VA

U.S. Department of Veterans Affairs

Office of Construction & Facilities Management

Physical Security and Resiliency Design Manual

OCTOBER 1, 2020

Revised January 1, 2021

Cover Photos

First row: Southeast Louisiana Veterans Health Care System, 1601 Perdido Street, New Orleans, Louisiana 70112; Washington D.C. Veterans Affairs Medical Center's (DCVAMC) Community Resource and Referral Center (CRRC), 1500 Franklin Street N.E., Washington, D.C. 20018.

Second row: Orlando VA Medical Center, 13800 Veterans Way, Orlando, Florida 32827; Willamette National Cemetery, 11800 Southeast Mt. Scott Boulevard, Portland, Oregon 97086; Alaska VA Healthcare System, 1201 North Muldoon Road, Anchorage, Alaska 99504.

U.S. DEPARTMENT OF VETERANS AFFAIRS

PHYSICAL SECURITY & RESILIENCY DESIGN MANUAL

October 1, 2020

Revised January 1, 2021

This page is intentionally blank.

PREFACE

It has long been the policy of the U.S. Government to assure the continuity and viability of infrastructure that is critical to the mission of a Federal agency. Laws and regulations applicable to VA include:

Executive Order 12656, issued November 18, 1988, requiring the head of each Federal department and agency to be prepared to respond adequately to all national security emergencies

Public Law 107-188, Public Health Security and Bioterrorism Preparedness and Response Act of 200*2*

Public Law 107-287, Department of Veterans Affairs Emergency Preparedness Act of 2002

38 USC Sec. 901, which 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 properties.

In response, the Department of Veterans Affairs (VA) conducted physical security assessments of 118 VA facilities, which resulted in 24 physical security strategies. The VA Secretary approved the Adoption of Physical Security Strategies for VA Facilities in 2006. Physical security and resiliency design requirements were developed to implement these strategies. This Physical Security and Resiliency Design Manual (PSRDM) supersedes the 2015 Physical Security Design Manuals (PSDM). Recommendations from the 2016 Value Management Study were considered when updating the PSRDM. The PSRDM represents exemplary collaboration across the entire VA.

ACKNOWLEDGEMENTS

The Physical Security and Resiliency Design Manual for the Department of Veterans Affairs is the result of work and input from many departments and individuals. We wish to thank the following for their valuable contributions and support to this Design Manual.

Office of Construction & Facilities Management (CFM)

Lloyd H. Siegel, FAIA	Retired. Former Associate Executive Director, Office of Facilities Planning (OFP)
Donald Myers, AIA	Director, Facilities Standards Service (FSS)
John Bulick, RA	Director, Facilities Planning Development Service (FPDS)
Jay Sztuk, AIA	Retired. Former Director, Cost Estimating Service (CES)
Mark Wiersma, PE	Director, Consulting Support Service (CSS)
Juan Archilla, PE	Structural Engineer, FSS
Thomas Biery, PE	Retired. Former Mechanical Engineer, CSS
Ken Carrico, AIA	Director, Project Control Service
Fei (Linda) Chan, AIA	Planner/Architect, FPDS
Jihaad Davenport, EIT AVS	Value Management Coordinator, CES
Gary Fischer, AIA	Senior Healthcare Architect, FSS
Asok Ghosh, PE, PhD	Structural Engineer, CSS
Ronald Johnson	Architect/Specifications Writer, FSS
Michael Koch	Architect, CSS
Fred Lau, PE	Structural Engineer, FSS
Larry Lau, PE	Electrical Engineer, CSS
Mahmut Nazli, PE	Mechanical Engineer, FSS
Christine Rai	Leasing Team Lead, Office of Real Property (ORP)
Dennis Sheils	Retired. Former Deputy Director, FPDS
Matthew Shepardson	Management Analyst, FPDS
Michael Taylor, PE	Mechanical Engineer, FSS
Bryan Unger, PE	Structural Engineer, FSS
Lam Vu, PE	Electrical Engineer, FSS

Veterans Health Administration (VHA)

Edward A. Litvin, PE, CHFM	Deputy to Assistant Deputy Under Secretary for Health Operations & Administration
Jeffery C. Belczak	VISN 2 Fire Protection and Safety Engineer
Peter Brewster	Emergency Management Specialist, Office of Emergency Management
Troy Brown	VHA Senior Security Specialist

