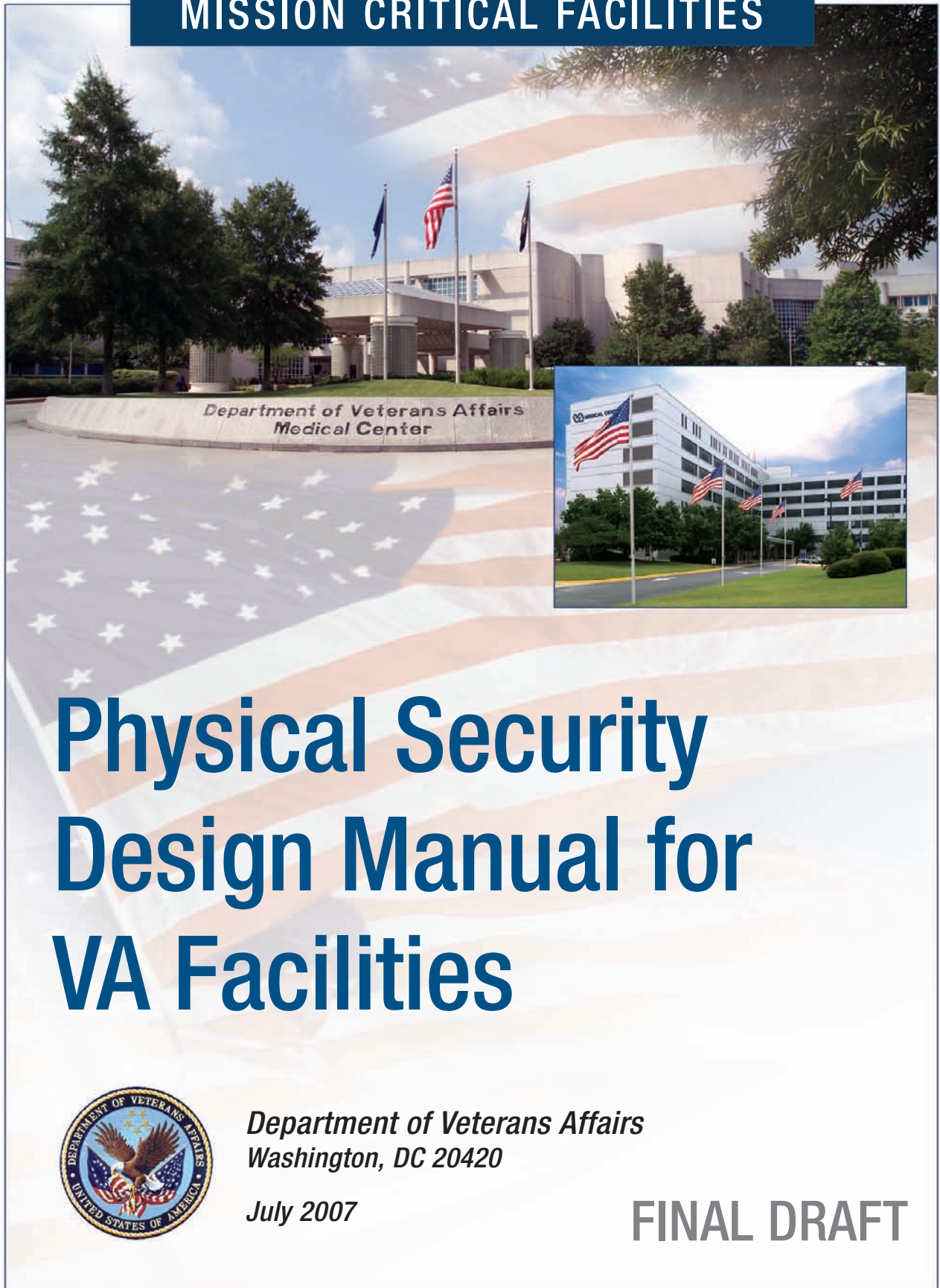


MISSION CRITICAL FACILITIES



Physical Security Design Manual for VA Facilities



*Department of Veterans Affairs
Washington, DC 20420*

July 2007

FINAL DRAFT

MISSION CRITICAL FACILITIES

Physical Security Design Manual for VA Facilities



*Department of Veterans Affairs
Washington, DC 20420*

July 2007

FINAL DRAFT

Project Team

Earle Kennett
Vice President
National Institute of Building Sciences
Washington, DC 20005

Nanne Davis Eliot, NCARB, Esq.
Project Manager
National Institute of Building Sciences
Washington, DC 20005

Stuart L. Knoop, FAIA
Principal
Oudens Knoop Knoop + Sachs Architects
Chevy Chase, MD 20815

Tom O. Sachs, AIA
Principal
Oudens Knoop Knoop + Sachs Architects
Chevy Chase, MD 20815

Eric J. Lorenz, AIA
Senior Architect
Oudens Knoop Knoop + Sachs Architects
Chevy Chase, MD 20815

Robert Smilowitz, PE, PhD
Principal
Weidlinger Associates, Inc.
New York, NY 10014

Peggy Van Eepoel, PE
Senior Structural Engineer
Weidlinger Associates, Inc.
Washington, DC 20006

William I. Nelson, PE
President
GLHN Architects & Engineers Inc.
Tucson, AZ 85716

Theodore C. Moeller, PE
Department Manager, Electrical Engineering
GLHN Architects & Engineers Inc.
Tucson, AZ 85716

John Lundgren, PE
Senior Mechanical Engineer
GLHN Architects & Engineers Inc.
Tucson, AZ 85716

Thomas A. Evans
Senior Electrical Designer
GLHN Architects & Engineers Inc.
Tucson, AZ 85716

Ellen G. Alexander
Project Manager
GLHN Architects & Engineers Inc.
Tucson, AZ 85716

J. Lisa Vickery
CAD Technician
GLHN Architects & Engineers Inc.
Tucson, AZ 85716

Robert A. Cizmada, CPP, FSO
Senior Program Manager
Risk Consulting Division
Post, Buckley, Schuh, & Jernigan, Inc.
Chantilly, VA 20151

Scott A. Matile
Security Specialist
Post, Buckley, Schuh, & Jernigan, Inc.
Chantilly, VA 20151

Walter Lee, CHS-IV
Senior Project Manager
Post, Buckley, Schuh, & Jernigan, Inc.
Chantilly, VA 20151

Phillip R. Waier, PE
Principal Engineer
RSMeans/Reed Construction Data
Kingston, MA 02364

Wanda Rizer
Publication Designer
design4impact
Abbottstown, PA 17301

Department Of Veterans Affairs Advisory Committee

Lloyd H. Siegel, FAIA
Director, Strategic Management Office
Office of Construction & Facilities Mgmt.
Department of Veterans Affairs
Washington, DC 20420

Kurt D. Knight, PE
Chief, Facilities Quality Service
Office of Construction & Facilities Mgmt.
Department of Veterans Affairs
Washington DC 20420

Marcelle Habibion, EdD
Director, Program Evaluation Service
Office of Policy, Planning, & Preparedness
Department of Veterans Affairs
Washington, DC 20420

Fred S. Lau, PE
Structural Engineer
Office of Construction & Facilities Mgmt.
Department of Veterans Affairs
Washington, DC 20420

William W. Graham, PE
Director of Operations Services
Office of Emergency Management
Department of Veterans Affairs
Washington, DC 20420

Keith Frost
Security Specialist
Team Leader, Policy and Security Operations
Office of Security & Law Enforcement
Department of Veterans Affairs
Washington, DC 20420

Scott A. Shorr
Industrial Engineer
Project Manager
Office of Facilities, Access & Administration
Veterans Benefits Administration
Washington, DC 20420

Katti Zand
Project Manager
Office of Facilities, Access & Administration

Veterans Benefits Administration
Washington, DC 20420

John D. Stenger
General Engineer
Veterans Health Administration
Department of Veterans Affairs
Washington, DC 20420

John D. Sourbeer
Architect
National Cemetery Administration
Department of Veterans Affairs
Washington, DC 20420

Louis Sinclair
Architect
National Cemetery Administration
Department of Veterans Affairs
Washington DC 20420

Ezra Safdie, PE
Director
Healthcare Engineering
Veterans Health Administration
Washington, DC 20420

Kevin Vassighi
Management Analyst
Assistant Secretary for Management
General Administration & Coordination Service
Department of Veterans Affairs
Washington, DC 20420

Patrick Villaloboz
Management Analyst
Assistant Secretary for Management
Office of Asset Enterprise Management
Department of Veterans Affairs
Washington, DC 20420

Julius Sztuk, AIA
Architect
Office of Construction & Facilities
Management
Department of Veterans Affairs
Washington, DC 20420

Table of Contents

1	Introduction	1-1
1.0	Purpose.....	1-1
1.1	Authority	1-2
1.2	VA Facilities.....	1-3
1.3	Introduction To Physical Security Concepts	1-4
1.3.1	Concentric Levels of Control and Protection	1-4
1.3.2	Crime Prevention Through Environmental Design (CPTED)....	1-5
1.3.3	Security Operation Requirements.....	1-5
1.4	Objectives of VA Physical Security Design	1-5
1.5	Budgeting and Programming for Physical Security.....	1-6
1.6	Risk Assessment of VA Facilities	1-6
1.7	Document Distribution, Use, and Control	1-6
1.8	Administration and Enforcement	1-7
1.9	Interpretations and Exceptions.....	1-7
1.10	Revisions.....	1-8
2	Glossary	2-1
3	Site Considerations.....	3-1
3.0	Scope.....	3-1
3.1	Stand-off Distance	3-1
3.1.1	Existing Facility – Stand-off Distance	3-1

3.2	Perimeter Fences	3-1
3.2.1	Location	3-1
3.2.2	Height.....	3-1
3.2.3	Material	3-2
3.2.4	Gates	3-2
3.2.5	Existing Facility – Perimeter Fences	3-2
3.3	Vehicle and Pedestrian Screening	3-2
3.3.1	Guard Houses.....	3-2
3.3.2	Vehicle Screening Area	3-2
3.3.3	Existing Facility – Vehicle and Pedestrian Screening.....	3-3
3.4	Vehicle Barriers	3-4
3.4.1	Active Barriers.....	3-4
3.4.2	Stationary (Passive) Barriers	3-4
3.4.3	Existing Facility – Vehicle Barriers	3-4
3.5	Parking	3-5
3.5.1	Location	3-5
3.5.2	Access	3-5
3.5.3	User Type	3-6
3.5.4	Existing Facility – Parking	3-6
3.6	Site Lighting	3-7
3.6.1	General Requirements.....	3-7
3.6.2	Lighting Locations	3-7
3.6.3	Existing Facility – Site Lighting	3-8
4	Building Entrances and Exits	4-1
4.0	Scope	4-1
4.1	Public Entrances and Lobbies	4-1
4.1.1	Entrances.....	4-1
4.1.2	Screening Vestibules	4-1
4.1.3	Public Entrances	4-2
4.1.4	Access for Emergency Responders	4-2
4.1.5	Planning, Construction Details, and Materials	4-2

4.1.6	Security Monitoring	4-3
4.1.7	Existing Facility – Entrances and Lobbies	4-4
4.2	Patient Drop-offs.....	4-5
4.2.1	Vehicular Access	4-5
4.2.2	Parking.....	4-5
4.2.3	Existing Facility – Patient Drop-offs	4-5
4.3	Building Exits and Life Safety Considerations.....	4-5
4.3.1	Site Requirements	4-5
4.3.2	Planning, Construction Details, and Materials	4-6
4.3.3	Security Monitoring	4-6
4.3.4	Existing Facility – Building Exits and Life Safety Considerations	4-6
5	Functional Areas.....	5-1
5.0	Scope.....	5-1
5.1	Agent Cashier	5-1
5.1.1	Adjacencies.....	5-1
5.1.2	Entrances.....	5-1
5.1.3	Construction.....	5-2
5.1.4	Security	5-2
5.1.5	Existing Facility – Agent Cashier	5-2
5.2	Cache.....	5-3
5.2.1	Adjacencies.....	5-3
5.2.2	Entrances.....	5-3
5.2.3	Construction.....	5-3
5.2.4	Security	5-4
5.2.5	Existing Facility – Cache.....	5-4
5.3	Childcare/Development Center.....	5-4
5.3.1	Adjacencies.....	5-4
5.3.2	Entrances.....	5-4
5.3.3	Construction.....	5-5
5.3.4	Security	5-5

5.3.5	Existing Facility – Childcare/Development Center	5-5
5.4	Computer Room	5-5
5.4.1	Adjacencies.....	5-5
5.4.2	Entrances.....	5-5
5.4.3	Construction.....	5-5
5.4.4	Security	5-6
5.4.5	Existing Facility – Computer Room.....	5-6
5.5	COOP Site.....	5-6
5.5.1	Adjacencies.....	5-6
5.5.2	Entrances.....	5-7
5.5.3	Construction.....	5-7
5.5.4	Security	5-8
5.5.5	Additional Requirements.....	5-8
5.5.6	Existing Facility – COOP Site	5-9
5.6	Emergency Department.....	5-9
5.6.1	Adjacencies.....	5-9
5.6.2	Entrances.....	5-9
5.6.3	Construction.....	5-10
5.6.4	Security	5-10
5.6.5	Existing Facility – Emergency Department.....	5-11
5.7	Emergency and/or Stand-by Generator Room	5-11
5.7.1	Adjacencies.....	5-11
5.7.2	Entrances	5-11
5.7.3	Construction.....	5-11
5.7.4	Security	5-11
5.7.5	Existing Facility – Emergency and/or Stand-by Generator Room	5-12
5.8	Energy Center/Boiler Plant	5-12
5.8.1	Adjacencies.....	5-12
5.8.2	Entrances.....	5-12
5.8.3	Construction.....	5-13
5.8.4	Security	5-13

5.8.5	Existing Facility – Energy Center/Boiler Plant	5-13
5.9	Loading Dock and Service Entrances	5-13
5.9.1	Adjacencies.....	5-13
5.9.2	Entrances.....	5-14
5.9.3	Construction.....	5-14
5.9.4	Security	5-15
5.9.5	Additional Requirements.....	5-15
5.9.6	Existing Facility – Loading Dock and Service Entrances	5-16
5.10	Mailroom.....	5-16
5.10.1	Adjacencies.....	5-16
5.10.2	Entrances.....	5-17
5.10.3	Construction.....	5-18
5.10.4	Security	5-18
5.10.5	Additional Requirements.....	5-18
5.10.6	Existing Facility – Mailroom	5-18
5.11	Pharmacy.....	5-18
5.11.1	Adjacencies.....	5-18
5.11.2	Entrances.....	5-19
5.11.3	Construction.....	5-19
5.11.4	Security	5-19
5.11.5	Existing Facility – Pharmacy	5-19
5.12	Police Operations Room and Holding Room.....	5-19
5.12.1	Adjacencies.....	5-19
5.12.2	Entrances.....	5-19
5.12.3	Construction.....	5-20
5.12.4	Security	5-20
5.12.5	Existing Facility – Police Operations Room and Holding Room	5-20
5.13	Records Storage and Archives.....	5-20
5.13.1	Adjacencies.....	5-20
5.13.2	Entrances.....	5-21
5.13.3	Construction.....	5-21

5.13.4	Security	5-21
5.13.5	Existing Facility – Records Storage and Archives	5-21
5.14	Research Laboratory and Vivarium	5-21
5.14.1	Adjacencies.....	5-22
5.14.2	Entrances.....	5-22
5.14.3	Construction.....	5-23
5.14.4	Security	5-24
5.14.5	Additional Requirements for Select Agent Storage	5-24
5.14.6	Existing Facility – Research Laboratory and Vivarium	5-24
5.15	Security Control Center (SCC)	5-25
5.15.1	Adjacencies.....	5-25
5.15.2	Entrances.....	5-25
5.15.3	Construction	5-25
5.15.4	Additional Requirements.....	5-26
5.15.5	Existing Facility – Security Control Center (SCC).....	5-26
6	Building Envelope	6-1
6.0	Scope	6-1
6.1	Walls	6-1
6.1.1	Non-load Bearing Walls	6-1
6.1.2	Existing Facility – Walls	6-2
6.2	Fenestration	6-2
6.2.1	Façade Fenestration	6-2
6.2.2	Existing Facility – Fenestration	6-2
6.3	Atria	6-3
6.3.1	Atria.....	6-3
6.3.2	Existing Facility – Atria	6-3
6.4	Roofs.....	6-3
6.4.1	Roof Structure.....	6-3
6.4.2	Skylights	6-4
6.4.3	Penthouses Enclosing Mission Critical Equipment	6-4

6.4.4	Existing Facility – Roofs	6-4
6.5	Air Intakes and Exhausts Servicing Mission Critical Equipment.....	6-4
6.5.1	Intakes and Exhausts.....	6-4
6.5.2	Existing Facility – Air Intakes and Exhausts Servicing Mission Critical Equipment.....	6-5
6.6	Calculation Methods.....	6-5
6.6.1	Design and Detailing.....	6-5
6.6.2	Blast Loads	6-5
6.6.3	Dynamic Response.....	6-6
7	Structural System	7-1
7.0	Scope.....	7-1
7.1	Blast Resistance.....	7-2
7.1.1	Priority for Protection	7-2
7.1.2	Existing Facility – Blast Resistance	7-2
7.2	Progressive Collapse.....	7-2
7.2.1	Existing Facility – Progressive Collapse	7-3
7.3	Column Protection.....	7-3
7.3.1	Existing Facility – Column Protection	7-3
7.4	Anti-ram Resistance	7-3
7.4.1	Vehicle Barriers.....	7-3
7.4.2	Existing Facility – Anti-ram Resistance	7-4
7.5	Calculation Methods.....	7-4
7.5.1	Design and Detailing.....	7-4
7.5.2	Blast Loading	7-4
7.5.3	Dynamic Response	7-4
8	Utilities and Building Services.....	8-1
8.0	Scope.....	8-1
8.1	Utility Entrances	8-1
8.1.1	Mechanical.....	8-1

8.1.2	Electrical	8-2
8.1.3	Telecommunications	8-2
8.1.4	Existing Facility – Utility Entrances	8-2
8.2	Site Distribution	8-3
8.2.1	Mechanical	8-3
8.2.2	Electrical	8-3
8.2.3	Telecommunications	8-3
8.2.4	Existing Facility – Site Distribution	8-4
8.3	Energy Center	8-4
8.3.1	Requirements	8-4
8.3.2	Sustained Service	8-4
8.3.3	Separation from Other Buildings	8-5
8.3.4	Stand-by Power	8-5
8.3.5	Long-Replacement-Time Equipment	8-5
8.3.6	Existing Facility – Energy Center	8-5
8.4	Water and Fuel Storage	8-5
8.4.1	Requirements	8-5
8.4.2	Storage Volume Criteria	8-5
8.4.3	Water Storage Emergency Connection	8-6
8.4.4	Water Treatment	8-6
8.4.5	On-site Water Well	8-6
8.4.6	Protection of Equipment	8-6
8.4.7	Existing Facility – Water and Fuel Storage	8-6
9	Building Systems	9-1
9.0	Scope	9-1
9.0.1	Modularity	9-1
9.0.2	Security Considerations	9-2
9.1	HVAC Systems	9-2
9.1.1	Requirements	9-2
9.1.2	Intakes and Exhausts	9-3
9.1.3	Existing Facility – HVAC Systems	9-3

9.2	Electrical Systems	9-3
9.2.1	Stand-by Power Systems	9-3
9.2.2	Uninterruptible Power Systems (UPS).....	9-4
9.2.3	Existing Facility – Electrical Systems.....	9-4
9.3	Telecommunications Systems	9-5
9.3.1	Demarcation Room (DEMARC).....	9-5
9.3.2	Telephone Equipment Room	9-5
9.3.3	Main Computer Room.....	9-6
9.3.4	Telecommunications Distribution Rooms	9-6
9.3.5	WLAN System	9-7
9.3.6	Portable Radio System	9-7
9.3.7	Satellite Radiotelephone System.....	9-8
9.3.8	Public Address System	9-8
9.3.9	Distributed Antenna System	9-9
9.3.10	VSAT Satellite Data Terminal	9-9
9.3.11	Existing Facility – Telecommunications Systems	9-9
9.4	Plumbing Systems	9-10
9.4.1	Medical Air and Oxygen Systems.....	9-10
9.4.2	Existing Facility – Plumbing Systems	9-10
9.5	Fire Protection Systems	9-10
9.5.1	Fire Department Hose Connections	9-10
9.5.2	Existing Facility – Fire Protection Systems.....	9-10
10	Security Systems	10-1
10.0	Scope	10-1
10.1	CCTV Monitoring and Surveillance (CCTV)	10-1
10.1.1	System Uses, Compatibility, and Integration	10-2
10.1.2	Networked versus Stand-alone CCTV System	10-2
10.1.3	Cameras	10-2
10.1.4	Additional CCTV System Components.....	10-6
10.1.5	Controlling and Recording Equipment	10-7
10.1.6	Video Motion Detection.....	10-8

10.1.7	Camera Locations	10-8
10.2	Intrusion Detection System (IDS)	10-9
10.2.1	System Elements and Features.....	10-9
10.2.2	System Integration	10-9
10.2.3	Planning and Selection Criteria	10-9
10.2.4	Networked versus Stand-alone.....	10-10
10.2.5	Hardwired versus Wireless	10-10
10.2.6	Environmental Conditions	10-10
10.2.7	Interior Sensors	10-10
10.2.8	Exterior Sensors	10-12
10.2.9	Alarm Conditions	10-12
10.2.10	Installation	10-13
10.2.11	IDS Locations	10-13
10.3	Physical Access Control System (PACS)	10-13
10.3.1	System Elements and Features	10-13
10.3.2	System Integration.....	10-13
10.3.3	Stand-alone versus Network Multiple-Portal System.....	10-13
10.3.4	Control/Communications Panel	10-14
10.3.5	Electronic Security Management System (SMS)	10-14
10.3.6	Picture ID and Badging Station Interface	10-15
10.3.7	Card Credentials and Readers	10-15
10.3.8	Entry Control Device	10-15
10.3.9	Biometric Systems	10-15
10.3.10	Portal Control Devices	10-15
10.3.11	Door Status Indicators	10-16
10.3.12	Transmission Media	10-16
10.3.13	Locations	10-16
10.4	Duress, Security Phones, and Intercom System (DSPI)	10-16
10.4.1	System Elements and Features	10-16
10.4.2	Security Phones or Emergency Call-Boxes	10-18
10.4.3	Duress/Panic Alarms	10-19
10.4.4	DSPI Locations	10-21

10.5 Security Control Center (SCC)..... 10-21

10.5.1 Operational Requirements..... 10-21

10.5.2 Primary and Secondary Locations..... 10-21

10.5.3 Accessibility 10-22

10.5.4 Physical Security 10-22

10.5.5 Construction..... 10-22

10.5.6 Space Requirements 10-22

10.5.7 Electrical 10-23

10.5.8 Environmental Applications 10-23

10.5.9 Security Console/Workstation 10-24

10.5.10 Security System Equipment and Interface..... 10-24

10.6 Detection and Screening Systems (DSS) Optional 10-25

10.6.1 System Elements and Features 10-25

11 References 11-1

Appendices

A Security Door Openings (SDO)..... A-1

B Security System Application Matrix..... B-1

Index

Introduction

1.0 PURPOSE

This Manual contains the physical security standards for improving the protection of mission critical facilities of the U.S. Department of Veterans Affairs (VA). Mission Critical facilities are those required to continue operation during a natural or man-made extreme event. Design and construction standards are provided for the physical security of new buildings, additions, and major alterations. In addition, recommendations and strategies are provided to improve the physical security for existing mission critical facilities.

