout this section where it is mandatory that construction or equipment be in an area that is not subject to flooding refer to the FEMA flood map information available at http://www.fema.gov/business/nfip/fmapinfo.shtm.

8.1 UTILITY ENTRANCES

8.1.1 Mechanical

8.1.1.1 Alternate connections for steam and chilled water: Provide means for the connection of an alternate source, such as a mobile boiler or chiller.

8.1.1.2 Water service: Two independent sources are required. This may consist of two independent services from an off-site water provider or a single source from an off-site provider and an on-site water well with treatment means. See section 8.4 for on-site water storage requirements.

8.1.1.3 Protection of utility-owned service equipment: Above-ground utility-owned service equipment shall be located within a building envelope when

possible or be protected by limited-access masonry enclosures and be located a minimum of 100 feet (31 m) in all directions from vulnerable areas. Coordinate with the serving utility.

8.1.2 Electrical

8.1.2.1 Number of services: Two utility services are required.

8.1.2.2 Separation of services: Electric service feeders shall be underground, located away from other utility services, and located away from vulnerable areas. Services shall be separated by a minimum distance of 100 feet (31 m).

8.1.2.3 Protection of utility-owned service equipment: Utility-owned service and metering equipment shall be located within a building envelope when possible or be protected by limited-access masonry enclosures and be located a minimum of 100 feet (31 m) in all directions from vulnerable areas. Coordinate with the serving utility.

8.1.3 Telecommunications

8.1.3.1 Number of services: Two services from each telecommunications provider are required, preferably with delivery from different central offices or sites.

8.1.3.2 Separation of services: Telecommunications cable pathways shall be underground, located away from other utility services, and located away from vulnerable areas. Where more than one service is obtained, services shall be separated by a minimum distance of 100 feet (31 m).

8.1.3.3 Redundant service paths to DEMARC: The DEMARC is the separation point between utility-owned and VA-owned equipment. Telecommunications cable pathways must be designed to provide redundant services to the DEMARC from the street or property line where the interface with the service provider takes place. Redundant conduit paths shall be separated by a minimum distance of 100 feet (31 m).

8.1.4 Existing Facility – Utility Entrances

8.1.4.1 Existing facilities shall comply with the redundancy requirements of section 8.1.

8.1.4.2 Relocate existing mechanical and electrical equipment to comply with section 8.1. Where existing equipment cannot be relocated to within an existing building envelope, protect the equipment with screen walls or barriers that comply with Chapters 6 and 7.

8.2 SITE DISTRIBUTION

8.2.1 Mechanical

8.2.1.1 Steam, chilled water, water, and fuel system distribution: Distribution systems shall be underground and shall be looped systems, such that an interruption at any one point can be isolated and service maintained to the facility. Piped utility systems, in particular fuel systems, shall include enhanced capability to resist external forces. Steam and condensate piping shall be installed above the flood zone.

8.2.1.2 Separation of sanitary sewer and storm drain systems: Sanitary sewer and storm drain systems shall be separate.

8.2.1.3 Manhole and handhole covers: Manholes and handholes shall be equipped with lockable covers.

8.2.2 Electrical

8.2.2.1 Separation of feeders: Feeders that form a primary selective pair shall not be located closer than 100 feet (31 m) to each other, shall be encased in concrete, and shall enter served buildings at different locations. Feeder entry points will maintain a minimum distance of 100 feet (31 m) or greater in all directions from areas such as loading docks or similar defined areas of vulnerability.

8.2.2.2 Location of distribution equipment: All electrical distribution components, such as medium- and low-voltage switchgear and transformers, shall be located within a building envelope.

8.2.2.3 Manhole and handhole covers: Manholes and handholes shall be equipped with lockable covers.

8.2.3 Telecommunications

8.2.3.1 Telecommunications systems distribution: An underground ring topology shall be used for telecommunications cable pathways that connect multiple buildings. This will provide two underground pathways for telecommunications services to all buildings. Sizing of conduits shall be based on a 40% fill, and there will be a minimum of two spare four inch (100 mm) conduits between buildings. Conduits shall be encased in concrete. Distance between manholes or handholes shall not be greater than 400 feet (122 m).

8.2.3.2 Separation of pathways: Ring distribution pathways shall not be located closer than 100 feet (31 m) to each other. Pathways shall enter served buildings at different locations and shall not be exposed on the building exterior. Quantity and size of conduits shall be determined by site design. Telecommunications entry points shall maintain a minimum distance of 100 feet (31 m) or greater in all directions from areas such as loading docks or similar defined areas of vulnerability.

8.2.3.3 Location of telecommunications equipment: All telecommunications components other than inter-building cabling shall be located within the building envelope.

8.2.3.4 Manhole and handhole covers: Manholes and handholes shall be equipped with lockable covers.

8.2.4 Existing Facility – Site Distribution

8.2.4.1 Existing facilities shall provide emergency connections for electricity, steam, and all water systems.

8.2.4.2 Where existing outdoor above-ground distribution equipment cannot be relocated to within an existing building envelope, protect the equipment with screen walls or barriers that comply with Chapters 6 and 7.

8.3 ENERGY CENTER

8.3.1 Requirements

The energy center contains utility production and distribution equipment, as well as incoming services from off-site utility providers, and is responsible for providing utility services during normal operating conditions as well as during and after natural and manmade disaster events. The utility services feeding into the energy center include but may not be limited to electricity, potable water, natural gas, and fuel oil. The utilities feeding to and/or from the energy center and the mission critical facility shall be electricity, steam and condensate return, and chilled water supply and return.

8.3.2 Sustained Service

The energy center shall sustain utility services for a minimum time period of four (4) days.

8.3.3 Separation from Other Buildings

Refer to Chapters 3 and 4 for separation distances between the energy center and other mission critical buildings and the property boundary.

8.3.4 Stand-by Power

Paralleled diesel generators shall provide complete stand-by power to the energy center and may provide full stand-by power to other buildings.

8.3.5 Long-replacement-time Equipment

For equipment that has a long replacement time, provide for additional physical protection and/or installation of redundant equipment or connections that will alleviate extended shutdown time.

8.3.6 Existing Facility – Energy Center

No additional physical security requirements.

8.4 WATER AND FUEL STORAGE

8.4.1 Requirements

Storage shall be provided for potable and industrial water, fire protection, wastewater, and contaminated water, and fuels for use during the period under which off-site utilities are unavailable. At a minimum, water and generator fuel storage shall support 4 days of operation, boiler fuel storage shall support 10 January days of operation.

8.4.2 Storage Volume Criteria

8.4.2.1 Water: Minimum criteria to be used in determining storage requirements are:

- Potable water: 40 gal/day/person.
- Industrial water: Industrial water requirements include cooling tower and boiler make-up water. A peak summer and winter consumption shall be normalized over a 7 day period. The profile with the greatest consumption shall be used to determine industrial water storage requirements.
- Wastewater retention: 40 gal/day/person.
- Fire protection water: Minimum of 120,000 gallons, and when unfavorable conditions occur, minimum fire demand shall not be less than 180,000 gallons. NFPA 1 requirements apply in all cases.
- Contaminated water: Minimum 5,000 gallons of holding capacity for water contaminated with hazardous material(s).

8.4.2.2 Generator Fuel: A peak summer and winter consumption profile shall be normalized over a seven day period. The profile with the greatest consumption shall be used to determine generator fuel storage requirements.

8.4.2.3 Boiler Fuel On-site boiler fuel storage in the amount necessary for 10 January days of operation is required. See VHA Directive 2003-050 *Boiler Plant Operations*.

8.4.3 Water Storage Emergency Connection

The water storage system shall include emergency connections to allow for a change in supply source or change in delivery points.

8.4.4 Water Treatment

Provide water treatment equipment to mitigate from environmental contaminants including but not limited to fungi, dust, debris, outside condensation, and corrosion.

8.4.5 On-site Water Well

Where available, use an on-site water well as an alternate source for potable, industrial, and/or fire protection water.

8.4.6 Protection of Equipment

Protect all water and fuel storage, pumping, metering, and regulating equipment with screen walls or barriers that comply with Chapters 6 and 7.

All tanks shall remain functional and accessible during emergencies. Tanks shall be water tight and secured to prevent buoyancy. Intakes and vents shall be located above the base flood elevation, unobstructed, and in areas not subject to flooding.

8.4.7 Existing Facility – Water and Fuel Storage

Existing facilities shall comply with the requirements of section 8.4.

9 Building Systems

9.0 SCOPE

This chapter describes criteria for building mechanical building systems (fuels, steam, and chilled water), building plumbing systems (potable water, fire protection water, sanitary sewer, and medical and laboratory air and vacuum systems), building water storage systems (potable and industrial water storage tanks, water wells, pumps, and water purification systems), building electrical systems (electrical distribution equipment and electrical rooms and closets), stand-by power systems (generators, paralleling equipment, automatic transfer switches, and fuel storage), building uninterruptible power supply systems, and building telecommunications systems (DEMARC room, telephone equipment room, main computer room, telephone system, telecommunications distribution rooms, WLAN system, portable radio system, satellite radiotelephone system, public address system, distributed antenna system, and VSAT data terminal system). The utility services shall be designed in accordance with the VA Design Manuals including the Electrical, HVAC, Plumbing, Fire Protection, and Sanitary Design Manuals. In addition, building systems that are necessary to keep a mission critical facility in operation shall not be located at an elevation subject to flooding at any time. Throughout this section where it is mandatory that construction or equipment be in an area that is not subject to flooding refer to the FEMA flood map information available at http://www.fema.gov/business/nfip/fmapinfo.shtm.

9.0.1 Modularity

Component modularity of major mechanical, electrical, and telecommunications systems is an overarching physical security precept, which suggests that building systems be designed and constructed from interchangeable components. Modularity is also integral to the VA Hospital Building System Research Study Report (VAHBS or Red Book) and its Supplement, which describe integrated and modular design for new facilities. Building

systems for mission critical facilities shall employ the principles of modularity outlined in the VAHBS.