Randall B. Dell, MSSI, CAAMA	Acting Director, Office of Emergency Management (OEM)
James Johnson	Retired. Former Capital Program Consultant, OCAMES
David Klein, PE	Deputy Director and Fire Protection Program Manager, Office of Occupational Safety, Health, and GEMS Programs
Oleh Kowalskyj, MSCE, CHFM, CCS	Deputy Director for Healthcare Engineering, Office of Healthcare Engineering, Healthcare Environment and Facilities Programs (HEFP)
Gary Krupa, PE	Retired. Former Senior Electrical Engineer, Office of Healthcare Engineering, HEFP
Peter Larrimer, PE	Fire Protection Operations Manager, Office of Occupational Safety, Health, and GEMS Programs
Dennis Olson	EMCAP Program Manager, OEM
Paul Phillips	VISN 20 Emergency Manager/Capital Support
Abid Rahman, MD	Associate Director for Program Coordination, OEM
Vincent Rizzo, PE	Compliance Engineer, Office of Healthcare Engineering, HEFP
David Sine, DrBE, CSP, ARM, CPHRM	Chief Risk Officer, Office of Quality, Safety, and Value
Kevin Thompson	Field Program Manager, OEM
Don Wainwright, FACHE	Retired. Former Compliance Engineer, Office of Healthcare Engineering, HEFP

Veterans Benefits Administration (VBA)

John Green	Assistant Director, Emergency Preparedness, Safety, Security and Watch Officers Division
Saeed Noorbakhsh	Architect/Senior Project Manager

National Cemetery Administration (NCA)

Michael Roth	Director, Design and Construction Service
Peggy Jensen	Project Manager, Design and Construction Service
Glenn Madderom	Chief, Cemetery Development & Improvement Service

Office of Information and Technology (OIT)

David Cheplick	Director, Wide Area Network, IT Operations and Services
Kelly Bates, DCIE, CPMM	Data Center & Infrastructure Engineer, Solution Delivery, Data Center & Infrastructure Engineering

Kevin Grzelka, CTIA, CISSP	Data Center & Infrastructure Engineer, Solution Delivery, Data Center & Infrastructure Engineering
John Wernau, DCIE	Data Center & Infrastructure Engineer, Solution Delivery, Data Center & Infrastructure Engineering
Michael Julian, RCDD	Data Center & Infrastructure Engineer, Solution Delivery, Data Center & Infrastructure Engineering
Curtis Derbigny	Data Center & Infrastructure Engineer, Solution Delivery, Data Center & Infrastructure Engineering
Matthew Hammaker	TVE Project Manager, IT Operations and Services

Office of Management (OM)

Nikki Zook	Management Analyst, Office of Asset Enterprise Management

Office of Operations, Security, and Preparedness (OSP)

Darryl G. Blackwell	Division Chief, Policy and Infrastructure Protection Division, Office of Security and Law Enforcement
Keith Frost	Retired. Former Chief, Policy and Infrastructure Protection Division, Office of Security and Law Enforcement
Joel Andrews	Security Specialist
Larry Casserly	PACS-Program Manager
Forrest Frakes, GCL, CET, PC	Acting Chief, Special Systems
Hector Marcayda	Deputy HSPD-12 Program Manager
John Robertson	Program Analyst
Keith Van Bakel	Telecommunications Specialist

National Institute of Building Sciences (NIBS) Project Team

Michael Chipley, PhD, GICSP, PMP, LEED AP	President, The PMC Group, LLC
Theodore C. Moeller, PE, LEED AP	Director of Electrical & Technology Engineering, GLHN Architects & Engineers, Inc
Terrence P. Ryan, CPP	President, TRyan AT/FP LLC
Tom O. Sachs, AIA	Director of Architectural Services, OKKS Studios, a subsidiary of Delta Engineers, Architects & Land Surveyors, PC,
Kenneth Schram, PE LEED AP	Principal-in-Charge Mechanical Engineer, Plumbing/Fire Protection Engineer, Syska Hennessy Group
Robert Smilowitz, PhD, PE	Principal, Thornton Tomasetti, Weidlinger Protective Design Practice

Peggy Van Eepoel, PE	Associate Principal, Thornton Tomasetti, Weidlinger Protective Design Practice
Nanne Davis Eliot, AIA, NCARB, PMP	Esquire, Program Director, National Institute of Building Sciences