The requirements of this manual are to be coordinated with all VA design and construction requirements for the mitigation of other hazards, such as earthquake and hurricane, in order to complete a multi-hazard approach to physical security planning, design, and construction. Throughout this manual 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>.

In order to meet the physical security standards of this manual the design team must include a security specialist as well as a structural blast specialist. These specialists must be experts and have a minimum of five years experience in physical security or blast design. This manual assumes the use of qualified security and blast experts.

1.1 AUTHORITY

It has long been the policy of the United States to assure the continuity and viability of mission critical infrastructure. Executive Order 12656, issued November 18, 1988, states, “The head of each Federal department and agency shall be prepared to respond adequately to all national security emergencies.” Furthermore, the “head of each Federal department and agency shall ensure the continuity of essential functions in any national security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities.” The Order also requires that the “head of each Federal department and agency shall: identify facilities and resources, both government and private, essential to the national defense and national welfare, and assess their vulnerabilities and develop strategies, plans, and programs to provide for the security of such facilities and resources, and to avoid or minimize disruptions of essential services during any national security emergency.”

Public Law 107-188, Public Health Security and Bioterrorism Preparedness and Response Act of 2002 enacted June 12, 2002, requires actions to enhance the readiness of Department of Veterans Affairs medical centers to enable them to fulfill their obligations as part of the Federal response to public health emergencies. Under section 154 the law specifically requires that the “Secretary of Veterans Affairs shall take appropriate actions to enhance the readiness of Department of Veterans Affairs medical centers to protect the patients and staff of such centers from chemical or biological attack or otherwise to respond to such an attack and so as to enable such centers to fulfill their obligations as part of the Federal response to public health emergencies.”

Public Law 107-287, Department of Veterans Affairs Emergency Preparedness Act of 2002 enacted November 7, 2002, requires that the “Secretary take appropriate actions to provide for the readiness of Department medical centers to protect the patients and staff of such centers from chemical or biological attack or otherwise to respond to such an attack so as to enable such centers to fulfill their obligations as part of the Federal response to public health emergencies” and that the “Secretary take appropriate actions to provide for the security of Department medical centers and research facilities, including staff and patients at such centers and facilities.” This Act also states that the “Secretary may furnish hospital care and medical services to individuals responding to, involved in, or otherwise affected by that disaster or emergency.”

38 USC Sec. 901 gives the Secretary the authority to prescribe regulations to provide for the maintenance of law and order and the protection of persons and property on VA property.

1.2 VA FACILITIES

The Department of Veterans Affairs (VA) is composed of a Central Office (VACO) and three administrations, the Veterans Health Administration (VHA), the Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA). VHA manages one of the largest health care systems in the U.S. In addition to providing health care, VHA also has missions to provide training for health care professionals; to conduct medical research; to serve as a contingency backup to DoD medical services; and, during national emergencies, to support the National Disaster Medical System (NDMS). VBA provides benefits and services to veterans including compensation and pension, education, loan guaranty, and insurance. NCA delivers burial benefits to veterans and eligible dependents. In total, VA provides a mission critical medical and economic infrastructure to the government and population of the United States.

Mission critical facilities shall include all of the following:

- | | |
|--------------------------------|---|
| ■ Acute Care | ■ Ambulatory Care |
| ■ Animal Facility | ■ Boiler Plant |
| ■ Communications Center | ■ Consolidated Mail-Out Pharmacy |
| ■ Dietetics | ■ Domiciliary |
| ■ Drug/Alcohol Rehabilitation | ■ Emergency Command Center |
| ■ Emergency Generator | ■ Fire/Police Station |
| ■ Hazardous Material Storage | ■ Hospital |
| ■ Information Technology | ■ Long-Term Care |
| ■ Medical Equipment Storage | ■ Medical Gas Storage |
| ■ Medical Records | ■ Medical Research |
| ■ Mental Health – Inpatient | ■ National Continuity of Operations Center |
| ■ Outpatient Clinic | ■ Psychiatric Care Facility |
| ■ Rehabilitation Medicine | ■ Rehabilitation/Prosthetics |
| ■ Security and Law Enforcement | ■ Water Tower, Utility Supply Storage Structure |

1.3 INTRODUCTION TO PHYSICAL SECURITY CONCEPTS

VA has adopted the medium level of protection of the *Interagency Security Committee (ISC) Security Design Criteria* (September 29, 2004) for all new mission critical facilities. The *VA Natural Disaster Non-Structural Resistive Design* (September 2002) is subsumed and superseded by this physical security design manual. The physical protection strategies used to develop this manual are documented in the *Physical Security Strategies Report* (January 10, 2006).

1.3.1 Concentric Levels of Control and Protection

The physical security of facilities requires the use of concentric levels of control and protection to provide progressively enhanced levels of security.

1.3.1.1 The first point of control should be at the perimeter of the property consisting of fences and other barriers with one or two points of entry through gates controlled by police or other guard personnel. In certain urban sites, the building perimeter may be on the property line. Increased levels of screening of persons and vehicles, as the Department of Homeland Security Threat Levels are changed, must be accommodated at the perimeter without burdening surrounding roads with vehicles waiting to enter the site.

1.3.1.2 The second point of control should be at the building perimeter consisting of doors and other openings protected as appropriate to the level of protection needed with or without the first point of control. This includes access control hardware, intrusion detection, surveillance, and, at selected entrances at various times, personnel for control and screening.

1.3.1.3 The third point of control should be to segregate with barriers and hardware generally accessible public and patient areas from staff-only areas such as pharmacy preparation, food preparation, sterile corridors, research laboratories, and building operations and maintenance areas.

1.3.1.4 The fourth point of control should be to segregate authorized from unauthorized staff areas with barriers and access controls such as card reader-activated hardware. Unauthorized areas may include patient records, laboratories, vivariums, and cash-handling tellers.

1.3.1.5 The fifth point of control should be to restrict access to restricted areas to a minimum with card-reader access controls, CCTV monitors, intrusion detection alarms, and forced-entry-resistant construction. Restricted access areas may include select agent storage, narcotics storage and pharmaceutical caches, laboratories, and COOP sites.

The more effective the perimeter barrier and screening are the less protection is needed within the site, such as between buildings, from patient and visitor parking and the building lobby, and from the site entrance to the other buildings on the site. In highly urban areas where the VA building may front on a city street with no stand-off or separation, the building and its occupants can only be protected from hazards of breaking and entering, vandalism, and even explosive or armed attack by hardening the building itself to resist, which may lead to undesirable solutions such as façades with minimum openings and a fortress-like appearance.

1.3.2 Crime Prevention Through Environmental Design (CPTED)

VA follows the principles of Crime Prevention Through Environmental Design (CPTED, see www.cpted.net). CPTED promotes the principles that proper design and effective use of the built environment can lead to a reduction in the fear and incidence of crime and acts of terrorism. CPTED should be used to evaluate VA site and building designs to create and enhance the concentric circles or layers of security protection.

1.3.3 Security Operation Requirements

Design decisions for the physical security of a mission critical facility should be based on the concentric levels of control and protection—both physical and operational—as described in section 1.3.1.

1.4 OBJECTIVES OF VA PHYSICAL SECURITY DESIGN

The primary objective of this manual is to provide the design team with the criteria and standards for the full range of strategies available for existing and new buildings to provide unobtrusive protection for VA facilities while safeguarding the veterans, staff, visitors, and continued operation of the mission critical facilities during a national emergency or a natural or man-made extreme event.

The physical security standards account for VA operations and policies and must be cost effective when implemented. An objective of this manual is to provide cost effective design criteria that will, when constructed and implemented, provide the appropriate level of physical security to VA's mission critical facilities. The *Physical Security Cost Manual* should be used by the design team in conjunction with this manual to determine and develop the most cost effective physical security for each mission critical facility.

1.5 BUDGETING AND PROGRAMMING FOR PHYSICAL SECURITY

When establishing a design and a budget for a mission critical project, the key point is that physical security is fully integrated into the program, rather than an added requirement. When physical security is seen as an add-on to an otherwise complete project, the costs for implementation will be higher and the results less satisfactory. As such, it is essential to establish the physical security goals within the programming phase of the project and to ensure that the budget is set to reflect the physical security requirements within the program goals.

1.6 RISK ASSESSMENT OF VA FACILITIES

Risk assessments of existing VA facilities showed that the primary threats faced by the Department continue to be routine criminal activity and violence in the workplace; however, the proximity of some VA facilities to high vulnerability targets, the expanded threat caused by the Iraqi War and treatment of Iraqi War veterans, and the role of VA medical centers as backup to DoD and communities in the public health system, elevate VA's risks from both internal and external man-made threats.

It is not possible to eliminate all risk to a facility and every project will face resource limitations. Cost effective risk management is a requirement of every project. Prior to design development of a new mission critical facility or major alterations of an existing mission critical facility a risk assessment must be performed. Cost effective strategies must be implemented to make the facility capable of mission critical operation.

The first task is to identify the assets and people that need to be protected. Next, a threat assessment is performed to identify and define the threats and hazards that could cause harm to a building and its occupants. After threats and assets are identified, a vulnerability assessment is performed to identify weaknesses. Using the results of the asset, threat, and vulnerability assessment, risk can be determined.

Comprehensive protection against the full range of possible natural and man-made threats to VA facilities would be cost prohibitive, but an appropriate level of protection obtained through the use of these standards can provide for continued operation of mission critical facilities at a reasonable cost.

1.7 DOCUMENT DISTRIBUTION, USE, AND CONTROL

This manual is unclassified.

1.8 ADMINISTRATION AND ENFORCEMENT

The provisions of these standards shall apply to all VA mission critical construction projects for which design is begun on or after the effective date of this design manual.

These standards apply to new construction and all additions, alterations, and modernization. Any facility undergoing a renovation of 50 percent or greater is required to conform to the standards of a new mission critical facility. Existing facilities are required to meet physical security standards defined in this design manual as may be determined by VA based on funding considerations, prioritization, and other mission driven requirements.

These standards apply to the space being renovated in an existing building, and do not extend to other spaces in the same building except as may be directed by VA.

Any VA campus on which a new mission critical facility is to be constructed shall bring the entire site into conformance with these standards.

1.9 INTERPRETATIONS AND EXCEPTIONS

VA facilities that are not designated mission critical are life-safety protected. Life-Safety Protected buildings, which are required to protect the life safety of the patients, staff, and visitors in case of an emergency; although indispensable to the mission of VA, are not required to remain operational in a natural or man-made extreme event or a national emergency. Physical security design requirements for life-safety protected facilities are covered in a separate manual.

The requirements of these standards are directed at all building types currently owned and operated by VA. VA buildings leased through the General Services Administration (GSA) are exempt from these requirements and are covered in the *Interagency Security Committee (ISC) "Security Standards for Leased Spaces"* (September 29, 2004).

Connecting corridor concourse and bridges shall be exempt from the stand-off distance requirements of Chapter 3 and the requirements of Chapters 6 and 7. Freestanding greenhouses shall be exempt from the requirements of Chapters 3, 6, and 7. Physical security requirements for temporary buildings shall be determined on a case by case basis by the security staff having cognizance.

The Project Manager has the role of approving deviations from the requirements and may waive requirements and give other instructions.

1.10 REVISIONS

Revisions to the Physical Security Design Manual will be issued shortly after the initial publication due to VA office re-organization, numbering and nomenclature changes, and updates of other VA standards.

Glossary

The following terms and definitions are related to the mitigation of man-made and natural hazards and do not include terms related to general facility design, construction, and operation.

Cache: A storage facility requiring a high level of security, often referring to pharmacy.

Charge Weight: The amount of explosives in a device in TNT equivalent.

Clear Zone: An area on either or both sides of a perimeter fence line that has been cleared of any materials that offer concealment to an intruder.

Closed Circuit Television (CCTV): A video system in which an analog or digital signal travels from a camera to video monitoring stations at a designated location.

Continuity of Operations (COOP): VA is required to have COOP capabilities that enable the Department to continue essential functions during a broad spectrum of emergencies. A COOP site is an alternate facility from which to continue essential agency functions should the primary facility be rendered unusable. A COOP site should provide a facility from which VA can continue to perform essential functions and operations during an emergency with reduced or mitigated disruptions to operations and where VA can achieve a timely and orderly recovery from an emergency and resume full service.

Controlled Access Area or Controlled Area: A room, office, building, or facility area which is clearly demarcated, access to which is monitored, limited, and controlled.

Crash-rated: Tested for resistance to a moving load impact at a given velocity and rated in terms of kinetic energy or “K” rating in tests for certification under Department of State programs.

Crime Prevention Through Environmental Design (CPTED): Design philosophy that effective use of the natural environment coupled with proper design of the built environment can lead to a reduction in the fear and incidence of crime.

Critical Assets: People and those physical assets required to sustain or support the facility's ability to operate on an emergency basis.

Critical Infrastructure, Critical Space: Building area(s) required to sustain or support the facility's ability to operate on an emergency basis.

Detection and Screening System (DSS): DSS are used for the pre-screening of persons, packages, and personal items for detection of contraband, such as, weapons, drugs, explosives, and other potential threatening items or materials prior to authorizing entry or delivery into the building. DSS includes X-ray machines, walk-through metal detectors (WTMD), hand-held metal detectors (HHMD), and desktop and hand-held trace/particle detectors (also referred to a "sniffers" and "itemizers").

Duress Security Phone Intercom (DSPI): DSPI systems are used to provide security intercommunications for access control, emergency assistance, and identification of personnel under duress requesting a security response.

Explosives Detector: Any device that detects components of explosive devices or explosive compounds by radiographic analysis, by analyzing chemical emissions, or by other methods.

Extraordinary Incidents: Events or conditions that exceed locally accepted design practice.

Hardening: Reinforcement of the building structure, components, and systems against impact of a blast, a ballistic assault, or ramming.

High Crime Area: Within a defined geographical location, the area with the highest arrest rates for violent crime and for such other crimes as drug sale, drug possession, prostitution, vandalism, and civil disturbances; with the highest reported crime volume of specific property crimes such as business and residential burglary, motor vehicle theft, and vandalism; the highest percentage of reported index crimes that are violent in nature; the highest overall index crime volume for the area; and the highest overall index crime rate for the geographic area.

Hurricane Areas: These requirements apply to VA medical and ambulatory care centers located within 16 kilometers (10 miles) of the Atlantic Ocean and 16 kilometers (10 miles) of the Gulf of Mexico. These requirements also apply to all inland VA medical and ambulatory care centers in Florida and those in Hawaii and Puerto Rico.

ID Check: Examination and verification of personal or vehicle identification visually or by other means.

Intrusion Detection System (IDS): A system combining mechanical or electric components to perform the functions of sensing, controlling, and announcing unauthorized entry into areas covered by the system. The IDS is intended to sound alarms or alert response personnel of an actual or attempted intrusion into an area.

Itemizer: A trace particle detection device capable of identifying both explosives and narcotics.

Life-Safety Protected: VA facilities which are required to protect the life safety of the patients, staff, and visitors in case of an emergency; although indispensable to the mission of VA, are not required to remain operational in a natural or man-made extreme event or a national emergency.

Local Alarm: An alarm that is annunciated in the immediate vicinity of the protected premises.

Magnetometer or Metal Detector: A walk-through portal or hand-held device designed to detect changes in magnetic fields used to identify hidden metal objects.

Mantrap: A double-door booth or chamber that allows a person to enter at one end, undergo an access identification routine inside the booth, and if the routine is satisfied, the lock on the booth door at other end is released.

Mission Critical: VA facility that is required to continue operation during a natural or man-made extreme event or a national emergency.

Mitigation: Actions taken to reduce the exposure to and impact of a hazard.

Pedestrian Barrier: A fence, wall, or other structure designed to delay pedestrians from entering the site without using the gates provided for pedestrians where *personnel screening* may be performed. The Pedestrian Barrier may or may not be coincident with the *vehicle barrier*.

Perimeter Barrier: A physical barrier used on the outside of a protected area to prevent, deter, or delay unauthorized entry.

Personnel Screening: Examining persons and their possessions for contraband such as weapons, explosives, and CBR agents using magnetometer, x-ray, search, or other device.

Physical Access Control System (PACS): A system combining mechanical or electrical components, such as card readers, keypads, biometrics, and electromagnetic locks and strikes, for the purpose of controlling access and monitoring building entrances, sensitive areas, mission critical asset areas, and alarm conditions.

Physical Security: That part of security concerned with physical measures designed to safeguard people, to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard against damage and loss.

Police Operations Unit: An area designed to facilitate the functions of the police and security services, which include the protection of patients, visitors, and employees; the protection of property; and the maintenance of law and order on property under the charge and control of the Department.

Protected Area: An area continuously protected by physical security safeguards and access controls.

Protection Level: The degree to which resources are used to defeat a threat.

Restricted Area: A controlled room, office, building, or facility area to which access is strictly and tightly controlled. Admittance to this area is limited to personnel assigned to the area and persons who have been specifically authorized access to the area.

Risk: The potential for a loss of or damage to an asset.

Screening Vestibule: Designated space or area located for access control between the public building entrance and the lobby which shall be of sufficient space and be provided with power, telecommunications, and data connections for installation of access control and screening equipment that may be used should the need arise.

Secured Door Opening (SDO): A door opening that requires security hardware such as electric strike, door contact, card reader, forced entry rating, or similar feature.

Security Control Center (SCC): A location for security personnel to monitor CCTV, alarms, and other security systems and devices. This may be in a separate space or, for small facilities, combined with a guard or reception desk at the entrance.

Select Agent: Select agents shall be as defined in Title 42, CFR, Part 73, including pathogens and toxins regulated by both DHHS and USDA and non-overlap select agents of DHHS.

Stand-off: Distance from event to target.

Tactic: Means of delivering a threat, such as a vehicle bomb.

Terrorism: An action that is intended to cause death or serious bodily harm to civilians or noncombatants, when the purpose of such an act, by its nature or context, is to intimidate a population or to compel a government or an international organization to do or to abstain from doing any act.

Threat: An indication of impending danger. The type of harm likely to be directed at a facility.

Urban Area: A geographic area with a population of more than 50,000 or a population density of at least 1,000 people per square mile (386 per square kilometer) and surrounding census blocks that have an overall density of at least 500 people per square mile (193 per square kilometer).

Vehicle Arrest: Means of stopping a vehicle from breaching a perimeter.

Vehicle Barrier: A passive or active physical barrier consisting of natural or man-made features designed to keep a vehicle carrying explosives at the required *stand-off* distance. This may or may not be coincident with a *pedestrian barrier*.

Vehicle Inspection: Examining vehicles for contraband such as explosives using physical search, K-9 searches, trace element sampling, x-ray, or other means.

Vulnerability: Susceptibility to physical injury or *threat*.

X-ray Screening System: A device or system that inspects the contents of a package or container for concealed explosives or contraband.

Site Considerations

3.0 SCOPE

This chapter focuses on security design concepts, elements, and site planning strategies that influence the protection of the built and natural environments.

3.1 STAND-OFF DISTANCE

No vehicle shall be parked or be permitted to travel closer than 50 feet (15 m) to any mission critical VA facility.

3.1.1 Existing Facility – Stand-off Distance

Requirements for stand-off distance at existing facilities shall be the same as in section 3.1.

3.2 PERIMETER FENCES

Perimeter barriers shall consist of fences, walls, a combination of these, and gates as needed for access. The barrier shall be designed to resist forced or surreptitious entry using hand tools, such as by spreading bars of a fence to provide a passable opening. Fences shall have sufficient lateral support to resist overturning by manual force.

3.2.1 Location

The perimeter barrier shall be on or in close proximity to the perimeter of the property.

3.2.2 Height

The perimeter barrier shall have at least 8 feet (2.4 m) between potential horizontal footholds or designed with other anti-climb measures.

3.2.3 Material

Fences shall be metal and of heavy industrial-grade construction with bar spacing at a maximum of 5 inches (127 mm) on center. Chain link fences and gates shall not be used. Walls shall be reinforced masonry or concrete.

3.2.4 Gates

Gates shall be of the same or similar design and materials as the adjacent fences. Gates shall be access card operated from the outside or as prescribed by the Project Manager.

3.2.4.1 Pedestrian gates: Pedestrian and bicycle gates shall swing in the outward direction and shall be fully accessible to persons with disabilities in width and operation.

3.2.4.2 Vehicular gates: Vehicular security gates shall be sliding or cantilevered (no tracks) and only wide enough to accommodate one vehicle lane.

3.2.5 Existing Facility – Perimeter Fences

All sites with mission critical facilities shall have perimeter fences meeting all the requirements of section 3.2.

3.3 VEHICLE AND PEDESTRIAN SCREENING

3.3.1 Guard Houses

Pedestrian and vehicle perimeter entrances shall be provided with enclosed guard houses for guard personnel, gate operation, vehicle inspection, and information.

- Guard house design shall be compatible with the facility architecture and the neighborhood.
- Guard houses shall be heated, air conditioned, and lighted to provide an appropriate work environment.
- Guard houses shall be provided with power, telephone, intercom, data, and other equipment as directed by the VA Police.

3.3.2 Vehicle Screening Area

Provide adequate space to accommodate vehicle screening without blocking public rights-of-way. The screening area shall provide adequate space and site utilities to accomplish the following tasks.

- Visual identity check of driver's license.
- Visual inspection of vehicle interior, including luggage compartment.
- Trace element swipes and sensors.

3.3.2.1 Stacking space: Stacking space shall be provided for vehicles awaiting inspection outside site entrance and off public roads.

- At entrances for employee vehicles, the stacking space shall be sufficient to handle the throughput of vehicles at peak inbound levels.
- At public entrances, stacking space shall be sufficient for average visitor vehicle traffic volume and include space to pull a vehicle aside out of the lane of inbound traffic.

3.3.2.2 Separation: In-bound and out-bound vehicles shall have separate lanes and gates at all vehicular entrances.

3.3.2.3 Reject lane: A turn-around lane shall be provided on the exterior of the entrance gate to permit vehicles to be sent away without interfering with traffic.

3.3.2.4 Parking: Parking shall be provided inside the entrance gate for two police vehicles.

3.3.2.5 Public transportation: Where public transportation is allowed on the VA site for employees and visitors, space shall be provided for the vehicle to be inspected.

3.3.3 Existing Facility – Vehicle and Pedestrian Screening

3.3.3.1 Pedestrian barriers and screening: Pedestrian barriers as described in section 3.2 shall be installed at any site with an existing mission critical facility.

3.3.3.2 Vehicle barriers and screening: Vehicle barriers as described in sections 3.2, 3.3, and 3.4 shall be installed at any site on which there are mission critical facilities.

- Site utility surveys shall be conducted prior to design and installation.
- Foundations for anchoring the barriers shall be coordinated with existing underground features such as utilities, tunnels, or other subsurface conditions.

3.4 VEHICLE BARRIERS

Active or passive vehicle barriers shall be selected on the appropriateness of the architecture of the facility and the specifics of the site and natural environment.

3.4.1 Active Barriers

Types of active barriers shall be hydraulic wedges or bollards recessed into the pavement for a flush condition when not deployed.