The primary objectives of VAHBS modularity are cost control, improved performance, adaptability, and the provision of a basis for building development and modification. The physical security benefit of VAHBS modularity is that it results in a facility composed of identical or nearly-identical service modules, each of which contains standardized mechanical, electrical, and telecommunications components that allow for isolation of service modules, simplification of maintenance and repair, and a higher degree of system capability and integrity. Each service module is in one fire compartment, and a fire compartment may contain more than one service module. VAHBS modularity reduces complexity in detailing and construction, reduces compromises in maintenance, and enhances physical security and future expansion.

9.0.2 Security Considerations

Refer to Chapters 5 and 10 and Appendix A, Security Door Openings, and Appendix B, Security System Application Matrix, for construction and security requirements for mechanical, electrical, and telecommunications spaces.

9.1 HVAC SYSTEMS

9.1.1 Requirements

9.1.1.1 Equipment location: Locate major mechanical equipment above the ground floor in an area not subject to flooding.

9.1.1.2 Emergency connections: Include emergency connections for chilled water and steam services at or near the building entrance point, where it will be unobstructed and accessible in an area not subject to flooding. Where looped systems enter the building at two points, the emergency connections need only be installed on one entry.

9.1.1.3 Security Control Center (SCC): In the SCC, provide a display-only terminal, which will display status and alarm conditions reported by the energy center, the building(s) environmental control system(s), medical gas and vacuum system alarms, stand-by and/or emergency generators, and other similar systems.

9.1.1.4 Entrances and lobbies: Maintain positive pressure in lobbies and entrance areas.

9.1.2 Intakes and Exhausts

9.1.2.1 Outdoor air intakes: All air intakes shall be located so that they are protected from external sources of contamination. Locate the intakes away from publicly accessible areas, minimize obstructions near the intakes that might conceal a device, and use intrusion alarm sensors to monitor the intake areas.

- Locate all outdoor air intakes a minimum of 100 feet (31 m) from areas where vehicles may be stopped with their engines running.
- Locate all outdoor air intakes a minimum of 30 feet (9 meters) above finish grade or on roof away from the roof line.

9.1.2.2 Air intakes and exhausts: Design to minimize the blast over pressure admitted into critical spaces and to deny a direct line of sight from a vehicle threat located at the stand-off distance to the critical infrastructure within. Refer to Chapter 6.

9.1.2.3 Hurricane areas: Louvers in areas prone to hurricanes or wind-debris hazards shall be certified by the manufacturer to meet the following Florida Building Code tests: Uniform Static Air Pressure Test, Cyclic Wind Pressure Test, Large Missile Impact Test, and Wind Driven Rain Resistance Test.

9.1.3 Existing Facility – HVAC Systems

Existing facilities shall comply with section 9.1.1.2. Refer to section 6.5.2.

9.2 ELECTRICAL SYSTEMS

9.2.1 Stand-by Power Systems

Generators are required to provide power for the entire mission critical facility load. See also Chapter 5 for functional area requirements.

The stand-by power system is not identical to the NFPA-required emergency power system, which supplies power to a specifically mandated set of health care facility loads. The stand-by power system is in addition to the emergency power system.

9.2.1.1 Stand-by generators: Generators shall be diesel compression engine type. Generators should provide power at the highest practical voltage level, preferably the medium-voltage utility service entrance voltage, and be paralleled into the normal power electrical system at a point as close as possible to the utility service entrance.

An assumed peak load of 10 watts per gross square foot of building area is suggested for sizing the capacity of the generator(s).

9.2.1.2 Location: Generators, paralleling equipment, and associated fuel and electrical components shall be located in dedicated structures or rooms. These structures or rooms shall be in compliance with the Physical Security Design Manual.

Stand-by power systems shall be located a minimum distance of 100 feet (31 m) or greater in all directions from areas such as loading docks or similar defined areas of vulnerability.

9.2.1.4 Load shedding controls: Automatic controls shall selectively shed load from the stand-by power system upon failure of one or more stand-by generators to operate. The last loads to be shed shall be the "normal" sources for the emergency electrical system automatic transfer switches.

9.2.1.5 Emergency connections: Include emergency connections for emergency and stand-by generators at or near the building entrance point. Where looped systems enter the building at two points, the emergency connections need only be installed on one entry.

9.2.2 Uninterruptible Power Systems (UPS)

Provide UPS equipment for mission critical telecommunications equipment. The telecommunications facilities include the entrance facility (DEMARC), main telephone room, and main computer room. UPS equipment and its associated power distribution unit (PDU) are essential pieces of bridging equipment, used during the time gap between loss of utility power and energization of the emergency or stand-by generator systems. They are also intended to provide time for an orderly shutdown of equipment in the event stand-by generators do not operate properly.

9.2.2.1 Modularity: Where multiple UPS are used, they shall be identically sized to allow for interchangeability.

9.2.2.2 Space for UPS: Provide required UPS floor space in rooms which require UPS-backed power.

9.2.2.3 Battery runtime: Size battery systems for a minimum of 20 minutes of full rated output. Individual project needs may dictate a longer runtime.

9.2.3 Existing Facility – Electrical Systems

9.2.3.1 Stand-by power: Existing facilities shall comply with section 9.2.1.5.

9.2.3.1 UPS: Provide UPS equipment for mission critical telecommunications equipment.

9.3 TELECOMMUNICATIONS SYSTEMS

Refer to Chapter 5 for functional area requirements.

9.3.1 Demarcation Room (DEMARC)

The DEMARC is where all telecommunications services from all service providers are delivered to the building.

9.3.1.1 Location: The DEMARC room must be located in a secure area of the building, on the ground floor or higher. The room shall not be located adjacent to either the telephone equipment room or the main computer room. The room shall not be located within 25 feet (7.62 m) of an outside wall or delivery area and shall not be located directly below laboratories, kitchens, laundries, toilets, showers, or other areas where water service is provided.

9.3.1.2 HVAC: The DEMARC room must be provided with generator-backed HVAC service.

9.3.1.3 Power: All equipment in the DEMARC room must be powered from either a building or local UPS that will provide a minimum of 4 hours of service at full rated output.

9.3.1.4 Conduit pathways: Conduit pathways used to interconnect the main telephone room, the DEMARC room, and the main computer room must be configured in a ring topology to provide two pathways to any of the three locations.

9.3.2 Telephone Equipment Room

The telephone equipment room shall house the main telephone switching equipment for the facility and contain public address system equipment, interconnection to the portable radio system, and other equipment that interconnects with the telephone system.

9.3.2.1 Location: The telephone equipment room must be located in a secure area of the building on the ground floor or higher. The room shall not be located adjacent to either the DEMARC room or the main computer room. The room shall not be located within 25 feet (7.62 m) of an outside wall or delivery area and shall not be located directly below laboratories, kitchens, laundries, toilets, showers, or other areas where water service is provided.

9.3.2.2 HVAC: The telephone equipment room must be provided with generator-backed HVAC service.

9.3.2.3 Power: All equipment in the telephone equipment room must be powered from either a building or local UPS that will provide a minimum of 4 hours of service at full rated output.

9.3.2.4 Conduit pathways: Conduit pathways used to interconnect the main telephone room, the DEMARC room, and the main computer room must be configured in a ring topology to provide two pathways to any of the three locations.

9.3.3 Main Computer Room

The main computer room contains all of the main data processing equipment for the mission critical facility.

9.3.3.1 Location: The main computer room shall not be located adjacent to either the DEMARC room or the main telephone room, and shall not be located directly below laboratories, kitchens, laundries, toilets, showers, or other areas where water service is provided.

9.3.3.2 HVAC: The main computer room must be provided with generator-backed HVAC service.

9.3.3.3 Power: All equipment in the main computer room must be powered from either a building or local UPS that will provide a minimum of 20 minutes of service at full rated output.

9.3.3.4 Conduit Pathways: Conduit pathways used to interconnect the main telephone room, the DEMARC room, and the main computer room must be configured in a ring topology to provide two pathways to any of the three locations.

9.3.4 Telecommunications Distribution Rooms

Telecommunications distribution rooms are located on all floors of the building and distribute telephone, data, and other telecommunications to work spaces located throughout the building.

9.3.4.1 Location: Telecommunications distribution rooms shall be centrally located on the floors so that cables connecting workstations are no longer than 295 feet (90 m). In many cases this will require more than one distribution room on the floor. Telecommunications distribution rooms must be stacked vertically.

9.3.4.2 HVAC: Telecommunications distribution rooms must be provided with generator-backed HVAC service.

9.3.4.3 Power: All equipment in the telecommunications distribution rooms must be powered from either a building or local UPS that will provide a minimum of 20 minutes of service at full rated output.

9.3.4.4 Cabling: For horizontal workstation cabling, use one type of cable throughout for both phone and data. This enables a universal wiring scheme that is very flexible. The type or grade of cable required will be determined during system design. Where plenum cable is required in sections of the building, use plenum cable throughout.

9.3.5 WLAN System

A wireless data system facilitates rapid restoration of limited data communications services in the building after a catastrophic event. Provide a wireless data access system, or install infrastructure (cabling) placed for later system installation.

Provisions shall be made during the initial telecommunications system design and installation to implement a wireless data system throughout the building. These provisions are required whether a wireless data system will be initially installed or not. Specific design requirements will include placement of data access points, plans to interface with antenna distribution system, and equipment space and power requirements in telecommunications distribution rooms.

System design must include provision for PoE (Power over Ethernet) to supply power to any individual access points.

Horizontal cabling used to connect Wireless Access Points (WAPs) shall be the same type as cable used for other building wireless access points.

Wireless LAN access points distributed throughout the facility must be secured to the ceiling or building in a way that requires a special tool for removal.

Data security on the WLAN must be implemented using the most secure industry standard at the time the system is actually put in operation.

System design must include the ability for the wireless data system to use the building distributed antenna system, if available, for distributing data signals.