TABLE OF CONTENTS

1 INTRODUCTION 1-1

1.1 Scope, Purpose, and Goals 1-1

1.2 Authority 1-2

1.3 Administration and Enforcement 1-3

1.4 VA Facilities 1-4

1.5 Planning, Budgeting, and Programming for Physical Security and Resiliency 1-20

1.6 Introduction to Physical Security and Resiliency Concepts 1-22

1.7 Coordination and Prioritization of Physical Security and Resiliency Requirements with Other Documents 1-23

1.8 Requirements for Subject Matter Specialists 1-23

1.9 Information Safeguarding and Dissemination Controls 1-24

2 GUIDANCE ON USING THE PHYSICAL SECURITY AND RESILIENCY DESIGN MANUAL 2-1

2.1 Scope, Purpose, and Goals 2-1

2.2 Risk Assessment of VA Facilities 2-3

2.3 Exceptions and Deviations 2-7

2.4 Application of Requirements in Common Project Scopes 2-9

3 SITE CONSIDERATIONS 3-1

3.1 Scope, Purpose, and Goals 3-1

3.2 Crime Prevention through Environmental Design (CPTED) 3-1

3.3 Standoff Distance 3-2

3.4 Perimeter Barrier 3-3

3.5 Vehicle and Pedestrian Screening 3-5

3.6 Anti-Ram Rated Vehicle Barriers 3-7

3.7 Parking 3-8

3.8 Site Lighting 3-12

3.9 Landscaping 3-14

3.10 Signage 3-15

4 BUILDING ENTRANCES AND EXITS 4-1
4.1 Scope, Purpose, and Goals 4-1
4.2 Public Entrances and Lobbies 4-2
4.3 Patient Drop-offs 4-7
4.4 Building Exits and Life Safety Considerations 4-8
5 FUNCTIONAL AREAS 5-1
5.1 Agent Cashier 5-1
5.2 Caches: All-Hazards Emergency Cache and Pharmacy Cache 5-3
5.3 Childcare/Development Center 5-5
5.4 Computer Room 5-6
5.5 Emergency Department 5-7
5.6 Emergency and/or Standby Generator Room 5-8
5.7 Energy Center/Boiler Plant 5-10
5.8 Fire Command Center (FCC) 5-12
5.9 Incident Command Center 5-12
5.10 Loading Dock and Service Entrances 5-13
5.11 Mailroom 5-17
5.12 Pharmacy 5-20
5.13 Police Operations Room and Holding Room 5-22
5.14 Records Storage and Archives 5-24
5.15 Research Laboratory and Vivarium 5-25
5.16 Security Control Center 5-29
5.17 Storage of Hazardous Materials 5-35
6 BUILDING ENVELOPE 6-1
6.1 Scope, Purpose, and Goals 6-1
6.2 Non-Load Bearing Exterior Walls 6-3
6.3 Fenestration and Doors 6-4
6.4 Atria 6-8
6.5 Roofs 6-9
6.6 Critical Equipment Protection 6-11

6.7 Calculation Methods and Documentation 6-12
7 STRUCTURAL SYSTEM 7-1
7.1 Scope, Purpose, and Goals 7-1
7.2 Blast Resistance 7-3
7.3 Design for Global Stability of the Structure 7-8
7.4 Prevention of Progressive Collapse 7-9
7.5 Anti-Ram Resistance 7-10
7.6 Calculation Methods 7-11
8 UTILITIES AND BUILDING SERVICES 8-1
8.1 Scope, Purpose, and Goals 8-1
8.2 Utility Entrances 8-2
8.3 Site Distribution 8-5
8.4 Energy Center 8-6
8.5 Water and Fuel Storage 8-7
8.6 Protection of Equipment 8-14
9 BUILDING SYSTEMS 9-1
9.1 Scope, Purpose, and Goals 9-1
9.2 HVAC Systems 9-2
9.3 Electrical Systems 9-4
9.4 Telecommunications Systems 9-5
9.5 Plumbing Systems 9-9
9.6 Fire Protection Systems 9-9
10 SECURITY SYSTEMS 10-1
10.1 Scope, Purpose, and Goals 10-1
10.2 Coordination with Telecommunication and Other Systems 10-5
10.3 Electronic Security Systems 10-12
10.4 Physical Access Control System/Electronic Access and Door Control 10-14
10.5 Intrusion Detection System 10-16
10.6 Security Surveillance Television 10-19
10.7 Duress, Security Phones, and Intercom System 10-26