3.4.1.1 Locations: Active vehicle barriers shall be located inside all vehicular perimeter entrance and exit gates at a distance that permits guard personnel adequate response time for deployment.

3.4.1.2 Structure: See Chapter 7, section 7.4 Anti-ram Resistance, for structural requirements of active barriers.

3.4.2 Stationary (Passive) Barriers

Natural or man-made stationary barriers may be used.

- Landscaping examples include berms, gullies, boulders, trees, and other terrain.
- Hardscaping examples include benches and planters.
- Structural examples include walls, bollards, and cables.

3.4.2.1 Locations: Adjacent to vulnerable perimeter fences, protection for site utility equipment, at building entrance, and other areas requiring additional protection from vehicles.

3.4.2.2 Structure: See Chapter 7, section 7.4 Anti-ram Resistance, for structural requirements of passive barriers.

3.4.2.3 Handicapped accessibility: Passive barriers, such as bollards, when placed adjacent to or across a path of pedestrian travel, shall have 4 feet (1.2 m) clear space in between.

3.4.3 Existing Facility – Vehicle Barriers

All sites with mission critical facilities shall have vehicle barriers installed in accordance with section 3.4.

3.5 PARKING

3.5.1 Location

3.5.1.1 Surface parking: Passenger vehicles shall not be parked or permitted to travel closer than 50 feet (15 m) to any VA facility.

3.5.1.2 Parking structures

3.5.1.2.1 Separate from VA facility: No parking structure, whether on or off site, shall be constructed closer than the following to any VA facility.

- Underground: no limit
- Above ground: same as for surface parking

3.5.1.2.2 In or under VA facility: Parking in or under a VA facility shall be restricted.

- No unscreened visitor vehicle shall be permitted within or under any VA facility.
- Official government-owned vehicles, regularly garaged in the facility and inspected for covertly placed explosives after leaving and returning to the facility, shall be permitted within or under any VA facility.
- At the discretion of the VA Police, selected employee-owned vehicles, regularly inspected for covertly placed explosives after leaving and returning to the facility, may be permitted within or under any VA facility.

3.5.2 Access

3.5.2.1 From vehicle entrance: Access roads for all vehicles shall allow for separate driveways to the building entrance, service yard, or parking.

- Separate entrances to the site shall be provided for patients and visitors, employees and staff, emergency, and service and delivery vehicles.
- Access roads from entrances to parking for each vehicle type shall be separated, but may be connected for maintenance and emergency vehicles through gates controlled by access cards.
- Access roads shall be configured to prevent vehicles from attaining speeds in excess of 25 mph (40 kph).
- Straight-line vehicular approaches to a facility shall be avoided.

3.5.2.2 From parking to facility: See Chapter 4 for further information on building entrances.

3.5.3 User Type

In addition to the requirements of sections 3.5.1 and 3.5.2, the following are parking and access requirements for physical security according to specific users.

3.5.3.1 Patients and visitors: Parking and access for patients, visitors, and the persons transporting them to and from the VA facility shall be as convenient as possible to the main entrance, subject to the requirements of section 3.5.1.1. Parking and facility access shall comply with handicapped accessibility requirements.

- Where vehicles are unscreened, make site provisions to accommodate a shuttle service for persons needing assistance.

- Accessible shuttle stops or shelters in parking areas.

- Shuttle parking at building entrance.

3.5.3.2 Emergency: Emergency entrance shall be provided with a small parking area for emergency patients and space for ambulances. Ambulances shall be permitted to approach the building directly and not be subjected to the distance requirements of this chapter.

3.5.3.3 Childcare parents and staff: All requirements for maintaining stand-off distance between vehicles and the building shall apply. Child drop-off and pick-up shall be visible from the office of the childcare/development center and shall be monitored by CCTV. All vehicular areas, on site and adjacent off-site, including parking and access roads, shall be separated from playground areas by fences designed to prevent children from entering the vehicular areas and vehicles from entering the playground.

3.5.3.4 Vendors: The stand-off distance and screening requirements of sections 3.1 and 3.3 apply. Vendors shall use the delivery vehicle entrance and service yard at the loading dock. Parking shall be provided for vendors in the service yard.

3.5.3.6 Employees: Where employees share access with patients and visitors, the entrance to the employee parking shall be controlled by a card-actuated gate. Employee parking areas shall be monitored by CCTV. Emergency alert systems, such as blue phones, shall be provided at the discretion of the VA Police.

3.5.4 Existing Facility – Parking

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

3.6 SITE LIGHTING

3.6.1 General Requirements

Provide minimum maintained illumination levels for pedestrian pathways, bicycle and vehicle routes, parking structures, parking lots, wayfinding, signage, pedestrian entrances, and building services which will provide safety and security for personnel, buildings, and site. Refer to the Electrical Design Manual for illumination requirements.

Lighting shall provide for safety and security without compromising the quality of the site, the environment (including neighboring properties), or the architectural character of the buildings.

3.6.1.1 Aesthetic: The site lighting shall provide desired illumination and enhancement of trees, landscaping, and buildings without providing dark shadowy areas compromising safety and security.

3.6.1.2 CCTV: Site lighting shall provide CCTV and other surveillance support with illumination levels and color that assists in proper identification. Lighting shall be coordinated with CCTV cameras to enhance surveillance and prevent interference. Avoid “blinding” CCTV cameras in the placement and selection of fixtures and their “cutoff” angles.

3.6.1.3 Luminance levels: Illumination levels shall be in compliance with the Illumination Engineering Society of North America (IESNA), VA Electrical Design Guide, and local and state governing agencies.

3.6.1.4 Signage and wayfinding: Shall be enhanced by site lighting, including providing improved security by assisting pedestrians and vehicles to locate their destinations expeditiously. Refer to VA Signage Design Guide dated 2/2005.

3.6.1.5 Environmental: Minimize light pollution and spill into neighboring properties by selection of fixtures’ cutoff angles to minimize their nuisance visibility from adjacent areas on and off VA property.

3.6.2 Lighting Locations

Comply with all requirements for site lighting as may be set forth in VA publications. In addition, the following areas require additional attention in lighting design to support security and safety needs.

3.6.2.1 Site entrances: Lighting shall be provided at all site entrances at illumination levels that assist in after-dark performance of security duties:

- To assist guards with visual personal identification into vehicles to see the driver's compartment and view ID.
- To provide illumination of wayfinding and other signage.

3.6.2.2 Perimeter fence: Lighting sufficient to support perimeter CCTV surveillance shall be provided without objectionable spill onto neighboring properties or rights-of-way.

- Where a perimeter road has been provided for patrols or other functions, the lighting may be combined with roadway lighting.

3.6.2.3 Building entrances and exits: Lighting at building entrances shall support CCTV surveillance and ID functions while providing illumination of surfaces and features for safety.

3.6.2.4 Parking areas: All parking areas covered and open shall be lighted in support of CCTV and other surveillance without objectionable spill into adjacent areas on or off site.

3.6.2.5 Pathways: Pedestrian and bicycle pathways and walks, including bike racks, gates, and other features shall be illuminated in support of CCTV and other surveillance while providing for safety without objectionable spill onto adjacent areas on and off site.

3.6.2.6 Signage: All signage shall be adequately illuminated to provide safe wayfinding and identification. Wayfinding maps and texts shall be individually illuminated.

3.6.2.7 Enclosures: Liquid oxygen tanks and other enclosures shall be illuminated in support of CCTV and visual surveillance without spillage into other areas on or off site.

3.6.2.8 Trash: Collection areas shall be illuminated in service yards as a part of the yard illumination. Individual trash bins may not require illumination.

3.6.2.9 Loading docks and associated yards: Loading areas shall be fully illuminated for operations and in support of CCTV and other surveillance and Identification needs.

3.6.3 Existing Facility – Site Lighting

All sites with mission critical facilities shall have site lighting installed in accordance with section 3.6.

4

Building Entrances and Exits

4.0 SCOPE

This section provides requirements for public entrances, entrance lobbies, patient drop-offs, and staff entrances. Reduce the number of public entrances to the minimum number required. Entrance requirements for specific functional areas, such as emergency department, loading dock, and other service entrances for mission critical facilities, are covered in Chapter 5. Specific requirements for security devices and their locations can be found in Appendix A, Security Door Openings, and Appendix B, Security System Application Matrix.

4.1 PUBLIC ENTRANCES AND LOBBIES

Public access to the facility should be restricted to a single or limited number of entrances.

4.1.1 Entrances

4.1.1.1 Public entrances: All public entrances to the In-Patient, Out-Patient, and Long-Term Care Facility shall have a screening vestibule that may be used when VA requires individuals entering the building to pass through access control and screening prior to entering the building lobby.

4.1.1.2 Staff entrances Staff entrances shall be located independently of main entrance lobbies and be convenient to staff parking.

4.1.2 Screening Vestibules

The screening vestibule shall have sufficient space and be provided with power, telecommunications, and data connections for installation of access control and screening equipment that may be used should the need arise. Prevent access from

drop-off to lobby in a straight line of travel and provide sufficient size to accommodate several people with mobility aids.

4.1.3 Public Entrances

4.1.3.1 Location: Vehicles may not approach within 50 feet (15 meters) of the entrance.

4.1.3.2 Doors: Entrance doors to the lobby shall be visible to or monitored by the security personnel in the main lobby and the Security Control Center.

4.1.3.3 Access within the facility: Access from the lobby to elevators, stairways, and corridors shall be controlled through the use of electronic access control or mechanical locking devices, limiting access to specific floors and areas that house functions requiring restricted access.

- Install elevator call buttons requiring use of key cards or other electronic access control when they are located in restricted areas.

4.1.4 Access for Emergency Responders

The Fire Command Center (FCC) and secure house key box for emergency responders shall be located near an entrance door at a location approved by the Project Manager. The door associated with the FCC shall be controlled and monitored by CCTV.

4.1.5 Planning, Construction Details, and Materials

4.1.5.1 Structural: The entrance itself shall be constructed to fail in a way that subjects persons inside or nearby to as little hazard as possible. (See Chapter 6, Building Envelope and Chapter 7, Structural.)

- Protection of entrances and lobbies from vehicle ramming must be accomplished outside and in front of the entrance. (See Chapter 3, section 3.4 Vehicle Barriers.)
- If a covered drop-off area is provided, its supporting structure shall be independent of the main building and protected from intentional and unintentional damage by vehicles.
- Separate the public lobby from the adjacent hospital areas with partitions that extend to the underside of the floor above.

4.1.5.2 Façade: Glazing in the lobby area shall be laminated glass.

4.1.5.3 Doors and hardware: Exterior doors shall be in size, operation, and other characteristics in compliance with applicable regulatory requirements. If doors

are lockable, they shall comply with emergency egress requirements. Refer to Program Guide PG-18-14, *Room Finishes, Door and Hardware Schedule*, and Appendix A, Security Door Openings, for additional requirements.

- Glass for entrance doors shall be laminated.
- Entrance doors shall be capable of being remotely locked and unlocked from the reception desk in the main lobby.
- Public entrance doors may be manually or power operated and may be swinging doors, horizontal sliding doors (power operated only), or revolving doors.
- Staff entrance doors shall prevent unauthorized access.
- Long-Term Care Unit shall be provided with electronic or mechanical locks on exterior doors as well as visual monitoring and voice communication with connection to information desk or security office.
- Staff entrance door hardware shall include either mechanical or electronic locks.
- Means of egress doors that do not also function as entrances shall be provided with delayed action and alarmed emergency egress hardware.

4.1.5.4 Receptacles: Letter boxes and receptacles for trash and smoking paraphernalia shall not be located within 5 feet (1524 mm) of load-bearing elements. Those within 50 feet (15 m) of the building shall be designed to prevent depositing of explosive charges or to contain explosions with a charge weight (defined in the *Physical Security Design Standards Data Definitions*) as directed by the Project Manager and coordinated with the structural engineer.

4.1.6 Security Monitoring

All public entrances require security monitoring. At public entrances create a “hard line” in the screening vestibule between the entrance and the lobby by providing a guard station with capacity to screen patients, visitors, and packages when screening is required.

4.1.6.1 Security guard stations: Guard stations shall be located at building entrances available to the public. Guard stations shall be located where pedestrian traffic can be monitored and controlled by security personnel. If guard stations are located outside, they shall be protected from weather and capable of being secured when not in use.

- Guard stations that are incorporated into a Security Control Center shall be separated from public areas with UL Level 3 bullet resistant construction.

- Guard stations that are not incorporated into an SCC shall be provided with a desk and capacity to communicate directly with the SCC.
- An intercom shall be provided from the front door to the guard station reception desk and SCC.

4.1.6.2 Screening devices: At all public entrances, where it may be necessary to screen all people entering a building, provide a screening vestibule. Provide the required connections for temporary installation of metal detectors and package screening equipment and sufficient space for their installation.

- Locate screening equipment in a manner that will prevent passage into the building or facility without passing through the devices.
- When screening devices are not permanently installed, provide secure storage in close proximity to their installation location.
- Locate screening equipment so as not to restrict emergency egress.

4.1.6.3 Security devices: CCTV cameras shall be provided to monitor activities in the vestibules and lobbies of new and existing mission critical facilities and shall be located to provide views of approaching pedestrian and vehicular traffic, drop-off areas, building entrances, and departing pedestrian and vehicular traffic.

4.1.7 Existing Facility – Entrances and Lobbies

4.1.7.1 Covered drop-off: Protect columns with anti-ram barriers such as bollards and from explosive devices by installation of barriers that prevent detonation within 18 inches (457 mm).

4.1.7.2 Screening Vestibules: Where space permits, provide a screening vestibule with the required connections for temporary installation of metal detectors and package screening equipment and sufficient space for their installation and of sufficient size to accommodate several people with mobility aids. Where possible arrange screening vestibule to prevent access from drop-off to lobby in a straight line of travel.

4.1.7.3 Glazing: Glazing in the lobby area shall be laminated glass or fitted with anti-fragmentation film.

4.1.7.4 Access within the facility: Modify existing elevator call buttons to require electronic access control to register calls when elevators open directly into restricted areas.

4.2 PATIENT DROP-OFFS

Patient drop-offs shall be located at primary building entrances or other locations that will provide convenient access to services without hindering the flow of traffic. Patient drop-off areas shall not be located near staff-only entrances.

4.2.1 Vehicular Access

Drop-offs and staging areas for vehicles, including public transportation vehicles, shall be separated from the main building structure by at least 50 feet (15 meters).

4.2.2 Parking

Parking shall not be permitted in patient drop-off areas.

4.2.3 Existing Facility – Patient Drop-offs

Patient drop-offs for existing mission critical facilities shall meet the requirements of 4.2.1 and 4.2.2.

4.3 BUILDING EXITS AND LIFE SAFETY CONSIDERATIONS

Means of egress shall not be obstructed by installation of security devices such as guard stations, screening equipment, or other security devices.

Delayed egress and alarmed exits shall comply with applicable codes and regulations.

4.3.1 Site Requirements

Provide an unobstructed and adequately lighted path from each means of egress to a safe location outside the building.

- Where the means of egress is accessible to persons with disabilities, provide an accessible route to a safe location outside the building.
- Where means of egress lead to loading docks or other service areas, direct users away from hazardous and pathological waste storage, mailrooms, and other areas that may be the source of injury or contamination.
- Plan and locate egress paths so that they are not obstructed by with anti-ramming barriers or other similar devices.

4.3.2 Planning, Construction Details, and Materials

Construction of building exits shall be consistent with the requirements for adjacent building envelope elements.

- Where laminated glass is required in nearby window openings, glazing for exit doors shall also be laminated.
- Where adjacent portions of the building require blast resistant construction, construct the means of egress with a similar level of protection.
- Means of egress doors shall be of construction that makes unauthorized entry from the exterior difficult. Provide hardware that minimizes the opportunity for unauthorized entry by using components such as continuous hinges and astragals.

4.3.3 Security Monitoring

Where means of egress do not also function as access points for the building, provide card reader for authorized users and delayed action, alarmed egress hardware to indicate unauthorized use.

- Provide CCTV cameras at locations with alarmed exits, at loading docks, and other areas subject to pilferage.
- Install door status monitors at doors intended to be used only for emergency egress.

4.3.4 Existing Facility – Building Exits and Life Safety Considerations

Existing facilities shall meet the requirements of section 4.3.

Functional Areas

5.0 SCOPE

This section discusses the specific spatial functional areas, their relationships, and adjacencies based on physical security requirements. Major renovations of existing functional areas within existing facilities shall bring the functional area into compliance with the requirements of this section. Functional areas not undergoing major renovation shall be brought into compliance with the requirements of this section for existing facilities. Additional requirements are shown in Appendix A, Security Door Openings, and Appendix B, Security System Application Matrix.

5.1 AGENT CASHIER

In addition to the requirements of this section: Program Guide (PG-18-9) *Space Planning Criteria for VA Facilities*, #234 *Fiscal Service* shall remain in full force and effect; the requirements of VA Handbook 0730 *Security and Law Enforcement*, Appendix B, as they apply to fiscal services shall also apply; and VA Program Guide (PG-18-3) *Design and Construction Procedures* apply.

5.1.1 Adjacencies

The agent cashier shall be located with the transaction window facing a corridor accessible to public and employees, but not opening to a lobby. There shall be no openings to the exterior of the building.

5.1.2 Entrances

The agent cashier space shall be accessed by a door to a corridor which is accessible only to employees of the facility.

5.1.3 Construction

The agent cashier space shall be fully enclosed in 1-hour fire resistive construction extending from structural slab to structure above.

5.1.3.1 Partitions and openings: Partitions and teller windows facing the public corridor shall be UL Level 3 ballistic construction and 15-minute forced entry construction, including partitions, doors, glazed openings, teller windows, and transaction trays.

- All surrounding partitions and walls, floor, and ceiling shall be permanently constructed and attached to each other. To provide visual evidence of attempted entry, all construction, to include above the false ceiling and below a raised floor, shall be done in such a manner as to provide visual evidence of unauthorized penetration.
- Partitions and walls shall be reinforced, slab-to-slab, with 9-gauge expanded metal. The expanded metal shall be spot welded every 6 inches (150 mm) to vertical and horizontal metal supports of 16-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.

5.1.3.2 HVAC: All vents, ducts, and similar openings in excess of 96 square inches (620 cm²) that enter or pass through an agent cashier space shall be protected with either bars or grills. If one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm²), bars are not required; however, all ducts must be treated to provide sufficient sound attenuation. If bars are used, they must be 1/2 inch (12.7 mm) diameter steel welded vertically and horizontally six (6) inches (150 mm) on center; if grills are used, they must be of 9-gauge expanded steel.

- Openings in construction above ceilings or below raised access floors shall be protected as above.

5.1.4 Security

5.1.4.1 CCTV: The agent cashier space and the transaction window shall be monitored by CCTV.

5.1.4.2 Duress alarm: A duress alarm shall be provided in a location not visible to customers at the transaction window.

5.1.4.3 Door: Entrance door shall be controlled and monitored as SDO 209.

5.1.5 Existing Facility – Agent Cashier

Existing agent cashier areas shall provide the security requirements of section 5.1.4.

5.2 CACHE

In addition to the requirements of this section: Program Guide (PG-18-9) *Space Planning Criteria for VA Facilities*, #268 *Pharmacy Service* shall remain in full force and effect; the requirements of VA Handbook 0730 *Security and Law Enforcement*, Appendix B, as they apply to pharmacy drug storage shall also apply to caches; and VA Program Guide (PG-18-3) *Design and Construction Procedures* apply.

5.2.1 Adjacencies

Pharmacy caches located within the main facility shall be on a corridor leading to the loading dock, but no closer than 50 feet (15 m) to the loading dock or mailroom. Pharmacy caches may be located in a separate building from the main facility on the VA facility site, subject to these requirements.

5.2.2 Entrances

Doors and frames to caches shall be opaque hollow metal, and shall be controlled and monitored as follows.

- From exterior to cache with no door from cache to interior of main building – SDO 211.
- From an interior corridor to the cache – SDO 211.

5.2.3 Construction

Caches shall be enclosed in Class 1 fire rated construction with surrounding construction 15-minute forced-entry resistant. Exterior construction shall be reinforced masonry or equivalent.

5.2.3.1 Partitions and openings: Interior partitions shall comply with the following when separating a cache from other building spaces, including corridors.

- Walls, floor and ceiling shall be permanently constructed and attached to each other. All construction, to include above the false ceiling and below a raised floor, shall be done in such a manner as to provide visual evidence of unauthorized penetration.
- Walls shall be reinforced, slab-to-slab, with 9-gauge expanded metal. The expanded metal shall be spot welded every 6 inches (150 mm) to vertical and horizontal metal supports of 16-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.
- No windows or skylights shall be permitted in caches.

5.2.3.2 HVAC: All vents, ducts, and similar openings in excess of 96 square inches (620 cm²) that enter or pass through a perimeter partition of the cache shall be protected with either bars or grills. If one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm²), bars are not required; however, all ducts must be treated to provide sufficient sound attenuation. If bars are used, they must be 1/2 inch (12.7 mm) diameter steel welded vertically and horizontally six (6) inches (150 mm) on center; if grills are used, they must be of 9-gauge expanded steel.

- Openings in construction above ceilings or below raised access floors shall be protected as above.

5.2.3.3 Electrical: All lighting, security devices, and refrigerators within the cache shall be on emergency power.

5.2.4 Security

Entrance doors to the cache and vault doors, if any, within the cache shall be monitored by CCTV.

5.2.5 Existing Facility – Cache

Existing caches shall comply with the requirements of section 5.2.

5.3 CHILDCARE/DEVELOPMENT CENTER

This section supplements Program Guide (PG-18-9) *Space Planning Criteria for VA Facilities, #420 Childcare/Development Center* which shall remain in full force and effect. Childcare/development centers shall also meet the licensure requirements of the jurisdiction in which they are located.

5.3.1 Adjacencies

If located within a portion of a main VA facility, such as a hospital, childcare/development centers shall be located on the ground floor away from main building entrance with separate access area for drop-off and pick-up.

5.3.2 Entrances

Doors shall be provided with an intercom to the reception desk with remote access from the desk.

5.3.2.1 Public entrances: Doors to childcare/development centers, including the main entrance and secondary entrances, shall be controlled and monitored as SDO 112.

5.3.2.2 Emergency exits: Emergency egress doors from childcare/development centers shall be controlled and monitored as SDO 104.

5.3.3 Construction

No additional physical security requirements.

5.3.4 Security

All entrances, including drop-off and pick-up areas, playgrounds, and other outdoor areas where children may be while at the childcare/development center shall be monitored by CCTV.

5.3.5 Existing Facility – Childcare/Development Center

Entrances and security for existing childcare/ development centers shall comply with the requirements of sections 5.3.2 and 5.3.4.

5.4 COMPUTER ROOM

This section applies to the main computer room. In addition to the requirements of this section, NFPA 75: *Protection of Electronic Computer/Data Processing Equipment* shall apply.

5.4.1 Adjacencies

The main computer room shall be located not closer than 50 feet (15 m) in any direction to main entrance lobbies, loading docks, and mailrooms, and in no case directly above or below such spaces.

5.4.2 Entrances

Entrance doors to the main computer room and other computer rooms shall be controlled and monitored as SDO 216.

5.4.3 Construction

Surrounding walls and partitions shall be 1-hour fire resistive construction and extend from slab to slab.