9.3.6 Portable Radio System

Provide a portable radio system. The portable radio system provides radio paging for security services and facilities management services both inside buildings and throughout the campus, where there are multiple buildings.

All fixed radio equipment must be mounted according to manufacturer's recommendations and mounting provisions must comply with applicable seismic requirements.

9.3.6.1 Location: Radio equipment may be located in a penthouse or one of the telecommunication distribution rooms. The location must be coordinated with access to both the antenna equipment and the vertical riser (telecommunications distribution room) spaces.

9.3.6.2 HVAC: Fixed radio equipment must be provided with generator-backed HVAC service.

9.3.6.3 Power: Fixed radio equipment must be powered from either a building or local UPS that will provide a minimum of 24 hours of service at full rated output.

9.3.7 Satellite Radiotelephone System

Provide a satellite radiotelephone system. The purpose of the satellite radiotelephone is to provide a very basic and limited telephone capability in the event internal and external phone systems failure. The satellite radiotelephone must be able to make local, long distance, and international telephone calls directly over a satellite connection without using any land facilities.

9.3.8 Public Address System

The public address (PA) system is defined as an emergency communication life safety system by the National Fire Protection Association (NFPA). The all call paging function for code one (blue) life support and interconnection to the facility's NFPA-identified critical care telephone system elevates classification of the system's emergency communication rating to critical care. Therefore, installation and operation shall adhere to all appropriate national, federal, and life safety and support codes, the more stringent of which shall govern.

All cabling and installation practices associated with equipment intended for use in a critical care facility will be adhered to.

The PA system must be able to be overridden by security personnel during an extraordinary event.

9.3.8.1 Location: All central PA equipment shall be located in the main telephone room to facilitate interconnection with the telephone system.

9.3.8.2 Power: PA system equipment must be powered from either a building or local UPS that will provide a minimum of 4 hours of service at full rated output.

9.3.8.3 Cabling: Comply with all cabling and installation practices associated with equipment intended for use in a critical care facility.

9.3.9 Distributed Antenna System

Provide a distributed antenna system in the facility. The distributed antenna system works in conjunction with the various radio systems in the building to improve portable radio system coverage in the building and provides the ability to use one common antenna system for multiple services. Services that may be supported include the portable radio system, public safety radio rebroadcast, cellular radio system rebroadcast, and support for WLAN data service.

9.3.9.1 Location: All distributed antenna system equipment shall be located in the telecommunications distribution rooms.

9.3.9.2 Power: Distributed antenna system equipment must be powered from either a building or local UPS that will provide a minimum of 4 hours of service at full rated output.

9.3.9.3 Cabling: Comply with all optical fiber, coaxial, and antenna system cabling and installation practices associated with cabling intended for use in a critical care facility.

9.3.10 VSAT Satellite Data Terminal

A Very Small Aperture Terminal (VSAT) data terminal acts as a backup data system and provides limited data capability if all ground based services were to fail. It provides a data capability that is not dependent on local service providers.

9.3.10.1 Location: VSAT equipment is roof-mounted and interfaces with data translation equipment located in the main computer room.

9.3.10.2 Power: VSAT equipment must be powered from either a building or local UPS that will provide a minimum of 20 minutes of service at full rated output.

9.3.11 Existing Facility – Telecommunications Systems

Existing facilities shall comply with section 9.3.

9.4 PLUMBING SYSTEMS

9.4.1 Medical Air and Oxygen Systems

Medical air and oxygen systems shall be secured to prevent unauthorized tampering, contaminating, or cross-connecting of systems.

9.4.2 Existing Facility – Plumbing Systems

No additional physical security requirements.

9.5 FIRE PROTECTION SYSTEMS

9.5.1 Fire Department Hose Connections

Fire department hose connections located on the exterior of a building shall be secured in suitable enclosure that limits access to authorized personnel. Coordinate with the serving fire department.

9.5.2 Existing Facility – Fire Protection Systems

Shall meet the requirements of 9.5.1.

10 Security Systems

10.0 SCOPE

The requirements of Chapter 10 shall apply to all Mission Critical facilities, both new and existing. Existing facilities shall be required to meet the same requirements as new facilities.

This chapter addresses physical security standards associated with the selection, application, and performance of electronic security systems (ESS). The ESS include the Closed Circuit Television (CCTV) monitoring and surveillance system; Intrusion Detection System (IDS); Physical Access Control System (PACS); Duress, Security Phones, and Intercom System (DSPI), commonly referred to as intercommunications system; and the optional use of Detection and Screening System (DSS). The integration and monitoring of the ESS, system operation, and space requirements associated with the ESS subsystems are discussed in the section on the Security Control Center (SCC), which also describes the security console operations and systems management criteria.

The ESS subsystems shall be designed and engineered by a qualified security consultant with a minimum of five years of relevant experience and who maintains current certification such as Certified Protection Professional (CPP) or Physical Security Professional (PSP) from the American Society for Industrial Security (ASIS).

10.1 CCTV MONITORING AND SURVEILLANCE (CCTV)

This section addresses physical security standards for the two basic uses of a video surveillance, or CCTV, system: access control and general surveillance. This section describes the selection, application, and performance of the CCTV system, which includes cameras, monitors, controlling and recording equipment, and centralized management and operations of the system.

10.1.1 System Uses, Compatibility, and Integration

Refer to Appendix A, Security Door Openings, and Appendix B, Security System Application Matrix, for CCTV system component locations.

10.1.1.1 System uses: CCTV system shall be used to monitor building entrances, restricted areas, mission critical asset areas, and alarm conditions. CCTV system shall be used for surveillance and observations of defined exterior areas, such as site and roadway access points, parking lots, and building perimeter, and interior areas from a centralized Security Control Center (SCC).

10.1.1.2 System compatibility: All components of the CCTV system shall be fully compatible and shall not require the addition of interface equipment or software upgrades to ensure a fully operational system.

10.1.1.3 System integration: The CCTV system shall be able to be fully integrated with other security subsystems.

10.1.2 Networked versus Stand-alone CCTV System

CCTV system shall be designed and engineered as either a networked or stand-alone system.

10.1.2.1 Networked CCTV system: A networked CCTV system shall be utilized when multiple cameras, monitors, controllers, and recording devices are configured and makeup what is defined as a whole CCTV system. All components of the system shall be monitored and controlled at a single point, the SCC, using either a matrix switcher or a desktop computer.

10.1.2.2 Stand-alone CCTV system: A stand-alone CCTV system may be used for a single application and designated location use only and may compliment the physical access control system (PACS) for a specific area. Fixed camera(s) shall be positioned in a manner to allow viewing of specific entry control point(s) through the use of a dedicated CCTV system monitor located in a common viewing area.

10.1.3 Cameras

The design, installation, and use of CCTV cameras shall support the visual identification and surveillance of persons, vehicles, assets, incidents, and defined locations.

10.1.3.1 General requirements: All cameras shall meet the following requirements.

- Cameras shall be charge coupled device (CCD) cameras and conform to National Television System Committee (NTSC) formatting criteria.
- Cameras shall be color and programmable to digitally switch from color to black and white at dusk and vise versa at dawn.
- Cameras shall be rated for continuous operation.
- Each camera function and activity shall be addressed within the system by a unique twenty (20) character user defined name. The use of codes or mnemonics identifying the CCTV action shall not be accepted.
- Cameras shall have built-in video motion detection that automatically monitors and processes activity information from each camera based upon how the surveillance field-of-view is programmed.
- When the camera is used as part of a CCTV system computer network, a video encoder shall be used to convert the signal from the NTSC criteria to Moving Picture Experts Group (MPEG) format.
- All cameras shall be home run to a monitoring and recording device via controlling video equipment such as a matrix switcher or network server that is monitored from a designated SCC location. The use of wireless cameras may also be considered. (See section 10.1.3.3)

10.1.3.2 Fixed versus pan/tilt/zoom (P/T/Z) cameras: CCTV cameras may be either fixed or pan/tilt/zoom (P/T/Z).

- Fixed cameras shall be the primary means of surveillance to monitor designated access control and monitoring points.
- P/T/Z cameras shall compliment the use of fixed cameras when large and multiple areas of surveillance are required and using video motion detection provides additional surveillance advantages.
- P/T/Z cameras shall be used and deployed for all site perimeter and exterior building areas.
- Fixed cameras shall be used to monitor interior building areas; P/T/Z cameras may be used to provide supplemental surveillance coverage of building interiors where necessary.

10.1.3.3 Hardwired versus wireless cameras: CCTV cameras classified as hardwired directly connect to a monitoring device using video signal imaging cable. A wireless CCTV camera application is directly connected via a remote receiver that requires constant line-of-sight communications with the camera and the monitoring device.

- Hardwired or IP cameras shall be the preferred method of installation.
- Hardwired cameras shall be connected to the monitoring equipment with continuous wiring used as the media transmission system.
- Prior to selection of wireless cameras consider the potential effects, such as geographical area of coverage, environmental interference, and distance from the monitoring location, that impacts the use of this technology.

10.1.3.4 Color versus black and white cameras: All CCTV cameras shall be color that allows for black and white applications.

- Cameras shall be able to switch between color and black and white through a programmable feature built into the camera.
- Color shall be the primary mode automatically switching to black and white when light levels drop below normal specifications.
- Cameras will be set to black and white on a full time basis only when installed in a low light level that requires the camera to operate at a higher resolution than normal.

10.1.3.5 Camera lenses: CCTV camera lenses shall be used in a manner that provides maximum coverage of the area being monitored and shall meet the following requirements.

- Two types of lenses shall be used for both interior and exterior fixed cameras.
  - Manual variable focus lenses shall be used in large areas monitored by the camera and shall allow for settings at any angle of field to maximize surveillance coverage.
  - Auto iris fixed lenses shall be used in areas where a small specific point of reference is monitored.
- Specific lens size shall be determined using a field-of-view calculation provided by the manufacture.

10.1.3.6 Camera enclosures: All cameras and lenses shall be enclosed in tamper resistant housing.

- Both interior and exterior cameras shall be housed within a tamper-proof camera enclosure.
- Exterior camera enclosures shall be environmental proof to protect against unique weather elements associated with the specific facility geographical area.