10.8 Public Address/Mass Notification System 10-31

10.9 Security Control Center, Integrated Operations Center, Emergency Operations Center 10-32

10.10 Patient or Staff Annunciator/Locator (PAL) 10-33

10.11 Behavioral Health Area (Psychiatric or Mental Health Area) 10-34

10.12 Narcotics Storage Alerting and Signal System 10-34

10.13 Detection and Screening Systems 10-35

11 GLOSSARY & ACRONYMS 11-1

12 REFERENCES 12-1

13 APPENDIX

A1 VA Standard Security Door Types

A2 Security Door Opening Schedule

A3 Door Opening Matrix

B Security System Matrix

1 INTRODUCTION

1.1 Scope, Purpose, and Goals

This manual contains the baseline physical security and resiliency requirements for improving the protection of Mission Critical (MC) Facilities, Life-Safety Protected (LSP) Facilities, and LSP Facilities with MC Utilities/Systems Redundancies of the U.S. Department of Veterans Affairs (VA). This updated manual has been retitled the *Physical Security and Resiliency Design Manual* (PSRDM). The physical security and resiliency design and construction requirements in this manual apply to new buildings, additions, and alteration/renovation of existing facilities and/or sites, owned by VA.

MC Facilities are those intended to remain fully functional during and following a natural or manmade extreme event or a national emergency. LSP Facilities are those intended to protect the life safety of the VA patients, staff, and visitors in case of an emergency. Although indispensable to the mission of VA, LSP facilities are not required to remain operational during and following a natural or manmade extreme event or a national emergency. LSP Facilities with MC Utilities/Systems Redundancies are those intended to remain functional with minor repairs, in addition to protecting the life safety of occupants. These facilities are listed in section 1.4 of this chapter.

The previous edition (2015) of the *Physical Security Design Manual* (PSDM) provided in two separate volumes the requirements for MC facilities and LSP facilities. This manual provides the physical security and resiliency requirements for VA facilities in one volume and now provides direction on the application of the requirements for various project scopes (see Section 2.4). The requirements of this manual must 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 planning, design, and construction for physical security and resiliency. The requirements also must be coordinated with the requirements of the *Life Safety Code,* NFPA 101; the PSRDM does not supersede any life-safety requirements, standards, or codes that have been recognized by VA.

The physical security and resiliency requirements in this manual account for VA operations and policies and balance cost with effectiveness. 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 and resiliency to support VA services and facilities.

This introductory section provides the general information on how physical security and resiliency requirements are to be applied by the VA facility director and the planner, designer, architect, engineer, and project manager, with the goal of improved decision-making during the project planning phase, which follows the Strategic Capital Investment Process (SCIP) and

precedes the Department's budget request to Congress. Chapter 2 of this manual provides direction on the use of this manual, specifically on risk and vulnerability assessments (section 2.2) and applicable requirements for common project scopes (section 2.4). Later chapters provide complete descriptions of the physical security and resiliency requirements by discipline. The requirements for new buildings and additions are listed under each section, while the specific or applicable requirements for alteration/renovation of existing facilities are listed at the end of each section within a gray text box.

Physical security and resiliency requirements are not the same as cybersecurity requirements. Chapter 10 includes cybersecurity requirements only where needed to support physical security and resiliency, and to maintain operation of VA facilities. The PSRDM supports cybersecurity and has been coordinated with required physical security systems as outlined in the 2016 VA Telecommunications Design Manual; therefore, Appendix B of this manual has been modified to address separation of networks as well as protection of IT assets.

Additional resiliency requirements for VA facilities are covered in other VA design guides and criteria and must be coordinated with the PSRDM requirements. A primary goal of the PSRDM is to support the resiliency of all VA facilities following a natural or manmade extreme event or a national emergency; therefore, included in this manual are resiliency requirements in support of continuity of operation of VA facilities. For MC facilities and LSP facilities with MC utilities/systems redundancies, resiliency requirements must support continued operations for a minimum of 96 hours during and following an extreme event.

1.2 Authority

It has long been the policy of the U.S. Government to assure the continuity and viability of infrastructure that is critical to the mission of a Federal agency. Executive Order 12656, issued November 18, 1988, states, "The head of each Federal department and agency must be prepared to respond adequately to all national security emergencies." Furthermore, the "head of each Federal department and agency must 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 must: 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 must 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.

1.3 Administration and Enforcement

The physical security and resiliency requirements in this manual apply to all design and construction projects for new facilities, and renovation/alteration of existing facilities. These projects include but are not limited to projects in VA's Major, Minor and Non-Recurring Maintenance (NRM) construction programs, for which design is begun on or after the effective date of this design manual.

All projects in VA's Major Construction Program that are in design at the effective date of the manual but have not concluded the 35-percent design milestone (defined as Schematic Design or SD2) must incorporate the requirements of this manual. For Major projects that have reached the 35-percent design milestone, they are required to be in compliance with the edition of this manual effective at the time OR the current version, at the discretion of the Project Delivery Team.