5.4.3.1 HVAC: All vents, ducts, and similar openings in excess of 96 square inches (620 cm²) that enter or pass through the perimeter of a computer room must be protected with either bars or grills. If one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm²) bars are not required; however, all ducts must be treated to provide sufficient sound attenuation.

If bars are used, they must be 1/2 inch (12.7 mm) diameter steel welded vertically and horizontally six inches (150 mm) on center; if grills are used, they must be of 9-gauge expanded steel.

- Openings in construction above ceilings or below raised access floors shall be protected as above.

5.4.4 Security

All doors shall have motion-activated CCTV camera coverage on the egress side of the door.

5.4.5 Existing Facility – Computer Room

Existing main computer rooms shall comply with the requirements of section 5.4.

5.5 COOP SITE

The Continuity of Operations (COOP) program is set forth in Federal Preparedness Circular (FPC) 67 of April 30, 2001, and as amended. This section supplements VA Handbook 0320 *Comprehensive Emergency Management Program* which shall remain in full force and effect. This section sets forth the requirements for national COOP sites. This section does not cover requirements for facility emergency operations centers or emergency command centers.

5.5.1 Adjacencies

The COOP space shall be located on the ground floor of the VA facility remote from the main entrance, loading dock, and mailroom. The interior doors to the COOP shall open to corridors not used by the public, infrequently used by facility staff, and leading to a secondary building entrance.

5.5.1.1 Other functions: A COOP space may be used for other purposes when not in use as a COOP, provided it can be made ready for COOP occupancy within the time specified in FPC 67.

5.5.1.2 Location in building: The COOP shall be on an exterior wall or, if located entirely internally, have direct access to a dedicated exterior entrance.

5.5.1.3 Site considerations: COOPs shall be provided with doors for emergency egress and receipt of supplies that lead to an inconspicuous outdoor space adjacent to the building and remote from the main entrance and from the service yard.

- Visually screen the outdoor space for delivery of supplies by Government-controlled vehicles.

- The entrance to the COOP shall be convenient to the helicopter landing pad, if one is on site.
- The door to the COOP shall be protected from vehicle ramming with passive vehicle barriers preferably designed as part of the landscape.

5.5.2 Entrances

5.5.2.1 Exterior doors: The exterior entrance to the COOP shall be through an opaque pair of UL 3 ballistic/15-minute forced entry doors monitored on the outside of the doors by CCTV and shall be controlled and monitored as SDO 233.

- An intercom shall be provided at the exterior to communicate with a COOP security officer at a location to be determined by the Project Manager.
- The electric strike shall be able to be unlocked by the COOP security officer above.

5.5.2.2 Interior entry doors: The interior door(s) to the COOP shall be opaque single or double leaf 15-minute forced entry construction and shall be controlled and monitored as SDO 233.

- Interior entry into the COOP shall be monitored on the outside of the COOP by CCTV.
- An intercom shall be provided at the exterior to communicate with a COOP security officer at a location to be determined by the Project Manager.
- The electric strike shall be able to be unlocked by the COOP staff person above.

5.5.3 Construction

5.5.3.1 Exterior walls: Construction shall be reinforced masonry, or equivalent construction, and shall be windowless.

5.5.3.2 Interior construction: Interior partitions between the COOP and surrounding spaces shall be 15-minute forced entry construction and extend from slab to slab.

- Walls, floor, and ceiling shall be permanently constructed and attached to each other. All construction, to include above the false ceiling and below a raised floor, shall be done in such a manner as to provide visual evidence of unauthorized penetration.
- Walls shall be reinforced, slab-to-slab, with 9-gauge expanded metal. The expanded metal shall be spot welded every 6 inches (150 mm) to vertical

and horizontal metal supports of 16-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.

- Partitions surrounding the COOP and all doors in them shall have a Noise Isolation Class (NIC) of not less than 53.

5.5.3.3 HVAC: All vents, ducts, and similar openings in excess of 96 square inches (620 cm²) that enter or pass through the perimeter of a COOP must be protected with either bars or grills. If one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm²) bars are not required; however, all ducts must be treated to provide sufficient sound attenuation. If bars are used, they must be 1/2 inch (12.7 mm) diameter steel welded vertically and horizontally six inches (150 mm) on center; if grills are used, they must be of 9-gauge expanded steel.

- Openings in construction above ceilings or below raised access floors shall be protected as above.

5.5.4 Security

All COOP CCTV shall be monitored by the COOP security officer and the facility security personnel in the Security Control Center.

5.5.5 Additional Requirements

The Project Manager will provide specific functional program needs, including occupancy population.

5.5.5.1 Duration of operation: The COOP shall be capable of operating for not less than thirty days independent of the host facility. The following services shall be maintained.

- Heating and cooling
- Power and light
- Potable water
- Fire extinguishment
- Sewage disposal from toilets and food preparation
- Communications

5.5.5.2 Functional area: The following shall be included in the design.

- Toilets for both genders – fully accessible in accordance with ADA and UFAS.
- Shower and change room with locker/storage for personal items.

- Break room with food preparation area and storage space for tableware and flatware, utensils, and cooking needs shall be provided.
- Food supplies will be presumed to be purchased from local sources and brought to the COOP as needed. Short-term holding for refrigerated and other consumable supplies shall be provided.
- Emergency treatment space shall be provided, but treatment for all but the most minor medical needs shall be presumed to be available in the host facility.

5.5.6 Existing Facility – COOP Site

Existing COOP sites shall be upgraded to meet the requirements of section 5.5. A new COOP in an existing building shall comply with the requirements of section 5.5.

5.6 EMERGENCY DEPARTMENT

This section supplements Program Guide (PG-18-9) *Space Planning Criteria for VA Facilities, #262 Ambulatory Care (Hospital Based)*.

5.6.1 Adjacencies

5.6.1.1 Vehicular Access: Only ambulances and emergency vehicles shall be allowed within 50 feet (15 meters) of the emergency department entrance. No other vehicles or traffic shall be allowed within 50 feet of the emergency department entrance.

- Drop-offs and staging areas for vehicles, including public transportation vehicles, shall be separated from the main building structure by at least 50 feet (15 meters).

5.6.1.2 Functional adjacencies: Provide direct observation of the waiting room from the Police Operations Room and direct access through a door controlled and monitored as SDO 204.

- Locate adjacent Police and Security Service Operations Room or as close thereto as feasible.
- Locate at least 50 feet (15 m) from loading docks, mailrooms, and public lobbies.

5.6.2 Entrances

Provide separate entrances for ambulatory patients and patients arriving by ambulance.

Provide space for screening of pedestrians (see 5.6.4 Security).

- **Exterior doors:** Entrances from the exterior shall be controlled and monitored as SDO 105 and SDO 106.
- **Interior entry doors:** Entrances from the emergency (urgent care) area to the main building shall be solid core wood or hollow metal and controlled and monitored as SDO 201.

5.6.2.1 Existing Facility –Entrances: Replace existing glass with laminated glass or install anti-fragmentation film on existing glass near the emergency department entrance.

5.6.3 Construction

5.6.3.1 Anti-ram barriers: Install stationary (passive) anti-ram barriers to prevent damage by vehicles approaching the emergency department entrance.

5.6.3.2 Façade: Provide laminated glass in doors and windows within 50 feet (15 m) of the emergency department entrance.

5.6.3.3 Construction separation: Separate treatment area and nurses' station from waiting area and entrances with full height construction.

5.6.3.4 HVAC: Locate all outdoor air intakes at least 100 feet (31 m) from ambulance parking areas.

5.6.4 Security

Provide a guard station and secondary SCC or direct connection to the SCC, with capacity to screen patients, visitors, and packages at the ambulatory patient entrance.

5.6.4.1 Exterior: Provide CCTV cameras capable of monitoring activity at the ambulance entrance and ambulance parking area and that display in the primary and secondary SCC.

5.6.4.2 CCTV Provide CCTV monitoring of ER Reception/waiting room and entrance from the exterior.

5.6.4.3 Intrusion detection: Provide door and lock status sensors and motion detectors in public toilets.

5.6.4.4 Duress alarm: Provide duress alarm for receptionist.

5.6.5 Existing Facility – Emergency Department

Existing emergency (urgent care) areas in existing buildings shall meet the requirements of sections 5.6.2 and 5.6.4.

5.7 EMERGENCY AND/OR STAND-BY GENERATOR ROOM

This section supplements Program Guide (PG-18-9) *Space Planning Criteria for VA Facilities, #230 Engineering Service*.

5.7.1 Adjacencies

Emergency and/or stand-by generators and related switchgear may be located in a separate structure from the main building or within the main building.

5.7.1.1 Elevation: The generator room shall not be located at an elevation subject to flooding at any time. Refer to the FEMA flood map for information.

5.7.1.2 Location in building: If within a main building such as a medical center, the generator room shall not be located closer than 50 feet (15 m) of a loading dock/receiving area or mailroom, and shall not be located beneath such facilities.

5.7.1.3 HVAC: Areaways and louver openings serving the generator shall not open to the service yard for the loading dock.

5.7.2 Entrances

5.7.2.1 Exterior doors: Entrances from the exterior shall not open to the loading dock service yard. Doors shall be hollow metal and controlled and monitored as SDO 111.

5.7.2.1 Interior entry doors: Entrances from the interior of the building shall be 2-hour fire resistive construction and shall be controlled and monitored as SDO 228.

5.7.3 Construction

Emergency and/or stand-by generators and related switchgear shall be surrounded by 1-hour fire resistive construction.

5.7.4 Security

Generators shall be monitored in the SCC as well as at the engineering control center.

5.7.5 Existing Facility – Emergency and/or Stand-by Generator Room

Where generators are adjacent to loading docks, mailrooms, or other potentially hazardous locations or may be subject to damage due to structural collapse, a blast mitigation analysis shall be performed and mitigation measures of hardening or relocation shall be taken.

- Doors shall be controlled and generators shall be monitored as required by sections 5.7.2 and 5.7.4.

5.8 ENERGY CENTER/BOILER PLANT

In addition to the requirements of Program Guide (PG-18-9) *Space Planning Criteria for VA Facilities*, #230 Engineering Service, the following shall be required.

5.8.1 Adjacencies

The energy center/boiler plant may be located within a main building or in an independent building. If in an independent building, see Chapter 3 for site planning requirements.

5.8.1.1 Elevation: The energy center/boiler plant, including emergency and/or stand-by generators and switchgear, and engineering control center, and access to fuel tanks, shall not be located at an elevation subject to flooding at any time. Refer to the FEMA flood map for information.

5.8.1.2 Location in building: If within a main building such as a medical center, the energy center/boiler plant shall not be located closer than 50 feet (15 m) of a loading dock/receiving area or mailroom and shall not be located beneath such facilities.

5.8.1.3 HVAC: Areaways and louver openings serving the energy center/boiler plant shall not open to the service yard for the loading dock and mailroom.

5.8.2 Entrances

The energy center/boiler plant shall not be entered from the service yard for the loading dock and/or mailroom.

- Doors from the exterior to the energy center shall be controlled and monitored as SDO 111.
- Doors from the energy center to the interior of a main building shall be controlled and monitored as SDO 228.

5.8.3 Construction

No additional physical security requirements.

5.8.4 Security

CCTV shall be provided to monitor any entrance to the energy center/boiler plant from the exterior.

5.8.5 Existing Facility – Energy Center/Boiler Plant

Access to the energy center/Boiler Plant shall be controlled and monitored as required by sections 5.8.2 and 5.8.4.

5.9 LOADING DOCK AND SERVICE ENTRANCES

5.9.1 Adjacencies

Loading docks shall be adjacent to, but structurally separate from, any VA facility.

5.9.1.1 Acceptable adjacencies: Loading docks may be located immediately adjacent the following areas.

- Service yard
- Trash containers
- Freight elevators
- Non-critical bulk storage
- Mailroom
- Non-critical support areas such as laundries and maintenance spaces.

5.9.1.2 Prohibited adjacencies: Loading docks shall not be located adjacent to or within 50 feet (15 m) of the following.

- COOP
- Fire Control Centers
- Security Control Center and Police Command Center
- Emergency or stand-by generators
- UPS
- Water storage – domestic and fire
- Main electrical switchgear

- Main utility service entrances
- Emergency egress from main building
- Childcare/development centers
- Flammable liquids or gas storage
- Outdoor air intakes

5.9.1.3 Coordination with vivarium: Research animals and animal pathological waste shall have separate loading dock facilities, but may be served by the same service yard as the general loading dock.

5.9.2 Entrances

Pedestrian doors, stairs, and ramps associated with loading docks shall be restricted to authorized personnel and be separated from the loading platform by not less than 4 feet (1.2 m) to discourage by-passing the entry door controls through the loading platform and other doors.

Provide electronic locks and door status monitors on doors serving loading docks.

- **Exterior doors:** Exterior pedestrian entrance doors and frames shall be constructed of heavy duty hollow metal and shall be controlled and monitored as SDO 107 and SDO 108.
- **Interior entry doors:** Doors and frames from the mailroom to the interior of the building shall be 2-hour fire resistive construction and controlled and monitored as SDO 228.

5.9.3 Construction

5.9.3.1 Structural: Structure shall be designed to sustain an explosion from a charge weight (defined in the *Physical Security Design Standards Data Definitions*) within the loading dock and receiving area as directed by the Project Manager.

5.9.3.2 Interior partitions: The loading dock and receiving area shall be separated from the corridors and spaces adjoining with reinforced masonry walls and doors of hollow metal construction controlled and monitored as SDO 228.

5.9.3.3 Secured storage: Provide secure storage areas for delivered items awaiting uncrating and distribution within the facility and for hazardous and pathological waste.

5.9.3.4 HVAC: Locate all outdoor air intakes at least 100 feet (31 m) horizontally and 30 feet (9 meters) vertically from parking areas or on roof away from the roof line.

5.9.3.5 HVAC: Air serving the loading dock and receiving areas shall not circulate to other parts of the building.

5.9.4 Security

A minimum of 400 ft² (37 m²) shall be provided within the receiving area for inspection and imaging of goods received.

5.9.4.1 Guard post: When a second guard post is provided for a building, it shall be located where the loading dock and associated doors can be seen and door status and other access control devices monitored by the guard.

- The guard's office may be near the loading dock supervisor or manager.
- Doors to the guard booth shall be controlled and monitored as SDO 114.

5.9.4.2 Exterior: Install CCTV cameras to provide surveillance of all loading dock areas, including the gate, vehicle inspection areas, service yard and various containers, parked vehicles, loading and unloading activities, and building entrances at the loading dock

5.9.4.3 CCTV: The loading dock, including vehicles parked at the dock, shall be monitored by CCTV.

5.9.4.4 Access control: Dock lift controls shall be secured with a card reader device to prevent unauthorized use for entry.

5.9.5 Additional Requirements

Loading docks shall be served from service yards enclosed by a secure fence or wall and power-operated sliding gate, controlled by card access device and/or remote release and operation by a guard, the dock manager, or other authorized person with intercom and CCTV ID.

5.9.5.1 Vehicle access: Vehicle access to the loading dock shall be restricted.

- Approaches to loading docks shall be configured to minimize the possibility of high speed approach by any type of vehicle.
- Where the entrance gate to a service yard is directly from a public right-of-way, deployable vehicle barriers shall be provided on the inside of the gate, and shall be integrated with gate controls.

- Provide an area for the inspection of delivery vehicles that will not interfere with the flow of traffic on public rights of way, the site, or the loading area.

5.9.5.2 Service yards: The yard shall be segregated from other vehicle and pedestrian traffic areas by screen walls.

- Delivery vehicle maneuvering and parking shall be within an enclosed service yard accessed by delivery vehicle roadways leading directly from the site perimeter.
- Trash, medical/pathological waste, and other containers, compactors, and other similar equipment shall be located within the enclosed service yard and under CCTV surveillance.

5.9.6 Existing Facility – Loading Dock and Service Entrances

Loading docks in existing facilities may remain in their original locations. Enclosed service yards as described in section 5.9.5.2 shall be provided. Existing loading docks shall meet the requirements of section 5.9.3.2 and the following.

5.9.6.1 Inspection area: A minimum of 400 ft² (37 m²) shall be provided within the receiving area for inspection and imaging of goods received.

5.9.6.2 Structural hardening: When located within the main building, structural columns passing through the loading dock and receiving area and floor slabs above the loading dock and receiving area shall be structurally hardened to sustain an explosion within the loading dock or receiving area from a charge weight (defined in the *Physical Security Design Standards Data Definitions*) as directed by the Project Manager.

5.9.6.3 Adjacencies: Research laboratories and vivariums in existing buildings may be served by existing loading docks; however, loading of animals and removal of animal pathological waste shall be screened from public view and shall be within a controlled access yard or area.

5.10 MAILROOM

5.10.1 Adjacencies

Mailrooms may be located in the main building or in a separate structure on the site shared with loading dock, storage, and other non-critical functions. Mailrooms within the main building shall be located on an exterior wall.

5.10.1.1 Location: Mailrooms within the main building shall be located on an exterior wall and adjacent to the loading dock.

5.10.1.2 Acceptable adjacencies: Mailrooms may be located immediately adjacent the following areas:

- Service yard
- Trash containers
- Loading dock
- Freight elevators
- Non-critical bulk storage
- Non-critical support areas such as laundries and maintenance spaces

5.10.1.3 Prohibited adjacencies: Mailrooms shall not be located adjacent to or within 50 feet (15 m) of the following.

- COOP
- Fire Control Centers
- Security Control Center and Police Command Center
- Emergency or stand-by generators
- UPS
- Water storage – domestic and fire
- Main electrical switchgear
- Main utility service entrances
- Emergency egress from the main building
- Childcare/development centers
- Flammable liquids or gas storage
- Outdoor air intakes

5.10.2 Entrances

5.10.2.1 Exterior doors: Exterior entrance doors and frames shall be constructed of heavy duty hollow metal and shall be controlled and monitored as SDO 111.

5.10.2.2 Interior entry doors: Doors and frames from the mailroom to the interior of the building shall be 2-hour fire resistive construction and controlled and monitored as SDO 203.

5.10.3 Construction

When located within the main building, structural columns passing through the mailroom and inspection area and floor slabs above them shall be structurally hardened to sustain an explosion within the mailroom or inspection area from a charge weight (defined in the *Physical Security Design Standards Data Definitions*) as directed by the Project Manager.

5.10.3.1 Mailboxes: Mailboxes, when provided, shall be in a separate room from the mailroom and inspection area, and shall comply with the mounting heights and other regulations of the US Postal Service.

5.10.3.2 Interior partitions: The mailroom shall be separated from the mailbox room, corridors, and spaces adjoining with reinforced masonry walls and doors of hollow metal construction.

5.10.4 Security

A minimum of 400 ft² (37 m²) shall be provided within the receiving area for inspection and imaging of mail received. This may be space shared with the loading dock inspection area.

5.10.4.1 CCTV: The mailroom, including the inspection area, and the exterior loading area serving the mailroom shall be monitored by CCTV.

5.10.5 Additional Requirements

Air serving the mailroom shall not circulate to other parts of the building.

5.10.6 Existing Facility – Mailroom

Existing mailrooms shall comply with the requirements of section 5.10.

5.11 PHARMACY

In addition to the requirements of this section: Program Guide (PG-18-9) *Space Planning Criteria for VA Facilities*, #268 *Pharmacy Service* which shall remain in full force and effect; the requirements of VA Handbook 0730 *Security and Law Enforcement, Appendix B*, as they apply to pharmacy drug storage apply; and VA Program Guide (PG-18-3) *Design and Construction Procedures* apply.

5.11.1 Adjacencies

Deliveries to and shipments from pharmacies may be via the main loading dock and service yard. Pharmacies shall not be immediately adjacent the loading dock or mailroom.

5.11.2 Entrances

No additional physical security requirements.

5.11.3 Construction

No additional physical security requirements.

5.11.4 Security

Provide CCTV monitoring of pharmacy dispensing area, vault entrance, and controlled substance storage.

5.11.5 Existing Facility – Pharmacy

Existing pharmacies shall comply with the requirements of section 5.11.4.

5.12 POLICE OPERATIONS ROOM AND HOLDING ROOM

This section supplements the following documents which shall remain in full force and effect: Program Guide (PG-18-9) *Space Planning Criteria for VA Facilities*, #279 *Police and Security Service* and VA Handbook 0730 *Security and Law Enforcement*.

5.12.1 Adjacencies

5.12.1.1 Police operations room: Shall be located, in accordance with VA Handbook 0730, on the first floor of the main patient care building adjacent to the highest potential trouble area, such as admissions, emergency or urgent care room, or lobby and shall be located to allow appropriate response and deployment to respond to a security related event.

5.12.1.2 Holding room: Shall be located within or adjacent to the police operations room.

- An additional holding room may be located within or adjacent to a perimeter screening facility.

5.12.2 Entrances

5.12.2.1 Police operations room: Doors shall be from a corridor used only by staff and shall be controlled and operated as SDO 204.

5.12.2.2 Holding room: Doors and frames shall be heavy gauge hollow metal steel construction and door hardware shall be 15-minute forced entry rated controlled and monitored as SDO 205.

5.12.3 Construction

5.12.3.1 Police operations room: When the police operations room is adjacent to or opens onto areas occupied by unscreened public, such as lobbies, emergency rooms, and public corridors, construction, including partitions from slab to slab, doors, windows, and other openings separating the unit from such spaces, shall be 1-hour fire resistive, UL level 3 ballistic-resistant.

5.12.3.2 Holding room: Construction of the holding room shall be 15-minute forced entry resistant and as follows.

- Walls shall be constructed of reinforced masonry extended to the underside of the structure above; drywall and steel stud construction shall not be used.
- Door frames shall be grouted solid and anchored into the masonry walls.
- An observation window consisting of reflective glass protected by clear polycarbonate shall be provided.
- The interrogation table shall be firmly anchored to the floor and to one wall.
- Shackle hasps shall be anchored to wall construction and be capable of resisting pullout of not less than 250 pounds (114 kg).

5.12.4 Security

CCTV surveillance shall be provided of the entire room through an opening glazed with transparent polycarbonate in a steel frame firmly anchored to the wall. If requested by the Project Manager, the CCTV camera shall be covert and use lenses made for the purpose.

5.12.5 Existing Facility – Police Operations Room and Holding Room

Existing police operations rooms and holding rooms in existing facilities, when a police operations room opens directly to other parts of the building, including corridors and elevator lobbies, partitions and control doors shall be constructed to separate the lobby as required by section 5.12.2 and 5.12.3.

5.13 RECORDS STORAGE AND ARCHIVES

In addition to the requirements of this section, Department of Veterans Affairs publication, *Essential Records Vulnerability Assessment* (October 2003) shall apply.

5.13.1 Adjacencies

Records storage rooms shall be located not nearer than 50 feet (15 m) in any direction

from main entrance lobbies, loading docks, and mailrooms and in no case directly above or below such spaces.

5.13.2 Entrances

Entrances to archival storage spaces, including book stacks, computer main frames, and valuable or historical records and collections shall be controlled and monitored as SDO 213.

- Emergency egress doors from archival storage spaces shall be controlled and monitored as SDO 104 and shall have motion-activated CCTV camera coverage of the egress side of the door with all device monitors at a central location within the archival or library area.

5.13.3 Construction

Records storage rooms shall comply with National Archives and Records Administration (NARA) *Facility Standards for Records Storage Facilities – Part 1228, Subpart K*.

- Where electronic media or data storage facilities are essentially computer rooms, the area shall comply with the requirements of section 5.4.