10.1.3.7 Camera installation, mounts, poles, and bases: All camera equipment shall be installed to ensure that all components are fully compatible as a system. Adhere to guidance provided by the National Electrical Contractors Association Standard, NECA 303-2005, Installing Closed-Circuit Television (CCTV) Systems.

- Camera mounts shall be installed on approved mounting surfaces structured for weight, wind load, and extreme weather conditions.
- Camera mounts shall be installed in a manner that will not inhibit camera operation or field of view.
- Where camera is mounted to a rooftop or within a parapet, ensure that the mount is designed and installed in a manner that the equipment can be swiveled inward for maintenance and upkeep purposes.
- All camera poles shall be constructed of metal with a concrete base and shall be installed and grounded in accordance with the National Electrical Code (NEC).
- Camera poles shall be weather resistant.
- Camera pole heights shall be no less than 15 feet (4.6 m) and no greater than 50 feet (15.2 m) high.
- Cameras and their mounts may share the same pole with lighting when the following conditions are met:
  - A hardened wire carrier system is installed inside the pole to separate the high voltage power cables for the lighting from the power and signal cables for the camera and mount.
  - The camera and mount are installed and positioned in a manner that the lighting will not deter from, cause blind spots or shadows, and interfere with the video picture and signal.
- All camera poles and mounts shall be installed in locations that will allow for optimum view of the area of coverage.

10.1.3.8 Power source: All CCTV cameras and mounts shall be powered remotely by a UL listed power supply unit (PSU) as follows.

- The PSU shall have the ability to power at least four exterior cameras or eight interior cameras.
- A back-up direct power feed from a security system power panel shall be provided to the camera and mount. A step down transformer shall also be installed at the camera location to ensure a proper operating voltage is provided to the camera and mount.

- The CCTV system shall be supported by a UPS and/or dedicated stand-by generator circuit to ensure continuous operation of cameras including all surveillance monitoring and recording equipment.

10.1.3.9 Lightning and surge protection: With the exception of fiber optic cables, all cables and conductors that act as control, communication, or signal lines shall include surge protection.

10.1.3.10 Site coordination: Site and building exterior lighting shall be coordinated and installed in a manner that allows the CCTV system to provide positive identification of a person, vehicle, incident, and location.

- Lighting shall not provide bright illumination behind the main field of camera view.
- Cameras shall be installed in a manner that no lighting will point directly at the camera lens causing blind spots and black outs.
- Provide routine maintenance of lighting systems and replacement of lighting fixtures and luminaries that are necessary for operational integrity of the CCTV system.
- CCTV cameras shall be installed so that landscaping will not deter from the intended field of view.
    - Cameras shall not be mounted in trees, bushes, or any other natural landscape that will in the long term degrade the view or operation of the CCTV system.
    - Cameras shall not be installed behind, next to, or on any natural or man-made object that will restrict the field of view, cause signal loss, or prevent the camera from being fully operational.
    - Perform routine landscape maintenance that is necessary for operational integrity of the CCTV system.

10.1.4 Additional CCTV System Components

10.1.4.1 Monitors: All CCTV monitors shall be color and able to display analog, digital, and other images in either NTSC or MPEG format associated with the operation of the Security Management System (SMS).

10.1.4.2 Matrix switcher/network server (controlling equipment): Controlling equipment shall be used to call up, operate, and program all cameras associated CCTV system components. Controlling equipment shall have the ability to operate the cameras locally and remotely. A matrix switcher or a network server

shall be used as the CCTV system controller. The controlling equipment shall allow the transmission of live video, data, and audio over an existing Ethernet network or a dedicated security system network, requiring an IP address or Internet Explorer 5.5 or higher. The controlling equipment shall be able to perform as an analog-to-Ethernet "bridge," allowing for the control of matrices, multiplexers, and P/T/Z cameras.

10.1.4.3 Keyboards and joysticks: A keyboard shall provide direct operator interface with the controlling equipment to allow for call-up, operation of cameras and mounts, and programming of controlling equipment as well as cameras and monitors. Where a matrix switcher is used, ensure the keyboard is outfitted with a joystick to provide direct interface with CCTV camera controls.

10.1.5 Controlling and Recording Equipment

All cameras on the CCTV system shall be recorded in real time using a Digital Video Recorder (DVR), Network Video Recorder (NVR), or a Time Lapse Video Recorder (VCR). The type of recording device shall be determined by the size and type of CCTV system designed and installed, as well as the extent to which the system is to be used. The following criteria shall be followed when choosing a CCTV camera recording device.

10.1.5.1 DVR: The DVR shall be used within the CCTV system for large or small CCTV system set-ups. The DVR may be used in place of a time lapse VCR regardless of how the CCTV system is designed and installed. The DVR may be installed with the SMS or as part of a CCTV system network. The DVR shall be Internet Protocol (IP) addressable. Programming, troubleshooting, and all general maintenance and upgrades to the DVR shall be done locally at the recording unit.

- The DVR shall have a built-in compact disc-recordable (CD-R) for downloading of the buffer to compact disc (CD) for back-up.
- The DVR buffer shall be cleared and all information transferred to CD when the buffer is at no greater than 60% of capacity.
- Compact disc-read only memory (CD-ROM) shall be stored in a dry, cool, central location that is secure. Recordings shall be stored in accordance with VA Police directives.

10.1.5.2 NVR: The NVR shall be used within the CCTV system for large or small CCTV system set-ups. The NVR shall be used when the CCTV system is configured as part of the SMS only. Input to the NVR shall be considered when designing and installing all cameras that will be connected to the NVR.

- Ensure the proper signal converter is used to interface non-Power over Ethernet (PoE) cameras over to a Category Five (CAT-V) cable.
- The NVR shall provide for either direct download of data to a computer storage device or CD-ROM. All storage media shall be stored in a dry, cool, central location that is secure, and storage media shall be held as directed by the VA Police.

10.1.5.3 Time lapse VCR: The time lapse VCR shall be used for all CCTV systems of fewer than 16 cameras and that are not part of an SMS or connected to a CCTV system network.

- A time lapse VCR using analog tapes shall have the capability to record on a continuous 24-hour basis.
- These recordings shall be stored in a dry, cool, central location that is secured and shall be maintained in accordance with VA Police directives.
- The time lapse VCR shall be used as a back-up to DVR and NVR equipment.

10.1.6 Video Motion Detection

CCTV cameras shall have built-in video motion detection capability that automatically monitors and processes information from each CCTV camera. Cameras shall be programmed to automatically change viewing of an area of interest without human intervention and shall automatically record the activity until reset by the CCTV system operator.

10.1.6.1 Timing: This feature shall detect motion within the camera's field of view and provide the SCC monitors immediate automatic visual, remote alarms, and motion-artifacts as a result of detected motion.

10.1.6.2 Interface with IDS: The video motion detection shall be interfaced with the intrusion detection system (IDS) to provide redundancy in the security alarm reporting system.

10.1.6.3 Other system interface: Cameras shall be designed to interface and respond to exterior and interior alarms, security phones/call-boxes, duress alarms, and intercoms upon activation.

10.1.7 Camera Locations

Refer to Appendix A, Security Door Openings, and Appendix B, Security System Application Matrix, for CCTV system component locations.

10.2 INTRUSION DETECTION SYSTEM (IDS)

The Intrusion Detection System (IDS) includes motion detection, glass break, and door contact sensors, among other devices. These devices provide alternative methods to detect actual or attempted intrusion into protected areas through the use of alarm components, monitoring, and reporting systems. The IDS shall have the capability of being integrated with DSPI, PACS, and CCTV systems. All IDS shall meet UL 639 Intrusion Detection Standard.

10.2.1 System Elements and Features

IDS shall be used to monitor the site perimeter, building envelope and entrances, and interior building areas where access is restricted or controlled. Refer to Appendix A, Security Door Openings, and Appendix B, Security System Application Matrix, for IDS component locations.

10.2.2 System Integration

IDS shall be able to be fully integrated with other security subsystems using direct hardwire or computer interface.

10.2.3 Planning and Selection Criteria

IDS shall provide multiple levels or points of detection as far away as possible from an asset to be protected. The type of IDS sensor to be used shall be determined by the criticalness of the asset to protect, size of the protected space, local threat assessment results, and capability of the sensor.

10.2.3.1 Layout and zoning: Areas to be covered by sensors shall be charted and set up in protection or coverage zones prior to selection and placement of sensors. IDS devices of different technologies such as motion detection, glass break, and magnetic contacts shall be zoned separately.

10.2.3.2 Physical environment: A survey shall be conducted to determine whether conditions exist that may adversely affect the sensors and cause them not to detect within their performance limits or to cause false alarms.

- For exterior applications consider the effects of foliage, rain, fence fabric, underground utilities, and other environmental conditions.
- Interior applications of sensors shall consider HVAC location, heat sources, transient light, vibration, moving machinery, dust, and humidity.

10.2.4 Networked versus Stand-alone

10.2.4.1 Networked: IDS devices shall be networked when multiple sensors and controllers are being utilized. All components of the IDS shall be monitored and controlled at a single point.

10.2.4.2 Stand-alone: Stand-alone IDS shall be used for single office space only as determined by the Project Manager and shall be a means to compliment the physical access control system (PACS) and CCTV system.

10.2.5 Hardwired versus Wireless

10.2.5.1 Hardwired alarms: All sensors and controllers shall be hardwired and directly connected to the local controller, keypad, or other security subsystems using proper cabling.

10.2.5.2 Wireless alarms: Wireless alarms may be used only where the surrounding building construction and environment will not degrade the effective range of the alarm signal. Where a wireless IDS system is used it must meet Federal Communication Commission (FCC) wireless transmission standards.

10.2.6 Environmental Conditions

IDS devices shall be selected and installed to be fully functional under all environmental conditions for the specific location.