5.13.4 Security

Archives for rare and valuable artifacts and documents shall be provided with motion detectors and CCTV.

5.13.5 Existing Facility – Records Storage and Archives

Existing records storage facilities shall comply with sections 5.13.2 and 5.13.4.

5.14 RESEARCH LABORATORY AND VIVARIUM

This section supplements Program Guide (PG-18-9) *Space Planning Criteria for VA Facilities, #278 Research and Development* which shall remain in full force and effect. The requirements of *Laboratory Security and Emergency Response Guidance for Laboratories Working with Select Agents* (CDC Biosafety in Microbiological and Biomedical Laboratories (BMBL) 4th Edition, Appendix F) shall apply to facilities storing and handling select agents. (Select agents shall be as defined in Title 42, CFR, Part 73, including pathogens and toxins regulated by both DHHS and USDA and non-overlap select agents of DHHS.) Veterinary Medical Unit vivarium spaces shall comply with AAALAC accreditation requirements.

5.14.1 Adjacencies

Laboratories and other spaces storing or using select agents may be in an independent building or within a building such as a medical center.

5.14.1.1 Shared occupancy: When located within a building with other occupancies, the laboratory shall be located on a corridor restricted to authorized employee use.

5.14.1.2 Select agents: Laboratories and other facilities using select agents shall be located no closer than 50 feet (15 m) from public lobbies, mailrooms, or loading docks.

5.14.2 Entrances

Research and vivarium entrances shall be located away from public areas.

5.14.2.1 Exterior doors: Entrances to the vivarium from the exterior of a building shall be controlled and monitored as SDO 102.

- Emergency egress doors from vivarium spaces shall be controlled and monitored as SDO 102. The door shall be covered by CCTV camera (recording only) from the vivarium side.

5.14.2.2 Interior entry and emergency egress doors: Entrances to the vivarium from non-vivarium uses of a building shall be controlled and monitored as SDO 222.

- Emergency egress doors from vivarium spaces shall be controlled and monitored as SDO 222. The door shall be covered by CCTV camera (recording only) from the vivarium side.
- Doors to rooms containing Select Agents shall be controlled and monitored as SDO 229.
- All laboratory and laboratory “neighborhood” doors from public corridors accessible to all building occupants (such as those used for emergency egress) shall be controlled and monitored as SDO 227.
- All doors from public corridors to shared support rooms such as cold rooms, dark rooms, instrument rooms, autoclave rooms, ice machines, and other equipment shall be controlled and monitored as SDO 227.
- Doors to any room used to store radioactive waste, ongoing experiments using radioactive materials, or similar use of radioactive materials shall be controlled and monitored as SDO 223.

- Doors to Irradiator facilities shall be controlled and monitored as SDO 223.
- Entries to the containment area for BSL-3 facilities shall be controlled and monitored as SDO 230.
- Doors from “dirty” corridors to “clean” corridors shall be provided with a sensor and alarm at a central point in the vivarium when such door is left open longer than 18 seconds.

5.14.2.3 Elevator entrances: Control of elevator access opening directly into the vivarium shall be by card reader device in the elevator cab, or, if the elevator is dedicated to vivarium use, at any landing from which the elevator can be called. The elevator entrance door at the vivarium shall be monitored by a CCTV camera in the space looking at the entrance.

5.14.3 Construction

5.14.3.1 Partitions: Storage rooms containing Category A select agents and irradiator rooms shall be enclosed by 15-minute forced entry-resistant construction as follows.

- Walls, floor, and ceiling shall be permanently constructed and attached to each other.
- All construction, to include above the false ceiling and below a raised floor, shall be done in such a manner as to provide visual evidence of unauthorized penetration.
- Walls shall be reinforced, slab-to-slab, with 9-gauge expanded metal. The expanded metal shall be spot welded every 6 inches (150 mm) to vertical and horizontal metal supports of 16-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.

5.14.3.2 HVAC: All vents, ducts, and similar openings in excess of 96 square inches (620 cm²) that enter or pass through a perimeter partition must be protected with either bars or grills. If one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm²) bars are not required. If bars are used, they must be 1/2 inch (12.7 mm) diameter steel welded vertically and horizontally six inches (150 mm) on center; if grills are used, they must be of 9-gauge expanded steel.

- Openings in construction above ceilings or below raised access floors shall be protected as above.

5.14.4 Security

5.14.4.1 CCTV: BSL-3 Laboratories and vivariums shall have CCTV coverage of internal laboratory spaces which shall be monitored by personnel within the containment area

- CCTV cameras shall be placed to monitor any loading dock or other animal receiving area if not already monitored as a part of a general loading/receiving area as provided in this chapter.
- All CCTV coverage of access to areas surrounding the containment area shall be monitored in the SCC.

5.14.4.2 Intercom: An intercom shall be provided at each entrance door to a designated office or work station in BSL-3 laboratories or vivariums.

5.14.4.3 Biometric: Biometric identification devices shall generally be located at the entrance to the ante room, but if the device is placed at the door from the ante room to the laboratory, it must be functional for personnel in biosafety garments.

5.14.4.4 Access control: Use of other access control systems within the vivarium, including those used for automated watering and/or environmental control and monitoring (such as Edstrom “Watchdog”), shall only be permitted by written authorization of the Project Manager.

5.14.5 Additional Requirements for Select Agent Storage

Facilities handling select agents shall be designed to afford maximum visibility of all areas for observation of use and handling of the select agents.

5.14.5.1 Storage: Storage of select agents (typically in refrigerators and/or freezers) shall be in a separate room.

5.14.5.2 Equipment: Refrigerators and freezers for storage of select agents shall be lockable and covered by CCTV (digitally recorded and monitored) placed to allow view of any person accessing the refrigerator or freezer.

5.14.6 Existing Facility – Research Laboratory and Vivarium

Existing laboratories and vivariums in existing facilities shall comply with the requirements of sections 5.14.2 and 5.14.4.

5.15 SECURITY CONTROL CENTER (SCC)

This section supplements the Program Guide (PG-18-9) *Space Planning Criteria for VA Facilities*, #279 *Police and Security Service* and VA Handbook 0730 *Security and Law Enforcement* which shall remain in full force and effect.

5.15.1 Adjacencies

The SCC shall be readily accessible to authorized personnel, but shall be inconspicuous and located in areas not frequented by the general public, and shall contain office space, support space, and monitoring equipment that is not visible to unauthorized personnel.

5.15.1.1 Main lobby: The SCC containing monitoring devices and security personnel shall not be adjacent to the main public lobby.

5.15.1.2 Fire command center: The SCC shall be adjacent the building fire command center (FCC) but shall not be accessible to persons using the FCC.

5.15.1.3 Police operations unit: The SCC may be connected to the police operations unit but the two areas shall be served by separate entrances and each area shall be fully functional without requiring access to the other.

5.15.1.4 Holding room: The SCC shall not include a holding room.

5.15.1.5 Back-up SCC: Where provided shall be at a remote location from the primary SCC and meet the requirements of section 5.15.

5.15.2 Entrances

The SCC shall be entered from a corridor beyond the control doors leading out of the lobby to the building interior. Doors to the SCC shall be controlled and monitored as SDO 204.

5.15.3 Construction

5.15.3.1 Partitions: The SCC shall be fully enclosed with UL Level 3 ballistic construction and 2-hour fire resistive construction, including partitions, doors, glazed openings, teller windows and transaction trays.

- Walls, floor, and ceiling shall be permanently constructed and attached to each other.
- All construction, to include above the false ceiling and below a raised floor, shall be done in such a manner as to provide visual evidence of unauthorized penetration.

- Walls shall be reinforced, slab-to-slab, with 9-gauge expanded metal. The expanded metal shall be spot welded every 6 inches (150 mm) to vertical and horizontal metal supports of 16-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.
- Where raised access flooring is used for cable management in the SCC, all surrounding partitions shall be built from floor slab to ceiling slab or construction and sealed to an air tight condition.

5.15.3.2 HVAC: All vents, ducts, and similar openings in excess of 96 square inches (620 cm²) that enter or pass through a perimeter partition must be protected with either bars or grills. If one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm²) bars are not required. If bars are used, they must be 1/2 inch (12.7 mm) diameter steel welded vertically and horizontally six inches (150 mm) on center; if grills are used, they must be of 9-gauge expanded steel.

- Openings in construction above ceilings or below raised access floors shall be protected as above.
- HVAC serving the SCC shall be independent of the system(s) serving the main lobby.

5.15.4 Additional Requirements

The entire SCC shall be on generator-backed power for 100% of its operating needs.

5.15.5 Existing Facility – Security Control Center (SCC)

Where the existing SCC does not meet the requirements of section 5.15, a secondary SCC that complies with the requirements of section 10.5.2.1 shall be provided.

Building Envelope

6.0 SCOPE

This section provides requirements for exterior walls other than load bearing walls; glazed façade fenestration and glazed atria; for roof structures, including skylights; and air intakes and exhausts servicing mission critical equipment but does not pertain to stacks and wall openings for non-critical equipment. These requirements are in addition to the requirements for conventional façade 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.

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.

6.1 WALLS

6.1.1 Non-load Bearing Walls

Walls shall be designed to suffer damage but sustain a deformation no greater than $L/30$ in response to the calculated peak pressures and impulses resulting from the design level vehicle threat (W2) located at the stand-off distance, but no greater than GP2.

6.1.1.2 Supporting structure: Walls shall span from slab to slab and shall not be attached directly to gravity load bearing elements (such as columns and shear walls) unless an advanced analysis of the load bearing element demonstrates it can accept the maximum forces of the members framing into it without compromising its capacity.

6.1.1.3 Loads: Walls shall be able to accept the tributary loads transferred from glazed fenestration in addition to the design level pressures applied directly to their surface.

6.1.2 Existing Facility – Walls

No additional physical security requirements.

6.2 FENESTRATION

6.2.1 Façade Fenestration

All façade fenestration shall be designed to crack but fragments shall enter the occupied space and land on the floor no further than 10 feet (3 m) from the façade in response to the calculated peak pressures and impulses resulting from the design level vehicle threat (W2) located at the stand-off distance, but no greater than GP2.

6.2.1.1 Glass: Fenestration shall be constructed using debris mitigating materials such as laminated glass.

6.2.1.2 Glazing: The glass shall be restrained within the mullions with a sufficient bite or structural silicone adhesive to allow it to develop its post-damage capacity.

6.2.1.3 Mullions: The mullions shall be designed to accept the design level pressures while sustaining deformations no greater than $L/30$.

6.2.1.4 Curtainwall: Curtainwall framing members shall span from slab to slab and shall not be attached directly to gravity load bearing elements (such as columns and shear walls) unless an advanced analysis of the load bearing element demonstrates it can accept the maximum forces of the members framing into it without compromising its load bearing capacity.

6.2.2 Existing Facility – Fenestration

Façade fenestration shall be upgraded to meet the requirements of section 6.2.1. A mechanically anchored or wet glazed anti-shatter film may be used to satisfy the requirements of this section. The choice of film and the performance of the upgraded system shall be demonstrated using U.S. Government developed glass fragment hazard software. The means of attachment shall be based on the site specific features of the glass façade.

6.3 ATRIA

6.3.1 Atria

All vertical glass surfaces shall be designed to crack but fragments shall enter the occupied space and land on the floor no further than 10 feet (3 m) from the façade in response to the calculated peak pressures and impulses resulting from the design level vehicle threat (W2) located at the stand-off distance, but no greater than GP2.

6.3.1.1 Skylights: Skylights shall be designed to crack but remain in its frame in response to the calculated peak pressures and impulses resulting from the design level vehicle threat (W2) located at the stand-off distance, but no greater than GP2.

6.3.1.2 Glass: Atria shall be constructed using debris mitigating materials such as laminated glass.

6.3.1.3 Glazing: The glass shall be restrained within the mullions with a sufficient bite or structural silicone adhesive to allow it to develop its post-damage capacity.

6.3.1.4 Mullions: The mullions shall be designed to accept the design level pressures while sustaining deformations no greater than $L/30$.

6.3.1.5 Framing: Atria framing members shall be designed to continue carrying gravity loads while sustaining maximum allowable deformations.

6.3.2 Existing Facility – Atria

Atria shall be upgraded to meet the requirements of section 6.3.1. A mechanically anchored or wet glazed anti-shatter film may be used to satisfy the requirements of this section. The choice of film and the performance of the upgraded system shall be demonstrated using U.S. Government developed glass fragment hazard software. The means of attachment shall be based on the site specific features of the atria.

6.4 ROOFS

6.4.1 Roof Structure

Roof structure shall be designed to withstand the design level vehicle threat (W2) located at the stand-off distance, but no greater than GP2, while sustaining a deformation no greater than $L/30$. The blast loading shall take into account the presence of parapets, the diffusion of blast waves, and the spatial extent of the roof surface.

6.4.2 Skylights

Skylights shall be designed to crack but remain in its frame in response to the calculated peak pressures and impulses resulting from the design level vehicle threat (W2) located at the stand-off distance, but no greater than GP2.

6.4.2.1 Glazing: Skylight glass shall be restrained within the mullions with a sufficient bite or structural silicone adhesive to allow it to develop its post-damage capacity.

6.4.2.2 Mullions: The mullions shall be designed to accept the design level pressures while sustaining deformations no greater than $L/30$.

6.4.3 Penthouses Enclosing Mission Critical Equipment

Penthouse façade shall be designed to withstand the effects of hurricane wind loads and debris impact. Penthouse enclosures shall also be designed to resist the design level vehicle threat (W2) located at the stand-off distance to be consistent with the hardened intakes and exhausts, as described in section 6.5.1.

6.4.4 Existing Facility – Roofs

Skylights shall be upgraded to meet the requirements of section 6.4.

6.5 AIR INTAKES AND EXHAUSTS SERVICING MISSION CRITICAL EQUIPMENT

6.5.1 Intakes and Exhausts

Air intakes and exhausts shall be designed to minimize the blast over pressure admitted into critical spaces to the design level vehicle threat (W2) located at the stand-off distance by means of hardened plenums and structured baffles. The design shall deny a direct line of sight from the design level vehicle threat (W2) located at the stand-off distance to the critical infrastructure within.

6.5.1.1 Entrances and lobbies: Maintain positive pressure in lobbies and entrance 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.

6.5.1.1 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.

6.5.2 Existing Facility – Air Intakes and Exhausts Servicing Mission Critical Equipment

Air intakes and exhausts shall be upgraded to minimize the extent of debris that may enter critical spaces in response to the design level vehicle threat (W2) located at the stand-off distance. Hardened plenums and structured baffles shall be installed when a major interior renovation is performed.

6.6 CALCULATION METHODS

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

6.6.1 Design and Detailing

The performance of façade in response to blast loading is highly dynamic and often inelastic. Design and detailing of protected façade 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 U.S. Government (USG), may be used to supplement the analytical methods where a direct analytical representation is not feasible.

6.6.2 Blast Loads

Blast loads shall typically be developed using the semi-empirical relations of TM5-855 (CONWEP).

6.6.3 Dynamic Response

Dynamic structural response analyses shall be performed using either empirical data developed by an approved U.S. Government 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.

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.

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.shtml>.

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.

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 vice 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 in² (240 cm²) 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.



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 331 and 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&oid=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 Manufacturers 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



Security Door Openings (SDO)

- MATRIX
- TYPES
- SCHEDULE

The Security Door Openings (SDO) Matrix provides a summary of the primary components and functional requirements for the various opening types found in VA facilities. The Matrix is organized by facility type and entry type and is used in conjunction with the Security Door Opening Schedule and the Security Door Types. The Security Door Opening Schedule identifies specific hardware devices and operational requirements for each opening type. The Security Door Types describes the doors and the placement of hardware devices that may be installed on or near the door to make the secured opening function properly.

BUILDING EXTERIOR

Facility Type	Entry Type	SDO	Locations and Descriptions	Facility Classification	Access Control					Monitoring		Other
					Card Reader	Fail Safe	Fail Secure	Other	ANSI/BHMA* or other function	Door Contact	Other	
Hospital ACC Outpatient Clinic NHCU	Public Entrance	101.A 101.B 101.C 101.D	Exterior to Building Main Entrance Lobby with emergency egress Single, opaque, or framed glass Single, laminated glass (frameless) Pair, opaque, or framed glass Pair, laminated glass (frameless)	MC New	yes	X			Magnetic lock or electric strike	yes		Intercom for NHCU
				MC Existing	yes	X			Magnetic lock or electric strike	yes		
VBA Where VA is the only tenant	Public Entrance	101.A 101.B 101.C 101.D	Exterior to Building Main Entrance Lobby with emergency egress Single, opaque, or framed glass Single, laminated glass (frameless) Pair, opaque, or framed glass Pair, laminated glass (frameless)	MC New	yes	X			Magnetic lock or electric strike	yes		
				MC Existing	yes	X			Magnetic lock or electric strike	yes		
Research Facilities and Vivariums	Public Entrance	102.A 102.C	Exterior to Building Main Entrance Lobby with emergency egress Single, opaque, or framed glass Pair, opaque, or framed glass	MC New	yes	X			Magnetic lock or electric strike	yes		Alarmed exit; intercom
				MC Existing	yes	X			Magnetic lock or electric strike	yes		Alarmed exit; intercom
Hospital ACC Outpatient Clinic NHCU	Staff Entrance	103.A 103.B 103.C	Exterior to Secondary Building Entrance with emergency egress Single, opaque, or framed glass Single, laminated glass (frameless) Pair, opaque, or framed glass	MC New	yes	X			Mag. lock, elec. strike, or F04 entry	yes		Alarmed exit
				MC Existing	yes	X			Mag. lock, elec. strike, or F04 entry	yes		Alarmed exit
VBA Where VA is the only tenant	Staff Entrance	103.A 103.B 103.C 103.D	Exterior to Secondary Building Entrance with emergency egress Single, opaque, or framed glass Single, laminated glass (frameless) Pair, opaque, or framed glass Pair, laminated glass (frameless)	MC New	yes	X			Mag. lock, elec. strike, or F04 entry	yes		Alarmed exit
				MC Existing	yes	X			Mag. lock, elec. strike, or F04 entry	yes		Alarmed exit
Research Facilities and Vivariums	Staff Entrance	102.A 102.C	Exterior to Secondary Building Entrance with emergency egress Single, opaque, or framed glass Pair, opaque, or framed glass	MC New	yes	X			Magnetic lock or electric strike	yes		Alarmed exit
				MC Existing	yes	X			Magnetic lock or electric strike	yes		Alarmed exit
Hospital ACC Outpatient Clinic NHCU VBA	Egress	104.A 104.C	Exterior emergency egress only– no access from exterior Single, opaque, or framed glass Pair, opaque, or framed glass	MC New	no				Exit 01	yes		Alarmed exit
				MC Existing	no				Exit 01	yes		Alarmed exit
Hospital	Emergency Department	105.C	Exterior from Ambulance Dock to ED - stretchers and gurneys Pair framed glass	MC New	yes				Power operated sliding or swinging	no		Operable manually during power outage
				MC Existing	no				Power operated sliding or swinging	no		
Hospital	Emergency Department	106.A 106.C	Exterior from Ambulance Dock to ED - pedestrian Single opaque or framed glass Pair opaque or framed glass	MC New	yes				F12 Exit Lock	no		Intercom to guard station
				MC Existing	no				F12 Exit Lock	no		

* References for ANSI/BHMA Designations: “F-__”– ANSI/BHMA A156.13; “Exit __”– ANSI/BHMA A156.3

BUILDING EXTERIOR (continued)

Facility Type	Entry Type	SDO	Locations and Descriptions	Facility Classification	Access Control					Monitoring		Other
					Card Reader	Fail Safe	Fail Secure	Other	ANSI/BHMA* or other function	Door Contact	Other	
Hospital ACC Outpatient Clinic NHCU VBA	Loading Dock	107.A 107.C	Exterior from Loading Dock area to Building Interior - pedestrian only Single opaque or framed glass Pair opaque or framed glass	MC New	yes	X			Electric Strike	yes	Hold open alarm	
				MC Existing	no				F07 Storeroom	yes		
Hospital ACC Outpatient Clinic NHCU VBA	Loading Dock	108.0	Exterior from Loading Dock area to Building Interior - equipment and material deliveries Overhead coiling steel	MC New	yes					yes		
				MC Existing	yes					yes		
Hospital ACC Outpatient Clinic NHCU	Storage	109.A 109.C	Exterior to Storage only with no entrance to building Single opaque Pair opaque	MC New	no				F07 Storeroom or card reader	yes		
				MC Existing	no				F07 Storeroom or card reader	yes		
Hospital ACC Outpatient Clinic NHCU VBA	Emergency Access	110.A	Exterior to Building or Fire Control Center Single opaque or framed glass	MC New	no			Secure Key Storage	F07 Storeroom	no		
				MC Existing	no			Secure Key Storage	F07 Storeroom	no		
Hospital ACC Outpatient Clinic NHCU VBA	Tunnel	111.A	Exterior to Utility Tunnel Single opaque	MC New	no				F07 Storeroom	yes	IDS with alarm	
				MC Existing	no				F07 Storeroom	yes	IDS with alarm	
Child Care/ Development Center	Child Care	112.A 112.B 112.C 112.D	Exterior to Main Entrance and exit Single, opaque, or framed glass Single, laminated glass (frameless) Pair, opaque, or framed glass Pair, laminated glass (frameless)	MC New	yes	X			Magnetic lock or electric strike	yes		
				MC Existing	no				Push-button combination lock	yes		
Hospital ACC Outpatient Clinic NHCU VBA Research and Vivarium	Utility Connections	111.A 111.C	Exterior to Commercial Power Connections Single, opaque Pair, opaque	MC New	no				F07 Storeroom	yes	IDS with alarm	
				MC Existing	no				F07 Storeroom	yes	IDS with alarm	
Hospital ACC Outpatient Clinic NHCU VBA Research and Vivarium	Utility Connections	111.A 111.C	Exterior to Telecommunications and Data Connections Single, opaque Pair, opaque	MC New	no				F07 Storeroom	yes	IDS with alarm	
				MC Existing	no				F07 Storeroom	yes	IDS with alarm	

* References for ANSI/BHMA Designations: “F-__”– ANSI/BHMA A156.13; “Exit __”– ANSI/BHMA A156.3

BUILDING EXTERIOR (continued)

Facility Type	Entry Type	SDO	Locations and Descriptions	Facility Classification	Access Control					Monitoring		Other
					Card Reader	Fail Safe	Fail Secure	Other	ANSI/BHMA* or other function	Door Contact	Other	
Hospital ACC Outpatient Clinic NHCU VBA Research and Vivarium	Utility Connections	113.A 113.C	Exterior to Bulk Medical Gas Storage Single, opaque Pair, opaque	MC New	no				F07 Storeroom	no		
				MC Existing	no				F07 Storeroom	no		
Hospital ACC Outpatient Clinic NHCU VBA Research and Vivarium	Site Perimeter Guard House	114.A	Exterior to Guard House Single, opaque, or framed glass	MC New	no				F07 Storeroom	no		FEBR (30 min./Level III)
				MC Existing	no				F07 Storeroom	no		FEBR (30 min./Level III)