10.2.7 Interior Sensors

Interior sensors shall be used to detect the presence of an intruder or an attempt to gain entry into controlled and restricted areas. These areas include but are not limited to exterior and interior entrances, such as doors, windows, walls, roof and ceilings, ventilation, underground tunnels, and pathways. The following sensor options shall be applied based upon the level of protection required and the type of area to be monitored.

10.2.7.1 Balanced magnetic switches (BMS): BMS shall be used to detect attempted access or entry of interior and exterior doors and fence gates. BMS may be either recessed or surface mounted; the preferred method is to use a recess mounted switch to reduce the ability to defeat the system.

- When double doors or gates require protection, each door shall be fitted with a separate magnetic switch.
- Surface mounted switches shall be mounted on the protected side of the door.
- When protecting roll-up doors wider than 80 inches (2 m), BMS shall be mounted on both left and right sides on the interior side of door.

10.2.7.2 Glass break sensors: Sensors shall be used to detect attempts to penetrate glass by detecting vibrations and acoustic emanations associated with breaking or cutting glass. All perimeter windows within 40 feet (12.2 m) of ground level and windows accessible from an adjoining building roof or within 25 feet (7.6 m) directly or diagonally opposite a window, building, roof, or fire escape shall use a glass break sensor. Glass break sensors shall be used on windows that exceed 37 in^2 (240 cm^2) with any dimension greater than 8 inches (200 mm).

- Windows with security mesh screen do not require glass break sensors. For windows with air conditioning units installed, the mesh screen must encompass the air conditioner.

10.2.7.3 Volumetric sensors: Also known as a "space sensor," volumetric sensors shall be used for interior confined spaces. Active or passive sensors may be used. Sensitivity shall be adjustable and set to provide maximum protection while reducing false alarms. PACS shall be provided in protected spaces where volumetric detection is provided and shall activate or deactivate the volumetric sensor upon presentation of a proper access control credential.

10.2.7.4 Passive infrared sensors (PIR): PIR shall meet the requirements of ANSI/SIA PIR-01, Passive Infrared Motion Detector Stands-Features for Enhancing False Alarm Immunity, and shall be capable of detecting changes in infrared energy or heat. A 360-degree field of view configuration shall be preferred for sensor monitoring purposes, but the final determination of configuration for field of view, which may be 360, 180, 90 or 45 degrees, shall be determined from a field survey and mounting surface availability. Sensitivity of the sensor shall be adjustable to provide the necessary area of protection.

10.2.7.5 Vibration sensors: The building boundary wall to be protected shall use vibration detection sensors mounted to the wall with close spacing to assure detection of attempted penetration before the wall is breached. Vibration sensors shall be used in combination with BMS for safes and vaults. Wall mounted shock/vibration sensors shall be provided with LEDs to indicate activation and shall be mounted to provide a clear view of the LED. Except for small areas, sensors zoned together shall not cover more than one wall.

10.2.7.6 Video motion detection sensor (VMD): Refer to section 10.1.

10.2.7.7 Pressure mats: Pressure mats shall be used on the interior side of an entry way and shall be concealed under a lightweight mat or carpeting. Pressure mats shall be used in conjunction with other sensor technologies and shall not be relied on as the sole intrusion detection device for space protection.

10.2.8 Exterior Sensors

Exterior sensors shall only be used for perimeter protection when the area to be protected is bordered by a fence or physical barrier. Exterior perimeter detection capability shall be applied to fenced areas around a site or building, loading docks, and outside storage areas or enclosures, using volumetric sensors in addition to BMS on access gates. Where CCTV cameras with video motion detection are used, exterior sensors may not be necessary. Facilities that use a fence to define boundaries shall address the use and necessity of fence mounted sensors, microwave sensors, or photoelectric beams.

10.2.8.1 Microwave: Microwave sensors shall use a multiple-beam configuration and only be used when there is a clear line of sight between a transmitter and receiver and the ground is fairly level. Microwave sensors shall not be used near outdoor fluorescent lights.

10.2.8.2 Infrared system: For outdoor applications active infrared systems shall be used in a multi-beam arrangement to create an invisible fence or corral around the protected area. These systems are affected by fog, rain, and snow and shall not be installed where local climatic conditions would cause interference.

10.2.8.3 Buried cable: For high-risk and mission critical facilities that require perimeter protection or perimeters that do not have a fence that can provide protection, buried cable sensors shall be considered in combination with another outdoor perimeter detection technology. To reduce false alarms, buried cable sensors including seismic, pressure, and leaky coaxial cables shall not be used in extreme cold environments where there is heavy ice or locations with heavy ground disturbances, low-flying aircraft, or underground utility lines and pipes.

10.2.8.4 Fence mounted sensors: Fence mounted sensors include tension wire, capacitance, electric vibration, and shock sensors. When using fence mounted sensors a BMS shall be installed at the pedestrian and vehicle access point gates.

10.2.8.5 Video motion detection sensor (VMD): Refer to section 10.1.

10.2.9 Alarm Conditions

Conduct a field survey to determine security response capability to all alarm conditions, such as bells, sirens, strobes, or silent alarms. Silent alarms may be integrated with CCTV camera coverage. After activation, the SCC personnel and VA Police shall deactivate and re-set the alarms.

10.2.10 Installation

To ensure proper operation, maximum detection capability, and minimize false alarms, IDS shall be installed in accordance with manufacture instructions, National Fire Protection Agency (NFPA) 731 *Standard for the Installation of Electronic Premises Security Systems* and UL 681 *Installation and Classification of Burglar and Holdup Alarm Systems*. All IDS shall be capable of continuous operation and monitoring through the use of battery backup, uninterrupted power supply, stand-by generator, and/or a backup monitoring location.

10.2.11 IDS Locations

The IDS shall be designed to interface with CCTV cameras. Refer to Appendix A, Security Door Openings, and Appendix B, Security System Application Matrix, for CCTV system component locations.

10.3 PHYSICAL ACCESS CONTROL SYSTEM (PACS)

The Physical Access Control System (PACS) shall include, but not be limited to: card readers, keypads, biometrics, electromagnetic locks and strikes, and electronic security management system (SMS).

10.3.1 System Elements and Features

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.

10.3.2 System Integration

PACS shall be able to be fully integrated with other security subsystems using direct hardwire or computer interface.

10.3.3 Stand-alone versus Network Multiple-Portal System

10.3.3.1 Stand-alone: Stand-alone systems shall be used to control access to a single entry control point and shall be available either as one integral unit or as two separate components. Data for the entire user population will be stored within a communication panel for future reference and reporting purposes.

10.3.3.2 Network multiple-portal system: Multiple-portal systems shall be part of a large network of readers and controllers that are connected to a central

processing unit (CPU) that will regulate activities at more than one entry point at a time. All systems will be directly under the control of the CPU and will be programmed to receive periodic programming updates and upload data according to a preprogrammed schedule.

10.3.4 Control/Communications Panel

All panels shall be centrally located within a space that will prevent panels from being damaged, tampered with, and accessed by unauthorized personnel.

10.3.5 Electronic Security Management System (SMS)

The SMS shall allow the configuration of an enrollment and badging, alarm monitoring, administrative, asset management, digital video management, intrusion detection, visitor enrollment, remote access level management, and integrated security workstations or any combination of all or some.

10.3.5.1 Head-end hardware: Head-end hardware shall provide direct interface of all PACS equipment via a hardwired input.

10.3.5.2 Entry control software: Software shall allow for programming of the PACS via a CPU. All software shall be updated per manufacturer's instructions.

10.3.5.3 Network interface devices: Interface devices shall consist of all hardware and software required to allow for full interface with other security subsystems via a CPU.

10.3.5.4 Records management and reports: The SMS shall have the ability to compose, file, maintain, update, and print reports for either individuals or the system.

- Individual reports shall consist of an employee's name, office location, phone number or direct extension, and normal hours of operation and shall provide a detail listing of the employee's daily events in relation to accessing points within a facility.
- System reports shall produce information on a daily/weekly/monthly basis for all events, alarms, and any other activity associated with a system user.
- All reports shall be in a date/time format and all information shall be clearly presented.

10.3.5.5 Functional requirements: The SMS shall provide the ability to control, program, and monitor the PACS and all additional security subsystems that are designed to interface with the PACS and SMS.

10.3.6 Picture ID and Badging Station Interface

The badging station shall provide a form-based interface for the entry of badge holder data and access information. All data, including images, shall be stored on the SMS system server. The badging station shall allow image and signature capture for use in badge production and provide tools for badge design. Both video and digital cameras may be used.

10.3.7 Card Credentials and Readers

All card credentials shall comply with Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, and the Federal Information Processing Standards (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors. Smart card implementation shall adhere to the Government Smart Card Interoperability Specification (GSC-IS).

10.3.8 Entry Control Device

All entry control devices shall be hardwired to the PACS main control panel and operated by either a card reader or a biometric device via a relay on the control panel.

10.3.8.1 Door devices: Entry control devices on a door may be any of the following: electronic strike, electronic mortise lock, or electromagnetic lock.

10.3.8.2 Turnstiles: Turnstiles may be considered as a means of access control as an option to controlling access through lobby areas based on the size and traffic throughput. Depending upon the application, the following security turnstile equipment may be utilized: optical, waist high, drop arm, rotary gate, or mass transit.

10.3.9 Biometric Systems

As a means of secondary access control to card readers, biometric devices may be used for high-level control and restricted areas. Biometric systems have unique and limited applications and are not suited to all access control requirements. The types of biometric devices that may be used include: hand/palm geometry, fingerprint verification, retinal verification, or voice verification.

10.3.10 Portal Control Devices

Portal control devices, such as a push button, request-to-exit, or panic/crash bar, shall be used as a means of assisting persons exiting a controlled space and shall provide a secondary means of access control within a secure area. Portal control devices provide the means to override the PACS via a keypad or key bypass and assists in

door operations using automatic openers and closures. Portal control devices shall be connected to and monitored by the main PACS panel or SMS.