BUILDING INTERIOR

Facility Type	Entry Type	SDO	Locations and Descriptions	Facility Classification	Access Control					Monitoring		Other
					Card Reader	Fail Safe	Fail Secure	Other	ANSI/BHMA* or other function	Door Contact	Other	
Hospital ACC Outpatient Clinic NHCU	General	201.A	Public Lobby to Building Interior Single, opaque, or framed glass	MC New	no				F04 Entry	no		
		201.B	Single, tempered glass (frameless)	MC Existing	no				F04 Entry	no		
		201.C	Pair, opaque, or framed glass									
		201.D	Pair, tempered glass (frameless)									
VBA Where VA is the only tenant	General	201.A	Public Lobby to Building Interior Single, opaque, or framed glass	MC New	no				F04 Entry	no		
		201.B	Single, tempered glass (frameless)	MC Existing	no				F04 Entry	no		
		201.C	Pair, opaque, or framed glass									
		201.D	Pair, tempered glass (frameless)									
Research Facilities and Vivariums	General	202.A	Public Lobby to Building Interior Single, opaque, or framed glass	MC New	yes	X			Magnetic lock or electric strike	yes		
		202.C	Pair, opaque, or framed glass	MC Existing	yes	X			Magnetic lock or electric strike, or push-but. combination.	yes		

* References for ANSI/BHMA Designations: “F-__”– ANSI/BHMA A156.13; “Exit __”– ANSI/BHMA A156.3

BUILDING INTERIOR (continued)

Facility Type	Entry Type	SDO	Locations and Descriptions	Facility Classification	Access Control					Monitoring		Other
					Card Reader	Fail Safe	Fail Secure	Other	ANSI/BHMA* or other function	Door Contact	Other	
Hospital ACC Outpatient Clinic NHCU VBA	Mail Room	203.A 203.C	Corridor to Mail Room Single, opaque, or framed glass Pair, opaque, or framed glass	MC New	yes		X		F07 Storeroom and electric strike	yes		
				MC Existing	no				Push-button combination lock	no		
Hospital ACC Outpatient Clinic NHCU VBA	Security Control Center	204.A	Corridor to SCC Single, opaque, or framed one-way glass	MC New	yes		X		F07 Storeroom and electric strike	yes		FEBR (30 min./Level III)
				MC Existing	no				Push-button combination lock	no		FEBR (30 min./Level III)
Hospital ACC Outpatient Clinic	Police Operations Unit	205.A	Holding Area Single, opaque, or framed one-way glass	MC New	yes		X		F07 Storeroom and electric strike	yes		
				MC Existing	yes		X		F07 Storeroom and electric strike	yes		
Hospital ACC Outpatient Clinic NHCU VBA	Guard Station	206.A	Corridor to Security Guard Station Single, opaque, or framed glass	MC New	yes				F07 Storeroom and electric strike	yes		
				MC Existing	no				Push-button combination lock	no		
Hospital NHCU	Canteen Retail Store	207.A	Corridor to Canteen Retail Store Single, opaque, or framed glass	MC New	no				F07 Storeroom	yes	IDS with alarm	
		207.B 207.C 207.D	Single, tempered glass (frameless) Pair, opaque, or framed glass Pair, tempered glass (frameless)	MC Existing	no				F07 Storeroom	yes	IDS with alarm	
Hospital NHCU	Canteen Storage	208.A	Canteen Storage Room Single, opaque	MC New	no				F07 Storeroom	yes	IDS with alarm	
		208.C	Pair, opaque	MC Existing	no				F07 Storeroom	yes	IDS with alarm	

* References for ANSI/BHMA Designations: “F-__”– ANSI/BHMA A156.13; “Exit __”– ANSI/BHMA A156.3

BUILDING INTERIOR (continued)

Facility Type	Entry Type	SDO	Locations and Descriptions	Facility Classification	Access Control					Monitoring		Other
					Card Reader	Fail Safe	Fail Secure	Other	ANSI/BHMA* or other function	Door Contact	Other	
Hospital	Agent Cashier	209.A	Corridor to Agent Cashier Single, opaque, or framed glass	MC New	yes	X			F07 Storeroom and electric strike	yes	IDS with alarm	
				MC Existing	yes	X			F07 Storeroom and electric strike	yes	IDS with alarm	
Hospital	Credit Union	209.A	Public Areas to Credit Union Single, opaque, or framed glass	MC New	yes	X			F07 Storeroom and electric strike	yes	IDS with alarm	
				MC Existing	yes	X			F07 Storeroom and electric strike	yes	IDS with alarm	
Hospital ACC Outpatient Clinic NHCU	Pharmacy Cache	210.A	Corridor to Pharmacy Cache Single, opaque, or framed one-way glass	MC New	yes	X		PIN or Biometrics	F07 Storeroom and electric strike	yes	IDS with alarm	30 minute forced entry
		210.C	Pair, opaque, or framed one-way glass	MC Existing	yes	X		PIN or Biometrics	F07 Storeroom and electric strike	yes	IDS with alarm	30 minute forced entry
Hospital ACC Outpatient Clinic	Pharmacy Dispensing	211.A	Corridor to Pharmacy Dispensing Area Single, opaque, or framed one-way glass	MC New	yes	X			F07 Storeroom and electric strike	yes	IDS with alarm	
				MC Existing	yes	X			F07 Storeroom and electric strike	yes	IDS with alarm	
Hospital ACC Outpatient Clinic	Pharmacy Manuf'g	211.A	Corridor to Pharmacy Manufacturing Area Single, opaque, or framed one-way glass	MC New	yes	X		PIN or Biometrics	F07 Storeroom and electric strike	yes	IDS with alarm	30 minute forced entry
				MC Existing	yes	X		PIN or Biometrics	F07 Storeroom and electric strike	yes	IDS with alarm	30 minute forced entry
Hospital ACC Outpatient Clinic	Narcotics Vault	212.A	Pharmacy Cache to Narcotics Vault Single, opaque, or wire mesh	MC New	yes	X		PIN or Biometrics	F07 Storeroom and electric strike	yes	Hold-open alarm	
				MC Existing	yes	X		PIN or Biometrics	F07 Storeroom and electric strike	yes	Hold-open alarm	
Hospital ACC Outpatient Clinic NHCU VBA	Veterans' Records	213.A	Corridor to Veterans' Records Single, opaque, or framed glass	MC New	yes	X			F07 Storeroom and electric strike	yes	IDS with alarm	15 minute forced entry
		213.C	Pair, opaque, or framed glass	MC Existing	no				Push-button combination lock	yes	IDS with alarm	15 minute forced entry
Hospital ACC Outpatient Clinic NHCU	Medical Supplies	214.A	Corridor to Medical Supply Storage Single, opaque	MC New	no				Push-button combination lock	no		
		214.C	Pair, opaque	MC Existing	no				Push-button combination lock	no		

* References for ANSI/BHMA Designations: “F-__”– ANSI/BHMA A156.13; “Exit __”– ANSI/BHMA A156.3

BUILDING INTERIOR (continued)

Facility Type	Entry Type	SDO	Locations and Descriptions	Facility Classification	Access Control					Monitoring		Other
					Card Reader	Fail Safe	Fail Secure	Other	ANSI/BHMA* or other function	Door Contact	Other	
Hospital ACC Outpatient Clinic NHCU	Linen Storage and Distrib.	215.A	Corridor to Central Linen Storage and Distribution Single, opaque Pair, opaque	MC New	no				Push-button combination lock	yes	IDS with alarm	
		215.C		MC Existing	no				Push-button combination lock	yes	IDS with alarm	
Hospital ACC Outpatient Clinic NHCU VBA Research Facilities	Information Resource Mgmt.	216.A	Corridor to Information Resource Management (IRM) Single, opaque or framed glass Pair, opaque or framed glass	MC New	yes	X		PIN or Biometrics	F07 Storeroom and electric strike	yes	IDS with alarm	
		216.C		MC Existing	yes	X		PIN or Biometrics	F07 Storeroom and electric strike	yes	IDS with alarm	
Hospital ACC Outpatient Clinic NHCU VBA Research Facilities	Communica-tions	217.A	Corridor to Telephone Equipment Room Single, opaque or framed glass Pair, opaque or framed glass	MC New	yes	X		PIN or Biometrics	F07 Storeroom and electric strike	yes	IDS with alarm	
		217.C		MC Existing	yes	X		PIN or Biometrics	F07 Storeroom and electric strike	yes	IDS with alarm	
Hospital ACC Outpatient Clinic NHCU VBA Research Facilities	Telephone and Data Closets	218.A	Corridor to Telephone and Data Closets Single, opaque Pair, opaque	MC New	no				F07 Storeroom	no		
		218.C		MC Existing	no				F07 Storeroom	no		
Hospital ACC Outpatient Clinic NHCU VBA Research Facilities	Electrical Closets	218.A	Corridor to Electrical Closets Single, opaque Pair, opaque	MC New	no				F07 Storeroom	no		
		218.C		MC Existing	no				F07 Storeroom	no		
Hospital ACC Outpatient Clinic NHCU Research Facilities	Medical Media Equip-ment Storage	219.A	Corridor to Medical Media Equipment Storage Single, opaque or framed glass Pair, opaque or framed glass	MC New	yes				F07 Storeroom and electric strike	yes	IDS with alarm	
		219.C		MC Existing	yes				F07 Storeroom and electric strike	yes	IDS with alarm	

* References for ANSI/BHMA Designations: “F-__”– ANSI/BHMA A156.13; “Exit __”– ANSI/BHMA A156.3

BUILDING INTERIOR (continued)

Facility Type	Entry Type	SDO	Locations and Descriptions	Facility Classification	Access Control					Monitoring		Other
					Card Reader	Fail Safe	Fail Secure	Other	ANSI/BHMA* or other function	Door Contact	Other	
Hospital ACC Outpatient Clinic	Evidence Storage	220.A	Corridor to Evidence Storage Single, opaque	MC New	yes		X		F07 Storeroom and electric strike	yes	IDS with alarm	FEBR (15 min./ Level III)
				MC Existing	yes		X		F07 Storeroom and electric strike	yes	IDS with alarm	FEBR (15 min./ Level III)
Hospital ACC Outpatient Clinic	Weapon Storage/ Armory	221.A	Security Control Center to Weapon Storage/Armory Single, opaque	MC New	yes		X	PIN or Biometrics	F07 Storeroom, electric strike, and magnetic lock	yes	IDS with alarm	FEBR (15 min./ Level III)
				MC Existing	yes		X	PIN or Biometrics	F07 Storeroom, electric strike, and magnetic lock	yes	IDS with alarm	FEBR (15 min./ Level III)
Hospital Research Facilities	Animal Research Facility	222.A 222.C	Public Area to Animal Research Facility or Vivarium Single, opaque or framed glass Pair, opaque or framed glass	MC New	yes	X		PIN or Biometrics	F07 Storeroom and electric strike, or magnetic lock	yes	IDS with alarm	
				MC Existing	yes	X		PIN or Biometrics	F07 Storeroom and electric strike, or magnetic lock	yes	IDS with alarm	
Hospital Research Facilities	Research and Clinical Labs	222.A 222.C	Public Areas to Research and Clinical Laboratories Single, opaque or framed glass Pair, opaque or framed glass	MC New	yes	X		PIN or Biometrics	F07 Storeroom and electric strike, or magnetic lock	yes	IDS with alarm	
				MC Existing	yes	X		PIN or Biometrics	F07 Storeroom and electric strike, or magnetic lock	yes	IDS with alarm	
Hospital ACC Outpatient Clinic NHCU Research Facilities	Radio-active Materials Storage	223.A 223.C	Corridor to Areas Containing Radioactive Materials Single, opaque Pair, opaque	MC New	yes	X		PIN or Biometrics	F07 Storeroom and electric strike	yes	IDS with alarm	
				MC Existing	yes	X		PIN or Biometrics	F07 Storeroom and electric strike	yes	IDS with alarm	
Hospital ACC Outpatient Clinic NHCU VBA Research Facilities	Fire Control Center	224.A	Fire Control Center to Building Interior Single, opaque	MC New	no				F07 Storeroom	yes	IDS with alarm	
				MC Existing	no				F07 Storeroom	yes	IDS with alarm	
Hospital Research Facilities	Restricted Access Floors	225.0	Elevator to Restricted or Controlled Floor Opaque elevator cab and entrance doors	MC New	yes		X		Elevator Door Control	yes		
				MC Existing	yes		X		Elevator Door Control	yes		
Hospital Research Facilities	Restricted Access Floors	226.A	Stair to Restricted or Controlled Area Single, opaque	MC New	yes	X			Electric Strike and Exit 13	yes		
				MC Existing	yes	X			Electric Strike and Exit 13	yes		

* References for ANSI/BHMA Designations: “F-__”– ANSI/BHMA ; “Exit __”– ANSI/BHMA A156.3

BUILDING INTERIOR (continued)

Facility Type	Entry Type	SDO	Locations and Descriptions	Facility Classification	Access Control					Monitoring		Other
					Card Reader	Fail Safe	Fail Secure	Other	ANSI/BHMA* or other function	Door Contact	Other	
Hospital Research Facilities	Restricted Access Floors	227.A 227.C	Corridor to Restricted or Controlled Area Single, opaque Pair, opaque	MC New	yes	X			F07 Storeroom and electric strike	yes		
				MC Existing	yes	X			F07 Storeroom and electric strike	yes		
Hospital ACC Outpatient Clinic NHCU VBA Research Facilities	El-elevator Equipment Room	228.A 228.C	Corridor to Elevator Equipment Room Single, opaque Pair, opaque	MC New	yes		X		F07 Storeroom and electric strike	yes		
				MC Existing	no				Push-button combination lock	yes	IDS with alarm	
Hospital ACC Outpatient Clinic NHCU VBA Research Facilities	Building Systems	228.A 228.C	Corridor to Building Systems Rooms Single, opaque Pair, opaque	MC New	yes		X		F07 Storeroom and electric strike	yes		
				MC Existing	no				Push-button combination lock	no		
Hospital ACC Outpatient Clinic NHCU VBA Research Facilities	Mech. and Electrical	228.A 228.C	Corridor to Mechanical and Electrical Rooms Single, opaque Pair, opaque	MC New	yes		X		F07 Storeroom and electric strike	yes		
				MC Existing	no				Push-button combination lock	no		
Hospital Research Facilities	Select Agents	229.A 229.C	Rooms with Select Agents Single, opaque or framed glass Pair, opaque or framed glass	MC New	yes		X		F07 Storeroom and electric strike	yes		
				MC Existing	yes		X		F07 Storeroom and electric strike	yes		
Hospital Research Facilities	BSL Labs	230.A 230.C	Public Areas to BSL-3 Laboratory Suites Single, opaque or framed glass Pair, opaque or framed glass	MC New	yes	X		PIN or Biometrics	Magnetic Lock or electric strike	yes		
				MC Existing	yes	X		PIN or Biometrics	Magnetic Lock or electric strike	yes		
Research Facilities	Vivariums	222.A 222.C	Public Area to Vivarium Single, opaque or framed glass Pair, opaque or framed glass	MC New	yes	X		PIN or Biometrics	Magnetic Lock or electric strike	yes		
				MC Existing	yes	X		PIN or Biometrics	Magnetic Lock or electric strike	yes		

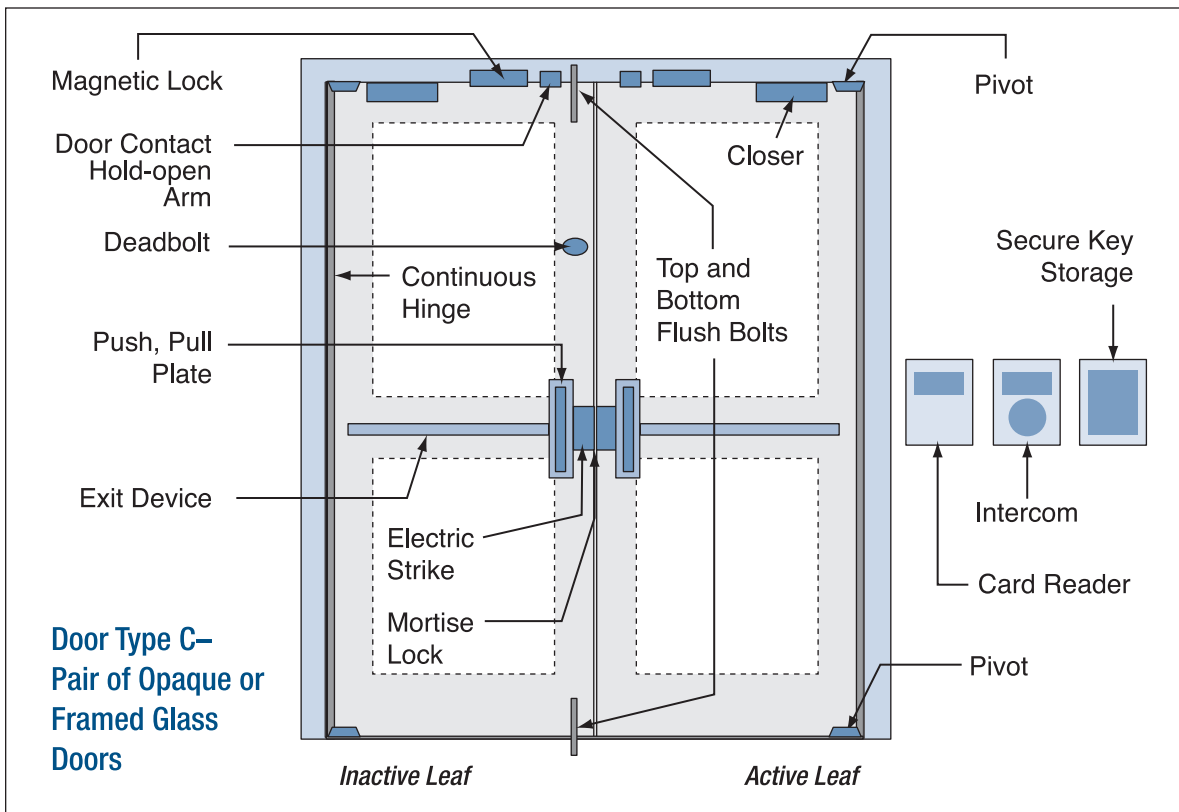
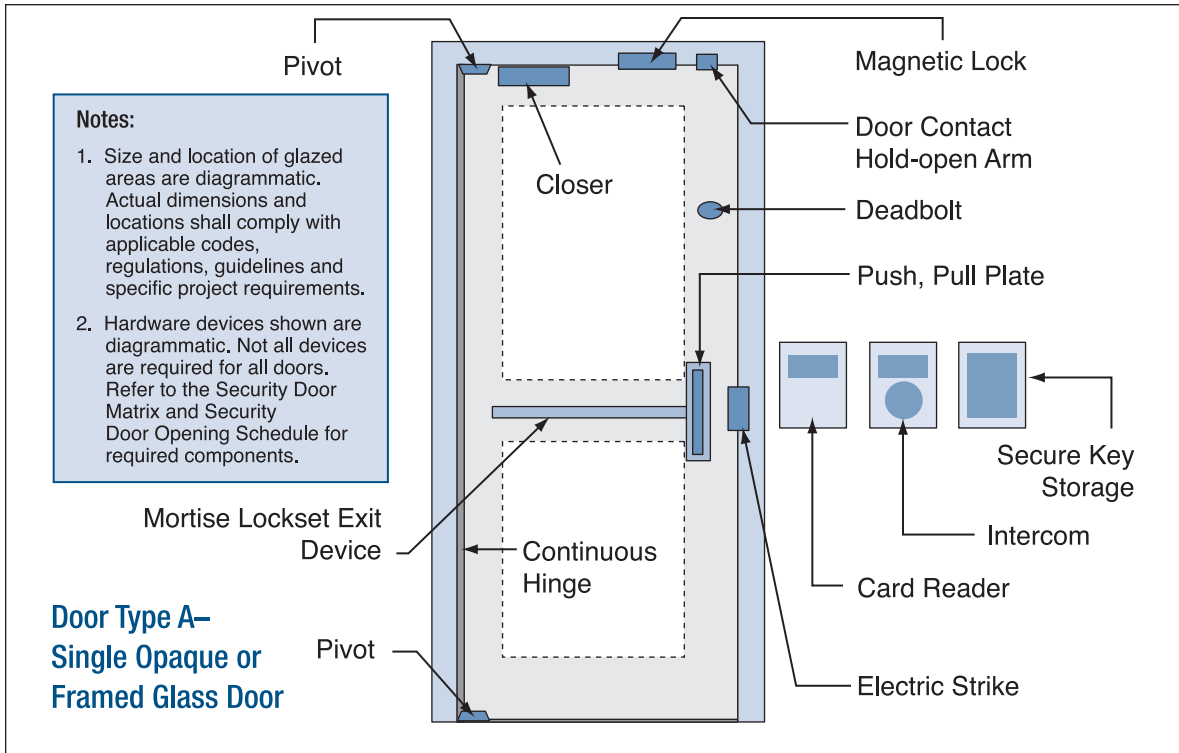
* References for ANSI/BHMA Designations: “F-__”– ANSI/BHMA A156.13; “Exit __”– ANSI/BHMA A156.3

BUILDING INTERIOR (continued)