10.3.11 Door Status Indicators

Door status indicators, such as a door position switch or request-to-exit push button, shall monitor and report door status to the SMS.

10.3.12 Transmission Media

All PACS control panels shall interface with a CPU in accordance with appropriate media connections. Panels shall be system specific addressable, Internet Protocol (IP) addressable, and programmable via a computer. All panels shall be interfaced directly from a computer or via the Internet or Intranet. Access to the panels shall be password protected. All individuals with access to the panels shall be assigned a user specific password.

10.3.13 Locations

Refer to Appendix A, Security Door Openings, and Appendix B, Security System Application Matrix, for PACS system component locations.

10.4 DURESS, SECURITY PHONES, AND INTERCOM SYSTEM (DSPI)

The section addresses physical security criteria associated with the selection, application, and performance of the intercommunications system, also referred to as duress, security phones or emergency call-boxes, and intercom system (DSPI).

10.4.1 System Elements and Features

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. Refer to Appendix B, Security System Application Matrix, for locations where DSPI devices shall be used.

10.4.1.1 DSPI system compatibility: 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.

10.4.1.2 System integration: DSPI shall be fully integrated with other security subsystems.

10.4.1.3 Handicapped accessibility: DSPI systems shall be handicapped accessible.

10.4.1.4 Security intercoms: The main components of this security subsystem are the hardwired master intercom and remote intercom stations. Intercom devices shall be integrated with the CCTV system upon initiation and activation of a two-way conversation. Where wireless systems are used, repeaters shall be required. Typical locations for security intercoms shall include:

- Access controlled entry points to a site, parking, and perimeter building areas.
- Gated access and service road entry points.
- Loading docks and shipping/receiving areas.
- Interior building access control points to restricted areas.

10.4.1.5 Intercom door release: Security intercom with remote door release capability shall be used for functional areas that require PACS. The security intercom system shall be integrated with electronic or magnetic remote door release allowing for remote communication and unlocking of doors from a reception desk or SCC master intercom station. The security intercoms for these areas shall have both an audio and built-in video capability. Video verification of person(s) requesting access at these points shall be required.

10.4.1.6 Intercom master station: The master station shall be capable of selectively calling and communicating with all intercom stations individually or system wide. Master stations shall have a "call in" switch to provide an audible and visual indication of incoming calls from remote stations. The master station shall include, but not be limited to, a handset, microphone/speaker, volume control, push-to-talk button, an incoming call/privacy indicator, and selectors to permit calling and communicating with each remote or other master stations.

10.4.1.7 Intercom substation: An Intercom substation shall be capable of calling into a pre-programmed single or group of master stations via the pressing of a button or voice activation. When a programmed master station is not available, the call shall automatically transfer to another master station.

10.4.1.8 Multi-intercom station: The multi-intercom station shall have the ability to call or monitor multiple stations individually or as a public address system.

10.4.1.9 Single intercom station: A single intercom station only calls or monitors one other intercom location or station at a time; intercoms are direct wired and do not require a master station.

10.4.1.10 Push-to-Talk (PTT) two-way communications: PTT is the typical type of intercom activation device, which requires a button be pressed in order to transmit conversation over the intercom.

10.4.1.11 Voice operated intercom switching (VOX): VOX automatically switches audio direction based on the sound of a voice. The switch works when a sound is detected by the speaker/transmitter and no push-button is required to transmit a communication. These intercoms shall be used in interior or exterior areas; however, not in areas with high background noise, such as parking garages.

10.4.2 Security Phones or Emergency Call-Boxes

An emergency call-box or telephone system shall be used instead of intercoms for a multi-facility environment, a stand-alone facility with a parking structure, or a site with a requirement to transmit call station communications to another site. Emergency call-boxes shall be used in areas such as parking garages/lots, sidewalks, pathways of large campuses, and in isolated areas.

10.4.2.1 Push button hardwired: Emergency call-box systems shall be hardwired to a master station located and monitored at a central location, preferably the SCC. Pushing and releasing the emergency call-box call button shall initiate a call-in to a pre-programmed master station. Once the button is pushed, hands-free operation shall occur.

10.4.2.2 Handset-telephone extension: Emergency call-boxes shall have the capability of using the existing VA PBX telephone system lines. The PBX shall direct calls to a pre-programmed extension that may be located at a receptionist desk, the SCC, or both. Lifting the handset shall automatically dial a pre-programmed monitoring station. The caller's location shall be defined in the PBX system. A minimum of two numbers shall be programmed into the system, so that if the first number is busy or unavailable the second number will be polled. VA facility telephone systems and emergency call-boxes shall not use automatic voice dialers to 911 or the municipal police department.

10.4.2.3 Speaker-handset stations: Emergency call-box stations shall have the capability to automatically cut out the loudspeaker at the station when the phone handset is lifted, allowing conversations to occur through the handset rather than a speaker.

10.4.2.4 Scream alert option: Emergency call-boxes shall provide the option that a speaker phone becomes activated when a loud scream is heard. This system shall be limited to indoor applications, such as stairwells and elevators or pre-defined high-threat locations, where background noise will not cause false activation of these devices.

10.4.2.5 Integration with CCTV Cameras: Emergency call-boxes shall provide coverage with CCTV when activated or have a built-in camera video

surveillance capability that can be monitored from the SCC upon device activation. See section 10.1.

10.4.2.6 Remote control and monitoring: Emergency call-box master stations shall have the capability of monitoring and automatically polling each call-box, report incoming calls, identify locations, and keep records of all call events via software and integration with the SMS. The system shall provide auto-answer capability to allow VA Police to monitor and initiate calls. The master stations shall have the capability to remotely adjust speakerphone and microphone capabilities and reset the call-box activation from the central monitoring station.

10.4.2.7 Signaling devices: Emergency call-boxes shall provide visual recognition devices such as strobes or beacons, which will provide identification of the activated call-box.

10.4.2.8 Outdoor vs. indoor locations: All emergency call-boxes shall be installed on rigid structures, columns, walls, poles, and/or freestanding pedestals that are easily identifiable through unique markings, striping or paint, signage or lighting, and shall remain easily visible during low light conditions. CCTV and call-boxes shall be integrated to provide automatic surveillance and priority monitoring of the caller's location.

- Emergency call-boxes in indoor locations shall be easily accessible to the public, clearly marked, and may be wall mounted.
- All emergency call-boxes must be meet handicapped accessibility requirements.

10.4.3 Duress/Panic Alarms

Duress/panic alarms shall be provided at locations where there is considerable public contact in isolated and pre-identified high-risk areas, such as the lobby reception desk, patient service areas, nursing stations, and isolated offices and buildings where VA personnel work. Upon activation, a silent alarm signal shall be sent to a centralized monitoring location that shall be capable of continuous operations. Other requirements associated with activated alarms shall include all of the following.

- Alarms shall be continuously monitored by the SCC.
- Activated alarms shall be integrated with CCTV coverage of the area.
- Alarms shall be mounted in such a manner as not to be observable and shall prevent unintentional operation and false alarms.
- At strategic locations use PACS keypads that are capable of activation by a code known only to the user to notify the central monitoring station that the person entering an area is under duress.

10.4.3.1 Switch/push button hardwired: The duress/panic alarm system shall be hardwired to a monitoring site or the SCC. Upon activation of the alarm both a visual and audible alarm will be activated in the SCC. The system shall identify the location of the alarm by phone extension and area description.

10.4.3.2 Wireless: Before selection and installation of a wireless system a survey shall be conducted to determine if a wireless application is feasible. Wireless systems shall use ultrasonic, infrared, and radio frequency waves to link duress/panic devices with distributed transmitters and receivers. Receivers shall be mounted throughout an area or building, as needed, and hardwired to a central monitoring console. Repeaters shall be used to ensure full coverage. All wireless duress systems must conform to Federal Communications Commission (FCC) standards for wireless communications systems.

10.4.3.3 Switch/push button telephone extension: This system shall use an existing telephone line and PBX to transmit a duress alarm. On activation the PBX shall direct the signal with the caller's location defined to a pre-programmed extension located at the SCC. VA facility telephone systems and emergency call-boxes shall not use automatic voice dialers to 911 or the municipal police department.

10.4.3.4 Wireless-pendant devices: Wireless duress/panic devices (also known as personal panic alarm, identification duress alarm, or man-down alarm) may be considered as an option. When the panic button is pushed a wireless alarm signal is sent to the closest installed wireless sensing unit, which sends the signal on to a designated alarm monitoring location. Only wireless alarms that provide both geographical location and identification of the individual and have been tested in the operational area, especially in isolated areas impacted by structures, topology and other influencing factors, shall be used. The use of these devices shall be limited to personnel identified as holding high-risk positions, work in isolated areas, or travel to/from parking areas and buildings that are isolated, especially during hours of darkness. The devices shall meet the following requirements.

- Be convertible and have the capability to be worn on a lanyard around the neck, belt clip, or wristband.
- Include rechargeable batteries with low battery indicators that notify the user and monitoring station of their use.
- Be equipped with a pull chain that activates the device should an attempt be made to forcibly remove it from the person carrying it.
- Only be operational while on VA facility property.

10.4.3.5 Locators and repeaters: The duress/panic alarm devices shall be integrated with SCC and SMS software to provide identification and location of the user. Locators shall be required for wireless/pendant devices. Requirements for locators and repeaters shall be as follows.

- Locators shall be placed in strategic locations such as hallways, gathering rooms, parking lots and garages, walking trails, or any place where the location of a person in duress is required.
- For large VA campuses and outside applications, repeaters shall be used that provide true line-of-sight range. The number of repeaters required will depend on the performance of a site survey, capabilities, and coverage distances.

10.4.3.6 Automated dispatch: Duress/panic alarm devices shall automatically announce or provide alarm notification signals to on-site pagers worn by VA Police and other designated personnel, hand held portable radios, cell phones, and landline telephones.