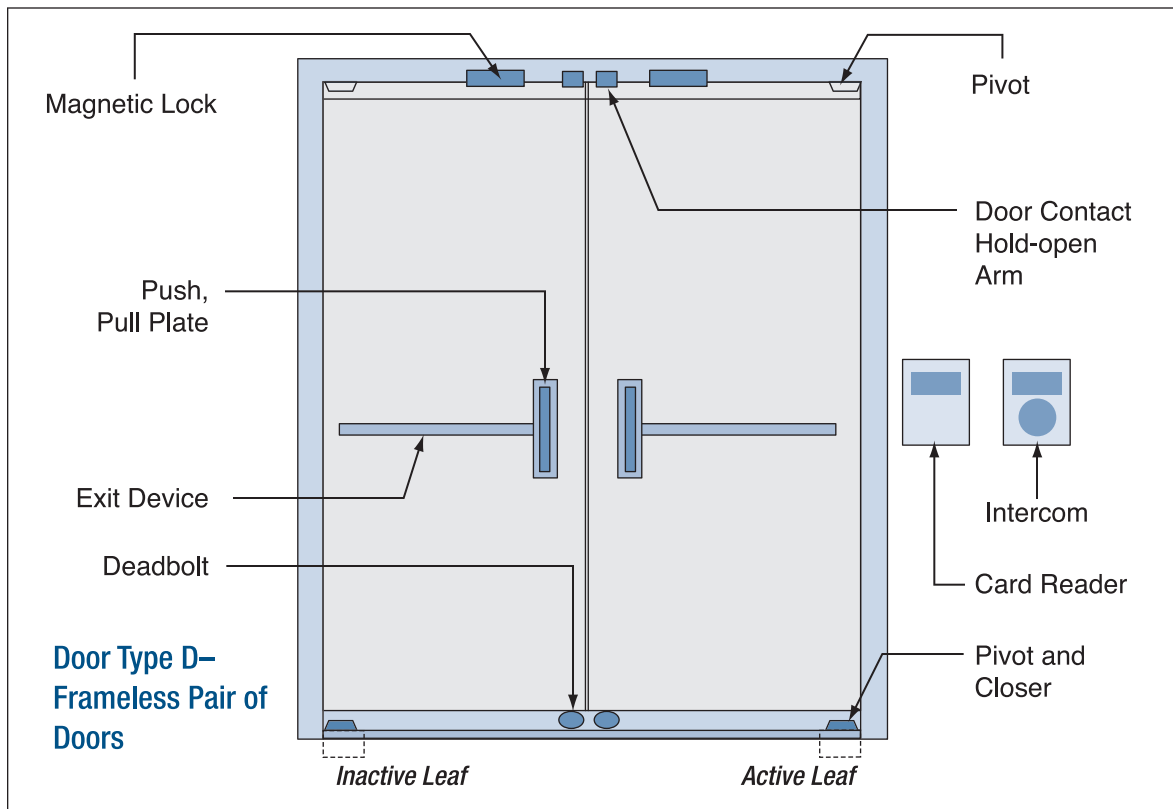
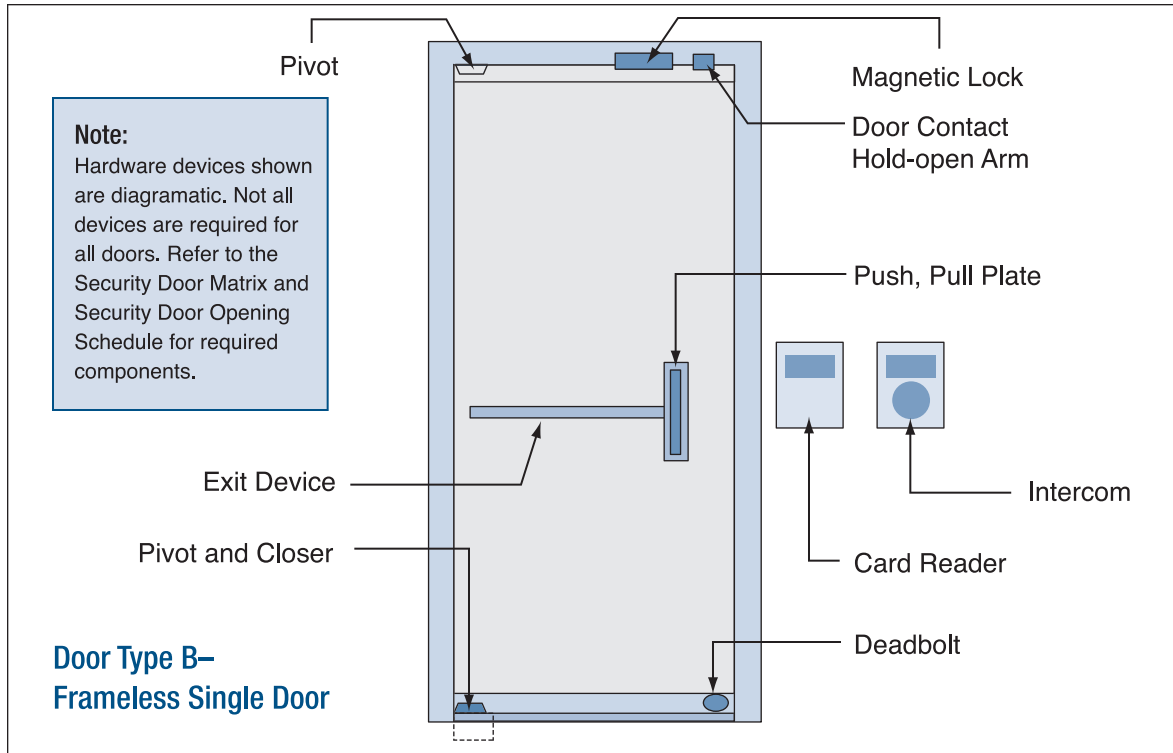
Facility Type	Entry Type	SDO	Locations and Descriptions	Facility Classification	Access Control					Monitoring		Other
					Card Reader	Fail Safe	Fail Secure	Other	ANSI/BHMA* or other function	Door Contact	Other	
Research Facilities	Vivariums	222.A	Vivarium Exit Single, opaque or framed glass	MC New	yes	X			EXIT 01	yes		
		222.C	Pair, opaque or framed glass	MC Existing	yes	X			EXIT 01	yes		
Hospital NHCU	Psychiatric Units	231.A	Public Areas to Psychiatric Unit Single, framed glass	MC New	yes	X			F01 Passage and magnetic lock	yes		Monitor at NS
				MC Existing	yes	X			F01 Passage and magnetic lock	yes		Monitor at NS
Hospital NHCU	Psychiatric Units	232.A	Psychiatric Unit Exit Only Single, framed glass	MC New	no				F01 Passage and magnetic lock	yes		Monitor at NS
				MC Existing	no				F01 Passage and magnetic lock	yes		Monitor at NS
Hospital	COOP	233.A	Public Areas to COOP Single, opaque	MC New	yes		X		F07 Storeroom, electric strike, and magnetic lock	yes	PIN or Biometrics	
		233.C	Pair, opaque	MC Existing	yes		X		F07 Storeroom, electric strike, and magnetic lock	yes	PIN or Biometrics	
Hospital Research Facilities	Interstitial Space	234.A	Stairs to Interstitial Space Single, opaque	MC New	yes	X			F07 Storeroom and electric strike	yes		
		234.C	Pair, opaque	MC Existing	no				Push-button combination	yes		

* References for ANSI/BHMA Designations: “F-__”– ANSI/BHMA A156.13; “Exit __”– ANSI/BHMA A156.3

VA Standard Security Door Types A and C



VA Standard Security Door Types B and D



Security Door Opening General Notes and Schedule

1. The hardware devices identified below indicate those generally required to meet the operational and security requirements. They are not all inclusive. Certain devices may not be applicable to every opening. For example, flush bolts are not required for single doors and neither continuous hinges nor electric strikes would be used on frameless doors.
2. When optional operational features are provided, refer to Security Door Opening Matrix for requirements by facility classification.
3. Items required for functional purposes that are not related to door operation are not included in the descriptions below. For example, an intercom may be required at a guard booth so that a visitor can communicate with the guard, but it is not required for door operation.

SDO 101

Hardware Devices:

- | | |
|------------------------------|-----------------|
| ■ Card Reader | ■ Flush Bolts |
| ■ Closer | ■ Intercom |
| ■ Continuous Hinge or Pivots | ■ Magnetic Lock |
| ■ Door Contact | ■ Mortise Lock |
| ■ Electric Strike | |
| ■ Exit Device | |

Normal Daytime Operation

- Free operation from either side

After Hours Operation

- Exterior lever inoperative
- Card reader on exterior releases electric strike or magnetic lock
- Remote release releases electric strike or magnetic lock
- Free operation from interior
- Door contact alarmed to central monitoring

SDO 102

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Exit Device
- Flush Bolts
- Hold-open Alarm
- Intercom
- Magnetic Lock
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Card reader releases electric strike
- Free operation from interior at all times

SDO 103

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge or Pivots
- Deadbolt
- Door Contact
- Electric Strike
- Exit Device
- Flush Bolts
- Hold-open Alarm
- Magnetic Lock
- Mortise Lock
- Pull

Normal Daytime Operation

- Free operation from either side

After Hours Operation

- Exterior lever inoperative
- Card reader on exterior releases electric strike or magnetic lock
- Delayed action and alarmed operation from interior when door is a means of egress; card reader for egress when door is not a required means of egress
- Door contact alarmed to central monitoring

SDO 104

Hardware Devices

- Closer
- Continuous Hinge or Pivots
- Door Contact
- Exit Device
- Flush Bolts
- Hold-open Alarm
- Mortise Lock

Operation At All Times

- Operation of exit device from inside retracts bolt and sounds local alarm and central monitoring station
- No operation from exterior

SDO 105

Hardware Devices

- Power Operator
- Card Reader
- Continuous Hinge
- Intercom
- Magnetic Lock

Normal Daytime Operation

- Power operated doors (swinging or horizontal sliding)
- Door activated by motion sensor on interior and exterior

After Hours Operation

- Power operated doors (swinging or horizontal sliding)
- Door activated from exterior by card reader or remote release
- Door activated by motion sensor on interior

SDO 106

Hardware Devices

- | | |
|------------------------------|-----------------|
| ■ Card Reader | ■ Exit Device |
| ■ Closer | ■ Flush Bolts |
| ■ Continuous Hinge or Pivots | ■ Intercom |
| ■ Door Contact | ■ Magnetic Lock |
| ■ Electric Strike | ■ Mortise Lock |

Normal Daytime Operation

- Free operation at all times

After Hours Operation

- Exterior lever inoperative
- Card reader on exterior releases electric strike or magnetic lock
- Remote release releases electric strike or magnetic lock
- Free operation from interior
- Door contact alarmed to nurses' station

SDO 107

Hardware Devices

- | | |
|--------------------|-------------------|
| ■ Card Reader | ■ Flush Bolts |
| ■ Closer | ■ Hold-open Alarm |
| ■ Continuous Hinge | ■ Mortise Lock |
| ■ Door Contact | |
| ■ Electric Strike | |

Operation At All Times

- Outside levers always rigid
- Card reader releases electric strike or key in outside lever retracts latchbolt
- Inside lever retracts latchbolt at all times
- Hold-open alarm annunciates at central monitoring station

SDO 108

Hardware Devices

- Card Reader
- Door Contact
- Intercom

Operation At All Times

- Card reader activates motorized door operator or provides access to manual operator

SDO 109

Hardware Devices

- Continuous Hinge
- Door Contact
- Flush Bolts

Operation At All Times

- Outside lever always rigid
- Inside lever retracts latchbolt at all times
- Door contact alarmed to central monitoring station

SDO 110

Hardware Devices

- Closer
- Continuous Hinge
- Knox Box®
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Key in Knox Box® retracts latchbolt from exterior
- Inside lever retracts latchbolt at all times

SDO 111

Hardware Devices

- Closer
- Continuous Hinge
- Door Contact
- Flush Bolts
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Key retracts latchbolt from exterior
- Inside lever retracts latchbolt at all times
- Door monitor alarmed at central monitoring station

SDO 112

Hardware Devices

- | | |
|------------------------------|-------------------|
| ■ Card Reader | |
| ■ Closer | ■ Hold-open Alarm |
| ■ Continuous Hinge or Pivots | ■ Intercom |
| ■ Door Contact | ■ Magnetic Lock |
| ■ Electric Strike | ■ Mortise Lock |
| ■ Exit Device | |
| ■ Flush Bolts | |

Normal Daytime Operation

- Outside lever always rigid
- Card reader or remote switch release electric strike or magnetic lock
- Inside lever releases latchbolt; card reader, remote switch or fire alarm release magnetic lock
- Door alarmed to central monitoring station

SDO 113

Hardware Devices

- Closer
- Continuous Hinge
- Flush Bolts
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Key retracts latchbolt from exterior
- Inside lever retracts latchbolt at all times

SDO 114

Hardware Devices

- Closer
- Continuous Hinge
- Mortise Lock

Operation At All Times

- Outside lever rigid when locked by mechanical device
- Outside lever free when unlocked by mechanical device
- Inside lever retracts latchbolt at all times

SDO 201

Hardware Devices

- Closer
- Continuous Hinge or Pivots
- Exit Device
- Flush Bolts
- Mortise Lock

Normal Daytime Operation

- Outside (lobby side) lever set for free operation
- Free passage from interior

After Hours Operation

- Outside (lobby side) lever rigid
- Free passage from interior

SDO 202

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Exit Device
- Flush Bolts
- Hold-open Alarm
- Intercom
- Magnetic Lock
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Card reader or remote switch release electric strike or magnetic lock
- Card reader and fire alarm release magnetic lock from interior
- Inside lever retracts latchbolt at all times

SDO 203

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Flush Bolts
- Hold-open Alarm
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Outside card reader releases electric strike or outside combination lock retracts latchbolt
- Inside lever retracts latchbolt at all times
- Door alarmed to central monitoring station

SDO 204

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Outside card reader releases electric strike or outside combination lock retracts latchbolt
- Inside lever retracts latchbolt at all times
- Door alarmed to central monitoring station

SDO 205

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Deadbolt
- Door Contact
- Electric Strike
- Mortise Lock

Operation At All Times

- Outside and inside levers always rigid
- Card reader releases electric strike
- Door monitor alarmed to central monitoring station

SDO 206

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Outside card reader releases electric strike or outside combination lock retracts latchbolt
- Inside lever retracts latchbolt at all times
- Door monitor alarmed to central monitoring station

SDO 207

Hardware Devices

- Closer
- Continuous Hinge or Pivots
- Door Contact
- Exit Device
- Flush Bolts
- Mortise Lock

Normal Daytime Operation

- Free operation from either side

After Hours Operation

- Outside lever always rigid
- Exit device releases latchbolts from interior
- Door monitor alarmed to central monitoring station

SDO 208

Hardware Devices

- Closer
- Continuous Hinge
- Door Contact
- Flush Bolts
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Inside lever retracts latchbolt at all times
- Door monitor alarmed to central monitoring station

SDO 209

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Mortise Lock

Normal Daytime Operation

- Outside lever always rigid
- Card reader releases electric strike
- Inside lever retracts latchbolt

After Hours Operation

- Outside lever always rigid
- Card reader releases electric strike from outside
- Inside lever retracts latchbolt
- Door monitor alarmed to central monitoring station

SDO 210

Hardware Devices

- | | |
|--------------------|-------------------|
| ■ Card Reader | ■ Flush Bolts |
| ■ Closer | ■ Hold-open Alarm |
| ■ Continuous Hinge | ■ Intercom |
| ■ Door Contact | ■ Mortise Lock |
| ■ Electric Strike | |

Operation At All Times

- Outside and inside levers rigid at all times
- Card reader with biometric or PIN identification retracts electric strike from either side
- Door monitor alarmed to central monitoring station

SDO 211

Hardware Devices

- | | |
|--------------------|-------------------|
| ■ Card Reader | ■ Electric Strike |
| ■ Closer | ■ Hold-open Alarm |
| ■ Continuous Hinge | ■ Intercom |
| ■ Door Contact | ■ Mortise Lock |

Operation At All Times

- Outside and inside levers rigid at all times
- Card reader with biometric or PIN identification retracts electric strike from either side
- Door monitor alarmed to central monitoring station

SDO 212

Hardware Devices

- | | |
|--------------------|-------------------|
| ■ Card Reader | ■ Electric Strike |
| ■ Closer | ■ Hold-open Alarm |
| ■ Continuous Hinge | ■ Mortise Lock |
| ■ Door Contact | |

Operation At All Times

- Outside and inside levers rigid at all times
- Card reader or remote release retracts electric strike from either side
- Door monitor alarmed to pharmacy and central monitoring station

SDO 213

Hardware Devices

- | | |
|--------------------|-------------------|
| ■ Card Reader | ■ Electric Strike |
| ■ Closer | ■ Flush Bolts |
| ■ Continuous Hinge | ■ Intercom |
| ■ Door Contact | ■ Mortise Lock |

Operation At All Times

- Outside lever always rigid
- Card reader or remote switch releases electric strike
- Inside lever retracts latchbolt at all times
- Door monitor alarmed to central monitoring station

SDO 214

Hardware Devices

- | | |
|--------------------|----------------|
| ■ Closer | ■ Flush Bolts |
| ■ Continuous Hinge | ■ Mortise Lock |

Operation At All Times

- Outside lever always rigid
- Latchbolt released from outside by combination lock
- Inside lever retracts latchbolt at all times

SDO 215

Hardware Devices

- Closer
- Continuous Hinge
- Door Contact
- Flush Bolts
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Latchbolt released from outside by combination lock
- Inside lever retracts latchbolt at all times

SDO 216

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Flush Bolts
- Intercom
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Card reader with biometric or PIN identification retracts electric strike
- Inside lever retracts latchbolt at all times
- Door monitor alarmed to central monitoring station

SDO 217

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Flush Bolts
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Card reader with biometric or PIN identification retracts electric strike
- Inside lever retracts latchbolt at all times
- Door monitor alarmed to central monitoring station

SDO 218**Hardware Devices**

- Continuous Hinge
- Flush Bolts
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Latchbolt released by key outside and lever inside

SDO 219**Hardware Devices**

- | | |
|--------------------|-------------------|
| ■ Card Reader | ■ Electric Strike |
| ■ Closer | ■ Flush Bolts |
| ■ Continuous Hinge | ■ Mortise Lock |
| ■ Door Contact | |

Operation At All Times

- Outside lever rigid at all times
- Card reader releases electric strike from outside
- Inside lever retracts latchbolt at all times
- Door monitor alarmed to central monitoring station

SDO 220

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Mortise Lock

Operation At All Times

- Outside lever rigid at all times
- Card reader releases electric strike from outside
- Inside lever rigid at all times
- Card reader releases electric strike from inside
- Door monitor alarmed to central monitoring station

SDO 221

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Deadbolt
- Door Contact
- Electric Strike
- Magnetic Lock
- Mortise Lock

Operation At All Times

- Outside lever rigid at all times
- Card reader with biometric or PIN identification releases electric strike and magnetic lock from outside
- Inside lever rigid at all times
- Card reader with biometric or PIN identification releases electric strike and magnetic lock from inside
- Door monitor alarmed to central monitoring station

SDO 222

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Flush Bolts
- Intercom
- Magnetic Lock
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Card reader with biometric or PIN identification releases electric strike or magnetic lock
- Inside lever retracts latchbolt at all times or request to exit button releases magnetic lock
- Door monitor alarmed to central monitoring station

SDO 223

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Flush Bolts
- Mortise Lock

Operation At All Times

- Outside and inside levers rigid at all times
- Card reader with biometric or PIN identification releases electric strike on either side
- Door monitor alarmed to central monitoring station

SDO 224

Hardware Devices

- Closer
- Continuous Hinge
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Key in outside lever retracts latchbolt
- Inside lever retracts latchbolt at all times
- Door monitor alarmed to central monitoring station

SDO 225

Hardware Devices

- Card Reader
- Door Contact

Operation At All Times

- Card reader permits elevator door to open on restricted access floors
- Door monitor alarmed to central monitoring station

SDO 226

Hardware Devices

- | | |
|--------------------|-------------------|
| ■ Card Reader | ■ Electric Strike |
| ■ Closer | ■ Exit Device |
| ■ Continuous Hinge | |
| ■ Door Contact | |

Operation At All Times

- Outside lever (stair side) always rigid
- Card reader releases electric strike
- Delayed action and alarmed operation from inside (occupied side) when door is a means of egress; card reader for egress when door is not a required means of egress
- Door monitor alarmed to central monitoring station

SDO 227

Hardware Devices

- | | |
|--------------------|----------------|
| ■ Card Reader | ■ Exit Device |
| ■ Closer | ■ Flush Bolts |
| ■ Continuous Hinge | ■ Intercom |
| ■ Door Contact | ■ Mortise Lock |
| ■ Electric Strike | |

Operation At All Times

- Outside lever always rigid
- Card reader or remote switch releases electric strike
- Inside lever retracts latchbolt at all times
- Door monitor alarmed to central monitoring station

SDO 228

Hardware Devices

- | | |
|--------------------|-------------------|
| ■ Card Reader | ■ Electric Strike |
| ■ Closer | ■ Flush Bolts |
| ■ Continuous Hinge | ■ Mortise Lock |
| ■ Door Contact | |

Operation At All Times

- Outside lever always rigid
- Card reader releases electric strike or combination lock retracts latchbolt
- Inside lever retracts latchbolt at all times
- Door monitor alarmed to central monitoring station

SDO 229

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Flush Bolts
- Intercom
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Card reader or remote switch releases electric strike from outside
- Inside lever always rigid
- Card reader releases electric strike from inside
- Door monitor alarmed to central monitoring station

SDO 230

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Flush Bolts
- Intercom
- Magnetic Lock
- Mortise Lock

Operation At All Times

- Outside lever always rigid
- Card reader or remote switch releases electric strike or magnetic lock from outside
- Inside lever always rigid
- Card reader or fire alarm releases electric strike or magnetic lock from inside
- Door monitor alarmed to central monitoring station

SDO 231

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Hold-open Alarm
- Intercom
- Magnetic Lock
- Mortise Lock

Operation At All Times

- Outside and inside levers always free (passage function for latching requirements only)
- Card reader or remote switch at nurses' station releases magnetic lock
- Fire alarm releases magnetic lock
- Door monitor alarmed at nurses' station

SDO 232

Hardware Devices

- Closer
- Continuous Hinge
- Door Contact
- Exit Device
- Magnetic Lock

Operation At All Times

- No hardware on outside
- Magnetic lock released by remote switch at nurses' station or by fire alarm
- Door monitor alarmed at nurses' station

SDO 233

Hardware Devices

- Card Reader
- Closer
- Continuous Hinge
- Door Contact
- Electric Strike
- Flush Bolts
- Intercom
- Magnetic Lock
- Mortise Lock

Operation At All Times

- Outside lever rigid at all times
- Card reader with biometric or PIN identification or remote switch release electric strike and magnetic lock from outside
- Card reader, remote release, or request to exit button release electric strike and magnetic lock from inside
- Door monitor alarmed to COOP and central monitoring station

SDO 234

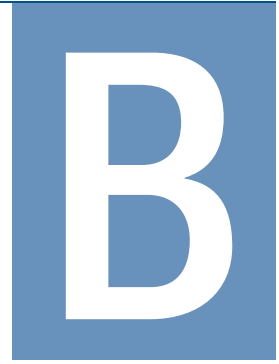
Hardware Devices

- | | |
|--------------------|-------------------|
| ■ Card Reader | ■ Electric Strike |
| ■ Closer | ■ Flush Bolts |
| ■ Continuous Hinge | ■ Mortise Lock |
| ■ Door Contact | |

Operation At All Times

- Outside lever rigid at all times
- Card reader on outside releases electric strike or combination lock on outside retracts latchbolt
- Inside lever retracts latchbolt at all times
- Door monitor alarmed at central monitoring station

Security System Application Matrix



BUILDING EXTERIOR

Area of Coverage	Fixed Camera	Pan/ Tilt/ Zoom ¹	Controller	Monitor ²	Recording Device	Matrix Switcher	Motion Det.	Glass Break	Door Contact ³	Card Reader	Biometrics ⁴	Intercom	Duress/ Panic Alarm	Emer. Phone/ Call Box	Optional ⁵			
															X-Ray Mach.	WTMD	HHMD	Itemizer
		CCTV						IDS			PACS		DSPI			DSS		
Access Roadways / Vehicle Gates	X	X								X		X						
Air Intake Areas	X						X		X									
ATM Areas	X																	
Cemetery																		
Administration Building							X	X	X				X					
Storage and Supply Buildings							X	X	X									
Common Ground / Pathways / Sidewalks	X	X												X				
Credit Union	X						X	X	X				X					
Child Care Center	X	X	X	X	X	X	X	X	X	X		X	X	X				
Drop Off / Pick Up Points	X													X				
Elevator Machinery Room	X						X		X	X		X						
Emergency Exit / Perimeter Doors	X	X					X		X									
Emergency Room / Facility Entrance	X	X					X	X	X	X		X						
Employee Entrance / Secondary Doors	X	X					X		X	X		X						
Exterior Windows (AC Unit Inserts)		X					X	X										
Exterior Windows (Ground Accessible)		X					X	X										
Hazardous Material Storage / Enclosures																		
Bio Hazard Waste	X	X					X	X	X	X								
Fuel	X	X					X	X	X									
Liquid Oxygen	X	X					X	X	X									
Medical Gas	X	X					X	X	X	X								
Propane	X	X					X	X	X									
Radioactive Materials Storage	X	X					X	X	X	X			X					
Select Agents Area	X	X					X	X	X	X			X					
Laundry Plant	X	X					X	X	X	X		X	X					
Loading Docks	X			X					X	X		X						
Main Entrance	X	X						X	X			X						
Maintenance Shop	X	X					X	X	X				X					
Nursing Home	X	X	X	X	X	X	X	X	X	X		X	X	X				
Parking Garages	X	X								X		X		X				
Parking Garages (Underground)	X	X								X		X		X				
Parking Lot Areas (Employees)	X	X								X		X		X				
Parking Lot Areas (Open / Visitor / Vendor)	X	X												X				
Pedestrian Access Point	X	X							X									

BUILDING EXTERIOR (continued)

Area of Coverage	Fixed Camera	Pan/ Tilt/ Zoom ¹	Controller	Monitor ²	Recording Device	Matrix Switcher	Motion Det.	Glass Break	Door Contact ³	Card Reader	Biometrics ⁴	Intercom	Duress/ Panic Alarm	Emer. Phone/ Call Box	Optional ⁵			
															X-Ray Mach.	WTMD	HHMD	Itemizer
		CCTV						IDS			PACS		DSPI			DSS		
Perimeter Fence / Wall / Barrier	X	X					X											
Rooftop Access	X	X					X		X	X		X						
Security Guard House / Vehicle Screening Area	X	X		X			X	X				X	X					
Service Entrance	X	X							X	X		X						
Service Vehicle Roadway Gates	X	X								X		X						
Service Yard	X	X												X				
Shipping / Receiving Area	X	X					X	X	X	X		X			X			X
Loading Dock Bay Areas	X	X					X	X	X	X		X	X		X			X
Mailroom	X	X					X	X	X	X		X	X		X			X
UPS Battery / Generator Area	X	X					X	X	X	X								
Utility Buildings																		
Electrical	X	X					X	X	X	X								
Energy Center	X	X					X	X	X	X		X	X					
Mechanical	X	X					X	X	X	X								
Signal	X	X					X	X	X	X								
Telecommunications	X	X					X	X	X	X								
Water Storage / Processing	X	X					X	X	X	X								
Utility Service Tunnel Entrance / Exit	X	X					X		X	X		X		X				
VA Benefits / Regional Office Building	X	X		X			X	X	X	X		X	X		X	X	X	X
Vehicle Entrances / Site Access (Open Access)	X	X												X				
Warehouse Building	X	X		X			X	X	X	X		X	X		X	X	X	X

Footnotes:

1. P/T/Z cameras shall be deployed primarily to monitor site and building exterior areas. They will supplement the use of fixed cameras if they can be programmed to monitor multiple areas with minimal human interface required.