10.4.3.7 Integration with CCTV cameras and IDS: Duress alarm areas shall be covered by CCTV cameras. Once the duress alarm has been activated the CCTV system shall monitor and record all events associated with the alarm. The IDS will provide monitoring of duress alarm. Refer sections 10.1 and 10.2.

10.4.4 DSPI Locations

Refer to Appendix B, Security System Application Matrix, for DSPI system component locations.

10.5 SECURITY CONTROL CENTER (SCC)

This section addresses the application, monitoring, control, programming, and interface of the SCC with all security subsystems: CCTV, IDS, PACS, DSPI, and DSS. Additional requirements for the SCC are covered in section 5.15 and should be coordinated with the fundamental planning concepts and criteria associated with the SCC design and security console operating environment covered in this section.

10.5.1 Operational Requirements

The SCC shall provide continuous and consistent monitoring, surveillance, response, and operation of security subsystems.

10.5.2 Primary and Secondary Locations

The SCC shall be located in an area that is within the first level of security defense

defined by the VA. The SCC shall also be located above any potential flood areas, such as basement.

The SCC shall be located in an area free of background noise influences that could impact equipment and SCC operations. To prevent potential compromise of operations, staff health, and safety, the SCC shall be located away from exterior building walls that are adjacent to roadway traffic, parking, and air intake areas and facility utility, environmental, and operational areas, that if compromised, damaged, or destroyed, could impact SCC operations.

10.5.2.1 Secondary SCC: A secondary or backup SCC shall be established in another building or location within the same facility that is far removed from the primary SCC. The secondary SCC shall be provided with full redundancy of the electronic security systems and associated security console operations. The security technology shall be designed and engineered to provide flexibility to monitor and operate security subsystems from remote and multiple facility locations and security workstations.

10.5.3 Accessibility

The SCC shall be fully handicapped accessible.

10.5.4 Physical Security

The SCC shall have physical security safeguards. The main entry door shall have a card reader or biometric security credential device for authorized personnel and an intercom or similar device for unauthorized persons to request assistance. Provide a fixed CCTV camera connected to a dedicated monitor within the SCC for direct communications and visual verification of the person using the intercom. Remote unlocking of the door shall be prohibited.

10.5.5 Construction

See section 5.15.

10.5.6 Space Requirements

The size of the SCC shall be defined by the number of console bays required to house and operate the security subsystems and provide adjacency to the VA Police operations area which includes offices, meeting and training rooms, armory, and holding room. The SCC shall meet UFAS requirements to provide accessibility to the security console, to access equipment and wiring, console pull-out trays and doors, telephones, master intercom stations, base radio communications, and computer terminals. Floor area planning decisions will depend upon whether or not some of the security equipment, such as video surveillance recording equipment, will be rack or wall mounted,

imbedded or adjacent to the security console, or located in a separate equipment room. Future expansion of the SCC and security console equipment requirements shall be addressed.

10.5.6.1 Small SCC: A small SCC shall contain no more than four security console bays. 150-300 square feet of space shall be provided for a small to medium size SCC operation.

10.5.6.2 Large SCC: A large SCC shall contain no less than five and no more than eight security console bays. For large SCC operating environments, 500 square feet of space shall be provided.

10.5.6.3 Back-up or secondary SCC: Area requirements for a back-up SCC shall be based on what ESS systems will be monitored.

10.5.7 Electrical

Adequate power shall be provided to accommodate the security console equipment and other VA Police and building equipment requirements. The SCC and security console power shall be provided from a dedicated security system power panel. The panel shall be connected to a back-up power source capable of providing continuous power seven days a week for 24 hours a day. All field-mounted security equipment and security closets that interconnect and are monitored by the SCC and surge-protection at the equipment head-end shall be provided with back-up power. There shall be a main power cut-off switch for the SCC equipment located inside the SCC.

Lighting shall be adequate and not cast shadows or create a glare that will reduce the security console operator's ability to monitor security console equipment. All fixtures shall also be on back-up generator power. Finally, special care and consideration shall be given to the use of incandescent and fluorescent lighting, wall mounted battery powered emergency lighting, and illumination to the console writing space.

10.5.8 Environmental Applications

The air quality and temperature within the SCC shall allow for a comfortable work environment for both personnel and the security equipment. Ventilation controls shall also be provided on a separate air handling system that provides an isolated supply and return system.

The SCC shall have a dedicated thermostat control unit and cut-off switch to be able to shut off ventilation to the SCC in the event of a chemical, biological, or radiological (CBR) event or other related emergency.

10.5.9 Security Console/Workstation

The SCC security console may use stand-up, sit-down, and vertical equipment racks in any combination to monitor and control the security subsystems. The console shall be ergonomically designed with efficient writing and storage space provided and all security equipment requiring repetitive interaction and response by the console operator shall be easily accessed, observed, and accomplished.

All console bays and equipment racks shall be made of metal, furnished with wire ways, power strips, thermostatic controlled bottom or top mounted fan units, a hinge mounted rear door, front hinged door of Plexiglas, and a louvered top. In addition, space shall be provided for telephones, master intercom units, portable base station radio unit, computer monitors, and printers. All console bays shall be mounted on lockable casters and all console wiring shall be neatly organized, labeled, and made easy to access.

10.5.10 Security System Equipment and Interface

The SCC shall be the central point for all monitoring, controlling, programming, and service for all security systems. Back-up and secondary locations and related security equipment and capabilities shall be identified to support the SCC should it become inoperable. All security subsystems shall be fully integrated by either direct hardwiring of equipment or a computer based electronic Security Management System (SMS). The SCC shall house all head-end equipment and primary power sources for each security subsystem.

The SCC and security console shall be integrated with field-equipment through the proper location, layout, and horizontal and vertical access to designated riser space or secure closets/rooms where the transmission of information from security subsystems will transfer to the SCC. This includes establishing, identifying, and gaining authorized consensus on the use of stand-alone versus shared space requirements with other telecommunication space.

Equipment locations, such as wall space for new and upgraded security systems equipment shall be defined in relation to security conduit, power, and panel requirements. Accessibility to areas for installation and security purposes needs to be defined and proximity of these areas to the SCC from an operational efficiency and cost effective perspective shall be addressed.

All equipment that is rack mounted or installed in a security console shall be clearly labeled as to its identification. Labeling, such as in the case of CCTV monitors, may be programmed with a message embedded or programmed on the monitoring screen.

10. 6 DETECTION AND SCREENING SYSTEMS (DSS) OPTIONAL

Detection and Screening Systems (DSS) include: X-ray machines, walk-through metal detectors (WTMD), hand-held metal detectors (HHMD), and desktop and hand-held trace/particle detectors (also called sniffers and itemizers). The use of DSS equipment may be provided as an optional means for screening persons, items, and materials that may possess or contain weapons, contraband, or hazardous substances prior to authorizing entry or delivery into a facility. Use of DSS equipment may be considered during changes in the Homeland Security Alert System. Each facility shall be addressed on a case-by-case basis concerning the use of DSS.

10.6.1 System Elements and Features

DSS are used for the pre-screening of persons, packages, and personal items for detection of contraband; weapons, drugs, explosives, and other potential threatening items or materials prior to authorizing building entry or delivery. Refer to Appendix B, Security System Application Matrix, for optional locations where DSS may be utilized.

10.6.1.1 DSS system compatibility: All components of the DSS shall be fully compatible and shall not require the addition of either software or hardware interface equipment.

10.6.1.2 System integration: The DSS shall be fully integrated with other security subsystems. Refer to sections 10.1 and 10.4.

11 References

This section lists applicable codes and regulations, standards, design guidelines, and resources.

American Hospital Association (AHA)
American Society for Healthcare Engineering (ASHE)

- ASHE *The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) Environment of Care Security Standards* at http://www.ashe.org/ashe/codes/jcaho/ec/index.html

American Institute of Architects (AIA)
Academy of Architecture for Health (AAH)

- *Guidelines for Design and Construction of Health Care Facilities*, 2006

American National Standards Institute (ANSI)

- ANSI S3.2-1989(R1999): *Method for Measuring the Intelligibility of Speech over Communications System*
- ANSI/SIA CP-01-2000: *Control Panel Standard – Features for False Alarm Reduction*
- ANSI/SIA PIR-01-2000: *Passive Infrared Motion Detector Standard – Features for Enhancing False Alarm Immunity*

American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE)
American Society of Mechanical Engineers (ASME)

- ASME B20.1-2003 *Safety Standard for Conveyor and Related Equipment*

American Society for Testing and Materials (ASTM)

- ASTM C 1238: *Standard Guide for Installation of Walk-Through Metal Detectors, December 10, 1997*
- ASTM F 476-84(2002): *Standard Test Methods for Security of Swinging Door Assemblies*
- ASTM F 567-00: *Standard Practice for Installation of Chain-Link Fence*
- ASTM F 588-04: *Standard Test Methods for Measuring the Forced Entry Resistance of Window Assemblies, Excluding Glazing Impact*
- ASTM F 792-01e2: *Standard Practice for Evaluating the Imaging Performance of Security X-Ray Systems*
- ASTM F 842-04: *Standard Test Methods for Measuring the Forced Entry Resistance of Sliding Door Assemblies, Excluding Glazing Impact*
- ASTM F 883-04: *Standard Performance Specifications for Padlocks*
- ASTM F 1233-98(2004): *Standard Test Method for Security Glazing Materials and Systems*

Architectural and Transportation Barriers Compliance Board (Access Board)

- *Uniform Federal Accessibility Standards,* 1984

Central Station Alarm Association (CSAA)

- CSAA.STA1 *Standard Documents,* April 1996

Code of Federal Regulations (CFR)

- 7 Code of Federal Regulations 331and 9 Code of Federal Regulations 121 Agricultural Bioterrorism Protection Act of 2002: *Possession, Use, and Transfer of Biological Agents and Toxins*; Final Rule, March 18, 2005
- 14 CFR 108.17 and 129.26: *Use of X-Ray Systems*
- 21 CFR 1020.40: *Cabinet X-Ray Systems* (2006)
- 28 CFR Part 36-90: *ADA Standards for Accessible Design* (2006)