2. A dedicated CCTV camera monitor may be required to provide staff with the ability to monitor access to these controlled areas.

3. Door contacts shall be installed as a back-up to the use of security motion detection devices.

4. Biometric security devices shall only be used as a secondary means of providing access control. Card readers will be the primary security access device used.

5. The use of DSS equipment is indicated as an optional means to screen persons, items, and materials carried into or delivered to a facility. Each facility shall be addressed on a case-by-case basis as to DSS equipment requirements.

BUILDING INTERIOR

Area of Coverage	Fixed Camera	Pan/ Tilt/ Zoom ¹	Controller	Monitor ²	Recording Device	Matrix Switcher	Motion Det.	Glass Break	Door Contact ³	Card Reader	Biometrics ⁴	Intercom	Duress/ Panic Alarm	Emer. Phone/ Call Box	Optional ⁵			
															X-Ray Mach.	WTMD	HHMD	Itemizer
	CCTV							IDS			PACS		DSPI			DSS		
Agent Cashier	X						X	X	X	X		X	X					
Animal Research / Vivarium	X		X	X		X	X	X	X	X	X	X	X					
ATM	X						X	X	X	X								
BSL Labs	X		X	X	X	X	X	X	X	X	X	X	X					
Building Corridors (Restricted / Controlled)	X	X					X	X		X		X						
Building Lobby / Reception Area	X	X						X							X	X	X	X
Cafeteria	X						X	X	X	X			X					
Canteen Office							X	X	X				X					
Canteen Retail Store	X						X	X	X				X					
Canteen Storage	X						X	X	X									
Child Care Center	X	X	X	X	X	X	X	X	X	X		X	X	X				
COOP Room / Facility	X	X	X	X	X	X	X	X	X	X	X	X						
Credit Union	X						X	X	X				X					
Domiciliary	X	X		X			X	X	X	X		X	X	X				
Elevator Equipment Room	X						X		X	X			X					
Elevator Lobby / Floor Access Areas	X						X	X		X		X						
Emergency Exit / Egress Doors	X	X					X		X									
Emergency (Urgent Care) Area										X		X			X	X	X	X
Nursing Station	X							X					X					
Waiting Room	X							X										
Fire Pump Room	X						X		X	X								
General Waiting Areas	X							X										
Hazardous Material Storage / Enclosure																		
Bio Hazard Waste	X	X					X	X	X	X								
Fuel	X	X					X	X	X									
Liquid Oxygen	X	X					X	X	X									

BUILDING INTERIOR (continued)

Area of Coverage	Fixed Camera	Pan/ Tilt/ Zoom ¹	Controller	Monitor ²	Recording Device	Matrix Switcher	Motion Det.	Glass Break	Door Contact ³	Card Reader	Biometrics ⁴	Intercom	Duress/ Panic Alarm	Emer. Phone/ Call Box	Optional ⁵			
															X-Ray Mach.	WTMD	HHMD	Itemizer
		CCTV						IDS			PACS		DSPI			DSS		
Medical Gas	X	X					X	X	X	X								
Propane	X	X					X	X	X									
Radioactive Materials Storage	X						X	X	X	X			X					
Select Agents Area	X						X	X	X	X			X					
Interstitial Space (Controlled Access)	X	X					X	X	X	X								
Information Resource Management (IRM)	X		X	X		X	X	X	X	X	X	X	X					
IRM Data Closet	X	X					X	X	X	X								
Laboratory (Clinical)	X	X	X	X		X	X	X	X	X		X	X					
Laundry Plant	X	X					X	X	X	X		X	X					
Library / Research	X						X	X	X	X			X					
Linen Supply / Storage	X						X	X	X									
Maintenance Shop	X	X					X	X	X				X					
Medical Directors Office	X	X					X	X	X	X		X	X					
Medical Gas Bulk Storage	X	X					X	X	X	X								
Medical Media Equipment Storage	X	X					X	X	X	X								
Medical Records Storage	X	X					X	X	X	X								
Nuclear Medicine Areas	X						X	X	X	X		X	X					
Nursing Home	X	X	X	X	X	X	X	X	X	X		X	X	X				
Operator Switchboard	X							X	X	X		X	X					
Pedestrian Corridor	X	X					X							X				
Pedestrian Tunnel/ Pathways	X	X					X							X				
Pedestrian Skywalk	X	X					X							X				
Pharmacy																		
Control Substance Room	X						X	X	X	X		X	X					
Dispensing Room	X						X	X	X	X		X	X					
Drug Cache	X						X	X	X	X		X						

BUILDING INTERIOR (continued)

Area of Coverage	Fixed Camera	Pan/ Tilt/ Zoom ¹	Controller	Monitor ²	Recording Device	Matrix Switcher	Motion Det.	Glass Break	Door Contact ³	Card Reader	Biometrics ⁴	Intercom	Duress/ Panic Alarm	Emer. Phone/ Call Box	Optional ⁵			
															X-Ray Mach.	WTMD	HHMD	Itemizer
															CCTV			
Drug Storage Room	X						X	X	X	X		X						
Inpatient / Outpatient Service Windows	X						X	X					X					
Manufacturing Area	X						X	X	X	X			X					
Primary Inventory (Medical Supplies)	X						X	X	X	X								
Psychiatric Units	X		X	X				X	X	X		X	X					
Research Clinical Labs	X		X	X			X	X	X	X		X	X					
Research Library	X		X	X			X	X	X	X		X	X					
Security Control Center (SCC)	X		X	X	X	X		X	X	X		X	X					
Security System Equipment Closets	X						X	X	X	X								
Shipping / Receiving Area																		
Loading Dock Bay Areas	X	X					X	X	X	X		X	X		X			X
Mailroom	X						X	X	X	X			X		X			X
Stairwells	X						X	X	X	X		X		X				
Telecommunication / Data Equipment Areas																		
Telephone Data Closet	X						X	X	X	X		X						
Main Computer Room	X						X	X	X	X		X						
Main Telephone Room	X						X	X	X	X		X						
Travel Office	X						X	X	X	X			X					
Utility Rooms																		
Battery-UPS-Generator Area	X						X	X	X	X		X						
Electrical	X						X	X	X	X		X						
Mechanical	X						X	X	X	X		X						
Signal	X						X	X	X	X		X						
Telecommunications	X						X	X	X	X		X						
Utility Tunnel Pathway	X	X					X		X	X				X				

BUILDING INTERIOR (continued)

Area of Coverage	Fixed Camera	Pan/ Tilt/ Zoom ¹	Controller	Monitor ²	Recording Device	Matrix Switcher	Motion Det.	Glass Break	Door Contact ³	Card Reader	Biometrics ⁴	Intercom	Duress/ Panic Alarm	Emer. Phone/ Call Box	Optional ⁵			
															X-Ray Mach.	WTMD	HHMD	Itemizer
	CCTV							IDS			PACS		DSPI			DSS		
VA Benefits / Regional Office Building	X	X					X	X	X	X		X	X		X	X	X	X
VA Police Office																		
Holding Area	X		X	X	X			X	X	X		X						
Processing Room							X	X	X	X								
Property / Evidence Room	X						X	X	X	X								
Weapon Storage/armory	X		X	X	X		X	X	X	X								
Ward / Medical Treatent Room	X						X	X	X	X		X	X					

Footnotes:

1. P/T/Z cameras shall be deployed primarily to monitor site and building exterior areas. They will supplement the use of fixed cameras if they can be programmed to monitor multiple areas with minimal human interface required.

2. A dedicated CCTV camera monitor may be required to provide staff with the ability to monitor access to these controlled areas.

3. Door contacts shall be installed as a back-up to the use of security motion detection devices.

4. Biometric security devices shall only be used as a secondary means of providing access control. Card readers will be the primary security access device used.

5. The use of DSS equipment is indicated as an optional means to screen persons, items, and materials carried into or delivered to a facility. Each facility shall be addressed on a case-by-case basis as to DSS equipment requirements.

Index

Agent Cashier, 5.1, 5.1.5, Appendix A

Air Intakes and Exhausts, 5.9.1.2, 5.10.1.3, 6.0, 6.5, 6.5.1, 6.5.2, 9.1.2, Appendix B

Anti-ram Resistance, 3.4.1.2, 3.4.2.2, 5.6.3.1, 7.4, 7.4.2

Atria, 6.3, 6.3.2

Blast Resistance, 4.3.2, 5.7.5, 6.6, 6.6.2, 7.0, 7.1, 7.1.1, 7.1.2, 7.3, 7.5, 7.5.1, 7.5.2

Building Exits, 4.0, 4.3, 4.3.2, 4.3.3, 4.3.4, 5.3.2.2, Appendix A, Appendix B

Cache, 5.2, 5.2.3.1, 5.2.3.2, 5.2.4, 5.2.5, Appendix A, Appendix B

Calculation Methods, 6.6, 7.5

Charge Weight, 4.1.5.4, 5.9.3.1, 5.9.6.2, 5.10.3

Childcare/Development Center, 3.5.3.3, 5.3, 5.3.1, 5.3.2.1, 5.3.2.2, 5.3.4, 5.3.5, 5.9.1.2, 5.10.1.3, Appendix A, Appendix B

Closed Circuit Television (CCTV), 1.3.1.5, 3.5.3.3, 3.5.3.6, 3.6.1.2, 3.6.2.2, 3.6.2.3, 3.6.2.4, 3.6.2.5, 3.6.2.7, 3.6.2.9, 4.1.4, 4.1.6.3, 4.3.3, 5.5.2, 5.5.4, 5.6.4.2, 5.9.4.2, 5.9.4.3, 5.9.5, 5.10.4.1, 5.11.4, 5.12.4, 5.13.4, 5.14.2.1, 5.14.2.3, 5.14.4.1, 5.14.5.2, 10.1, 10.1.1, 10.1.2, 10.1.3, 10.1.3.10, 10.1.4, 10.1.5, 10.2, 10.2.4, 10.2.8, 10.2.9, 10.2.11, 10.4.1.4, 10.4.2.5, 10.4.2.8, 10.4.3, 10.4.3.7, 10.5, 10.5.4, 10.5.10, 11.0, Appendix B

Column Protection, 7.3, 7.3.1

Computer Room, 5.4, 5.4.1, 5.4.2, 5.4.3.1, 5.4.5, 5.13.3, 9.0, 9.2.2, 9.3.1.1, 9.3.1.4, 9.3.2.1, 9.3.2.4, 9.3.3, 9.3.10, Appendix A, Appendix B

Continuity of Operations (COOP), 1.3.1.5, 5.5, 5.5.1, 5.5.2, 5.5.3.2, 5.5.3.3, 5.5.4, 5.5.5.1, 5.5.6, 5.9.1, 5.9.1.2, 5.10.1.3

COOP Site, 1.3.1.5, 5.5, 5.5.5, Appendix A, Appendix B

Controlled Access Area or Controlled Area, 1.3.1.2, 3.5.4, 5.9.6.3, Appendix A, Appendix B

Crime Prevention Through Environment Design (CPTED), 1.3.2

Critical Assets, 10.1.1.1

Detection and Screening System (DSS), 10.0, 10.5, 10.6, 10.6.1, Appendix B

Duress Security Phone Intercom System (DSPI), 10.0, 10.2, 10.4, 10.4.1, 10.4.4, 10.5

Electrical Systems, 9.0, 9.2, 9.2.1.1, 9.2.1.4, 9.2.3, Appendix A, Appendix B.

Emergency Department, 4.0, **5.6**, 5.6.1, 5.6.2.1, 5.6.3.1, 5.6.3.2, Appendix A, Appendix B

Emergency Department Entrances, 5.6.1, 5.6.2.1, 5.6.3.1, 5.6.3.2, Appendix A, Appendix B

Emergency and/or Stand-by Generator Room, **5.7**, 5.7.1.1, 5.7.1.2, 5.7.5, Appendix A, Appendix B

Energy Center/Boiler Plant, **5.8**, 5.8.1, 5.8.2, 5.8.4, **8.3**, 8.3.2, 8.3.3, 8.3.4, 8.3.6, 9.1.1.3, Appendix B

Fenestration, 6.0, 6.1.1.3, **6.2**, 6.2.1, 6.2.1.1, 6.2.2

Fire Protection Systems, 8.0, **9.5**, 9.5.2, Appendix A, Appendix B

HVAC Systems, 5.15.3.2, **9.1**, 9.1.3, 9.3.2.2, 9.3.3.2, 9.3.4.2, 9.3.6.2

Intrusion Detection System (IDS), 10.0, 10.1.6.2, **10.2**, 10.2.1, 10.2.2, 10.2.3.1, 10.2.4, 10.2.5.2, 10.2.6, 10.2.10, 10.2.11, 10.4.3.7, 10.5, Appendix B

Life-Safety Protected, 1.9

Loading Dock, 3.5.3.4, 3.6.2.9, 4.0, 4.3, 4.3.3, 5.2.1, 5.4.1, 5.5.1, 5.6.1.2, 5.7.1, 5.7.2.1, 5.7.5, 5.8.1.2, 5.8.1.3, 5.8.2, **5.9**, 5.9.1, 5.9.1.3, 5.9.2, 5.9.3, 5.9.3.5, 5.9.4, 5.9.4.2, 5.9.4.3, 5.9.5, 5.9.5.1, 5.9.6, 5.9.6.2, 5.10.1, 5.10.4, 5.11.1, 5.13.1, 5.14.1.2, 5.14.4.1, 7.1, 7.3, 8.2.2, 8.2.3.2, 9.2.1.2, 10.2.8, 10.4.1.4, Appendix A, Appendix B

Loading Docks and Service Entrances, 4.0, **5.9**, 5.9.1.3, 5.9.6, Appendix A, Appendix B

Mailroom, 4.3.1, 5.2.1, 5.4.1, 5.5.1, 5.6.1, 5.7.1, 5.7.5, 5.8.1.2, 5.8.1.3, 5.8.2, 5.9.1.1, 5.9.2, **5.10**, 5.10.1, 5.10.2.2, 5.10.3, 5.10.3.1, 5.10.3.2, 5.10.4.1, 5.10.5, 5.10.6, 5.11.1, 5.13.1, 5.14.1.2, 7.1, 7.3, Appendix A, Appendix B

Magnetometer or Metal Detector, 4.1.7.2, 10.6, Appendix B

Mission Critical, **1.0**, 1.1, 1.2, 1.3, 1.3.3, 1.4, 1.5, 1.6, 1.8, 1.9, 3.1, 3.2.53.3.1, 3.3.3.2, 3.4.3, 3.6.3, 4.0, 4.1.6.3, 4.2.3, 6.0, 6.4.3, 6.5, 6.5.2, 8.0, 8.3.1, 8.3.3, 9.0, 9.0.1, 9.2.1, 9.2.2, 9.2.3.1, 9.3.3, 10.0, 10.1.1.1, 10.2.8.3, 10.3.1

Parking, 1.3.1, 3.3.2.4, **3.5**, 3.5.1, 3.5.2, 3.5.2.2, 3.5.3, 3.5.4, 3.6.1, 3.6.2.4, 4.1.1.3, **4.2.2**, 5.6.3.4, 5.6.4.1, 5.9.3.4, 5.9.5.2, 7.1, 7.3, 10.1.1.1, 10.3.1, 10.4.1.4, 10.4.1.11, 10.4.2, 10.4.3.4, 10.4.3.5, 10.5.2

Patient Drop-offs, 4.0, 4.1.2, 4.1.5, 4.1.6.3, 4.1.7.1, **4.2**, 4.2.3, Appendix A, Appendix B

Pedestrian Barrier, 3.3.3.1, Appendix A, Appendix B

Perimeter Fences, 1.3.1.1, **3.2**, 3.2.3, 3.2.5, 3.3.1, 3.4.2.1, 3.6.2.2, 10.2.8, 10.2.8.2, 10.2.8.3, 10.2.8.4

Personnel Screening, 10.5.4, Appendix A, Appendix B

Pharmacy, 1.2, 1.3.1.3, 5.2, 5.2.1, **5.11**, 5.11.4, 5.11.5, Appendix A, Appendix B

Physical Access Control System (PACS), 10.0, 10.1.2.2, 10.2, 10.2.4, 10.2.7.3, **10.3**, 10.3.1, 10.3.2, 10.3.5.1, 10.3.5.2, 10.3.5.5, 10.3.8, 10.3.10, 10.3.12, 10.3.13, 10.4.1.5, 10.4.3, 10.5, Appendix A, Appendix B

Plumbing Systems, 8.0, 9.0, **9.4**, 9.4.2

Police Operations Room and Holding Room, 5.6.1.2, **5.12**, 5.12.1.2, 5.12.2.1, 5.12.2.2, 5.12.3.1, 5.12.3.2, 5.12.5, 5.15.1.4, 10.5.6, Appendix A, Appendix B

Protected Area, 10.2, 10.2.8.2

Protection Level, 1.3, 1.3.1, 1.3.1.2, 1.3.3, 1.6, 7.1, 7.3, 10.2.7

Progressive Collapse, 7.0, 7.1, 7.1.1, **7.2**, 7.2.1, 7.3, 11.0

Public Entrances and Lobbies, 3.6.1, **4.1**, 5.9.2, Appendix A, Appendix B

Records Storage and Archives, 1.1, 1.2, 1.3.1.4, **5.13**, 5.13.1, 5.13.3, 5.13.5, Appendix A, Appendix B

Research Laboratory and Vivarium, 1.3.1.4, **5.14**, 5.9.1.3, 5.9.6.3, 5.14.2, 5.14.2.1, 5.14.2.2, 5.14.2.3, 5.14.4, 5.14.5

Restricted Area, 1.3.1.5, 4.1.3.3, 4.1.7.4, 10.1.1.1, 10.2.7, 10.3.9, 10.4.1.4, Appendix A, Appendix B

Roofs, 6.0, **6.4**, 6.4.1, 6.4.4, 6.5.1.1, 7.1.1.1, 10.2.7, 10.2.7.2

Screening Vestibles, 4.1.2

Secured Door Opening (SDO), 5.1.4.3, 5.2.2, 5.3.2, 5.3.2.2, 5.4.2, 5.5.2, 5.5.2.2, 5.6.1, 5.6.2, 5.7.2, 5.8.2, 5.9.2, 5.9.3.2, 5.9.4.1, 5.10.2, 5.12.2, 5.13.2, 5.14.2, 5.15.2, **Appendix A**

Security Control Center (SCC), 4.1.3.2, 4.1.6.1, 5.5.4, 5.6.4, 5.7.4, 5.9.1.2, 5.10.1.3, 5.14.4, **5.15**, 5.15.1, 5.15.2, 5.15.3, 5.15.4, 5.15.5, 9.1.1.3, 10.0, 10.1.1.1, 10.1.2.1, 10.1.3.1, 10.1.6.1, 10.2.9, 10.3.1, 10.4.1.5, 10.4.2.1, 10.4.2.2, 10.4.2.5, 10.4.3, 10.4.3.1, 10.4.3.3, 10.4.3.5, **10.5**, Appendix A, Appendix B

Site Distribution (Utilities), **8.2**, 8.2.4

Site Lighting, **3.6**, 3.6.1, 3.6.1.1, 3.6.1.2, 3.6.1.4, 3.6.2, 10.1.3.10, 10.4.2.8, 10.5.7

Stand-off distance, **3.1**, 3.1.1, 3.5.3.3, 3.5.3.4, 6.1.1, 6.2.1, 6.3.1, 6.4.1, 6.4.2, 6.4.3, 6.5.1, 6.5.2, 7.1, 7.3, 9.1.2.2, 11.0

Telecommunications Systems, 8.0, 8.1.3, 8.2.3, 8.2.3.2, 9.0, 9.0.1, 9.0.2, 9.2.2, 9.2.3.1, **9.3**, 9.3.1, 9.3.5, 9.3.11, 11.0, Appendix A, Appendix B

Threat, 1.3.1.1, 1.6, 6.1.1, 6.2.1, 6.3.1, 6.3.1.1, 6.4.1, 6.4.2, 6.4.3, 6.5.1, 6.5.2, 7.0, 7.1, 7.2, 7.3, 9.1.2.2, 10.2.3, 11.0

Utility Entrances, 8.0, **8.1**, 8.1.4, Appendix A, Appendix B

Vehicle Inspection, 3.3.1

Vehicle and Pedestrian Screening, **3.3**, 3.3.2, 3.3.3, Appendix A, Appendix B.

Vehicle Barriers, 3.3.3.2, **3.4**, 3.4.1, 3.4.2, 3.4.3, 4.1.5.1, 5.5.1.3, 5.9.5.1, 7.0, 7.4.1

Water and Fuel Storage, 5.9.1.2, 5.10.1.3, 8.1.1.2, **8.4**, 8.4.2.1, 8.4.2.2, 8.4.2.3, 8.4.3, 8.4.6, 8.4.7, 9.0, Appendix B

X-ray Screening System, 10.6, 11.0, Appendix B