- 29 CFR 1910: *Occupational Safety and Health Standards* (2006)
- 36 CFR 1236.1236: *Management of Vital Records*, July 1, 1998
- 41 CFR 101-20.103-4: *Occupant Emergency Program*, July 1, 1998
- 42 CFR 72 & 73: *Possession, Use, and Transfer of Select Agents and Toxins*; Final Rule, March 18, 2005

Department of Defense (DoD)
Unified Facilities Criteria (UFC)

- *DoD Minimum Antiterrorism Standards for Buildings*, UFC 4-010-01, 8 October 2003 (Unrestricted)
- *DoD Security Engineering: Entry Control Facilities/Access Control Points*, UFC 4-002-01, 25 May 2005 (Unrestricted)
- *DoD Minimum Antiterrorism Stand-off Distances for Buildings*, UFC 4-010-10, 8 May 2002 (For Official Use Only)
- *Design of Buildings to Resist Progressive Collapse*, UFC 4-023-03, 25 January 2005 (Unrestricted)

Department of Health and Human Services (HHS)
Centers for Disease Control and Prevention (CDC)

- CDC list of high risk agents and material at http://www.cdc.gov/
- CDC-NIH Office of Health and Safety (OHS) *Biosafety in Microbiological and Biomedical Laboratories (BMBL)* 4th Edition, May 1999

Department of Homeland Security (DHS)
Federal Emergency Management Agency (FEMA)

- FEMA 426 *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* – Risk Management Series, December 2003
- FEMA 452 A *How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings* – Risk Management Series, January 2005

- Federal Preparedness Circular (FPC) 60: *Continuity of the Executive Branch of the Federal Government at Headquarters Level During National Security Emergencies*, November 20, 1990
- Federal Preparedness Circular (FPC) 65: *Federal Executive Branch Continuity of Operations*, July 29, 1999
- Homeland Security Presidential Directive (HSPD) 7: *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003
- Homeland Security Presidential Directive (HSPD) 12: *Policy for a Common Identification Standard for Federal Employees and Contractors,* August 27, 2004

Department of Justice (DOJ) Drug Enforcement Administration (DEA)

- Drug Enforcement Administration, Schedule II-V Drug Security http://www.deadiversion.usdoj.gov/21cfr/cfr/2108cfrt.htm

Department of Justice (DOJ) National Institute of Justice (NIJ)

- NIJ Standard 0108.01: *Ballistic Resistant Protective Material*, September 1985
- NIJ Standard 0601.02: *Walk-Through Metal Detectors for Use in Concealed Weapon and Contraband Detection*, January 2003
- NISTIR 6915: *The National Institute of Justice Standards for Hand-Held and Walk-Through Metal Detectors Used in Concealed Weapon and Contraband Detection*, October 2002

Department of State (DOS)

- SD-STD-01.01: *Forced Entry and Ballistic Resistance of Structural Systems,* April 30, 1993
- SD-STD-02.01: *Test Method for Vehicle Crash Testing of Perimeter Barriers and Gates,* March 2003

Department of Veterans Affairs (VA)

- VA Architectural Standard Details, Department of Veterans Affairs, Veterans Health Administration, Office of Facilities Management, Standard CAD Details Index
- VA Design Manuals, *Automatic Transport Systems*, February 2000
- VA Design Manuals, *Interior Design*, May 2006
- VA *Electrical Design Manual*, May 2006
- VA Handbook 0320 *Comprehensive Emergency Management Program*, March 24, 2005
- VA Handbook 0730 *Security and Law Enforcement*, Undated Current DRAFT
- VA Handbook 1200.06, *Control of Hazardous Agents in VA Research Laboratories*, October 21, 2005
- VA Handbook 1200.8, *Safety of Personnel Engaged in Research*, June 7, 2002
- VA Program Guide PG-18-3, *VHA - Design and Construction Procedures*, July, 2004
- VA Program Guide PG-18-9, *Space Planning Criteria for VA Facilities*, Undated
- VA Program Guide PG-18-10, *Architectural Design Manual*, May 2006
- VA Program Guide PG-18-14, *Room Finishes, Door and Hardware Schedule*, December 2004
- VA *Signage Design Guide*, 2/2005
- *Physical Security Design Standards Data Definitions*, 12/2006 (For Government Use Only)

Florida Department of Community Affairs

- Florida Building Code, www.floridabuilding.org

General Services Administration (GSA)

- *ISC Interagency Security Criteria for New Federal Office Buildings and Major Modernization Projects*, September 29, 2004 (For Official Use Only)

- GSA Rated Storage Containers http://www.gsa.gov/Portal/gsa/ep/programView.do?pageTypeId=8207&ooid=9760&programPage=%2Fep%2Fprogram%2FgsaDocument.jsp&programId=10598&channelId=-14005

- *Progressive Collapse Analysis and Design Guidelines for New Office Buildings and Major Modernization Projects,* June 2003

Government Accountability Office (GAO)

- GAO-03-8, *Building Security: Security Responsibilities for Federally Owned and Leased Facilities*, November 14, 2002

Institute of Electrical and Electronics Engineers (IEEE)

- IEEE C62.41.1-2002, *IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits*

- IEEE C95.1-1991, *Standards for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields*

International Code Council (ICC)

- International Building Codes, International Code Council

International Organization for Standardization (ISO)

- ISO 7816-1 1998: *Smart Card Standard: Physical Characteristics of Integrated Circuit Cards*

- ISO 7816-2 1999: *Smart Card Standard: Dimensions and Location of the Contacts*

- ISO 7816-3 2006: *Smart Card Standard: Electrical Signals and Transmission Protocols*

- ISO 7816-4 2005: *Smart Card Standard: Interindustry Commands for Interchange*

- ISO 14443 2003: *RFID cards; Contactless Proximity Cards Operating at 13.56 MHz in up to 5 inches distance*

- ISO 15693 2000: *RFID cards; Contactless Vicinity Cards Operating at 13.56 MHz in up to 50 inches distance*

National Electrical Contractors Association (NECA)

- NECA 303-2005, *Installing Closed-Circuit Television (CCTV) Systems*

National Electrical Manufactures Association (NEMA)

- NEMA 250-2003, *Enclosures for Electrical Equipment*

National Fire Protection Association (NFPA)

- NFPA 70 *National Electrical Code®*, 2005
- NFPA 101 *Life Safety Code®,* 2006
- NFPA 730 *Guide for Premises Security*, 2006
- NFPA 731 *Standard for the Installation of Electronic Premises Security Systems,* 2006
- NFPA *Extreme Event Mitigation in Buildings – Analysis and Design*, 2006

National Institute of Standards and Technology (NIST)

- Federal Information Processing Standards, FIPS Pub 201-1, *Personal Identification Verification (PIV) of Federal Employees and Contractors*, March 2006
- Interagency Reports, IR 6887, *Government Smart Card Interoperability Specification* (GSC-IS), v2.1, July 2003
- Special Publications 800-96 PIV, *Card/Reader Interoperability Guidelines,* September 2006

National Institutes of Health (NIH)

- NIH *Design Policy and Guidelines*, November 2003
- NIH *Guidelines for Research Involving Recombinant DNA Molecules,* Federal Register/Vol. 51, No. 88: 16957-16985

Occupational Safety and Health Administration (OSHA)

- OSHA 29 CFR 1926N.555 *Conveyer Belt Safety Standards* (2006)

Security Industry Association (SIA)

- SIA AC-01-1996.10: *Access Control Standard Protocol for the 26-bit Wiegand™ Reader Interface*
- SIA AC-03-2000.06: *Access Control Guideline Dye Sublimation Printing Practices for Access Control Cards*
- SIA AV-01-1997.11: *Audio Verification Standard - Protocol for Audio Verification and Two-Way Voice - Monitoring Service Command Set*
- SIA/IAPSC AG-01-1995.12(R2000.3): *Architectural Graphics Standard - CAD Symbols for Security System Layout - Release 2.0*

Underwriters Laboratories (UL)

- UL 50 *Standard for Enclosures for Electrical Equipment*, October 19, 1995
- UL 187 *Standard X-Ray Equipment*, April 30, 1998
- UL 294 *Standard for Access Control System Units*, January 29, 1999
- UL 305 *Standard for Panic Hardware*, January 31, 1997
- UL 444 *Communications Cables,* March 29, 2002
- UL 497C *Standard for Protectors for Coaxial Communications Circuits*, August 3, 2001
- UL 603 *Standard for Power Supplies for Use with Burglar-Alarm Systems*, March 26, 1998
- UL 609 *Standard for Local Burglar Alarm Units and Systems*, August 28, 1996
- UL 636 *Standard for Holdup Alarm Units and Systems,* November 26, 1996
- UL 639 *Standard for Intrusion-Detection Units,* February 21, 1997
- UL 681 *Standard for Installation and Classification of Burglar and Holdup Alarm Systems*, February 26, 1999
- UL 752 *Standard for Bullet-Resisting Equipment*, September 9, 2005
- UL 827 *Standard for Central-Station Alarm Services,* October 1, 1996

- UL 969 *Standard for Marking and Labeling Systems,* October 3, 1995
- UL 1481 *Standard for Power Supplies for Fire-Protective Signaling Systems,* December 12, 2006
- UL 1981 *Standard for Central-Station Automation Systems,* June 30, 2003
- UL 2058 *High-Security Electronic Locks*

U.S. Postal Service (USPS)

- Publication 166, *Mail Center Security Guidelines,* September 2002

The White House

- Executive Order 12472: *Assignment of national security and emergency preparedness telecommunications functions*, April 3, 1984
- Presidential Decision Directive (PPD) 62: *Protection Against Unconventional Threats to the Homeland and Americans Overseas,* May 22, 1998
- Presidential Decision Directive (PPD) 63: *Critical Infrastructure Protection*, May 22, 1998
- Presidential Decision Directive (PPD) 67: *Enduring Constitutional Government and Continuity of Government Operations*, October 21, 1998