Table 1-1 Authority Having Jurisdiction (AHJ) for Physical Security and Resiliency Requirements

VHA	VBA	NCA
Assistant Under Secretary for Health for Support Services	Executive Director for Office of Administration and Facilities	Under Secretary for Memorial Affairs

Deviations from the baseline requirements in this manual must be supported by a risk assessment of both the site and facility during the planning phase of the project before the development of project scope and budget. Requests for deviation must be submitted to the AHJ overseeing the implementation of physical security and resiliency requirements for the facility for review. When no risk assessment is performed during the project planning phase, the baseline requirements of this manual must apply. The processes for submitting requests for deviations from the baseline requirements are described in section 2.3 Exceptions and Deviations.

1.4 VA Facilities

1.4.1 Physical Security and Resiliency Designations for VA Facilities:

This section lists the VA facilities according to the following physical security and resiliency designations:

- MC Facilities
- LSP Facilities w/ MC Utilities/Systems Redundancies
- LSP Facilities
- Facilities w/ Varying Designations
- Exempt Facilities

1.4.1.1 MC Facilities: These facilities are intended to remain fully functional with little to no damage to impede operations during and following a natural or manmade extreme event or a national emergency. Type V construction (specifically light-frame wood and cold-formed steel framing structure) is not permitted for MC facilities.

Table 1-2 MC Facilities
Acute Care [Acute Beds] - inpatient medical/surgical beds

Table 1-2 MC Facilities
Acute Care [Acute Beds] - outpatient[1]
Drug/Alcohol Rehabilitation - inpatient
Emergency Command Center
Fire Station, Police Station
Hazardous Material Storage
Hospital
Imaging Center – inpatient
Medical Records - standalone central storage
Mental Health/Psychiatric Care - Inpatient
National Continuity of Operation Center
OIT - Core Data Center (CDC)
Polytrauma – inpatient
Research - Animal Facility
Research Facility w/ Wet Labs
Security & Law Enforcement

Notes:

1) Includes urgent care (not 24/7) and Emergency Department.

1.4.1.2 LSP Facilities with MC Utilities/Systems Redundancies: These facilities are intended to protect the life safety of the VA patients, staff, and visitors in case of an emergency, and to remain functional during and following a natural or manmade extreme event or a national emergency, with minor repairs. In addition to complying

with requirements of LSP facilities, MC Utilities and Systems Redundancies must be provided in accordance with Chapters 8 and 9 of this manual.

Table 1-3 LSP Facilities with MC Utilities/Systems Redundancies
Community Living Center (CLC) (LTC, ECRC, ECU)
Dietetics (serving inpatient/food production)[1]
Domiciliary/MH RRTP
Imaging Center - outpatient

Notes:

1) The purpose of the facility is serving inpatient and food production, not administrative office space.

1.4.1.3 LSP Facilities: These facilities are intended to protect the life safety of the VA patients, staff, and visitors in case of an emergency. Although indispensable to the mission of VA, LSP facilities are not required to remain operational during and following a natural or manmade extreme event or a national emergency.

Table 1-4 LSP Facilities
Canteen-Retail Store
Chapel (standalone building)
Child Care
Credit Union
Drug/Alcohol Rehabilitation – outpatient
Library/Museum
Maintenance Facility (Shops)
Mental Health/Psychiatric Care - Outpatient

Table 1-4 LSP Facilities
Office (e.g., Clinical Administrative, General Administrative, etc.)
OIT - National Call Center
OIT - Network Support Center (NSC)
Outbuilding (General Use)
Polytrauma - outpatient
Post Office
Quarters (Residential)
Recreational
Rehabilitation Medicine - outpatient
Research Facility w/ Dry Labs only
Spinal Cord Injury/Disorders Center (SCID Center) - outpatient
Student Housing
Training, Education
Veterans Services
Waste Management (incinerator & Recycle)

1.4.1.4 Facilities with Varying Designations: The physical security and resiliency designations for these facilities can range from LSP to MC. The determination of the

designations depends on the services provided in these facilities, or the designation of the primary facilities supported by these facilities.

Table 1-5 Facilities with/Varying Designations

Facilities	Possible Designations			Notes
	MC	LSP w/MC Utilities/ Systems Redundancies	LSP	
Ambulatory Surgery Center (ASC)	X	X	X	Default designation is MC. Request to lower the designation can be submitted for review/approval when there is identified alternate VA site of care.
Auditorium	-	X	X	Default designation is LSP. Follow Designation of the primary facility that it supports up to LSP w/Utility/System Redundancy. When the auditorium/facility, with public assembly as primary occupancy and with an occupant load greater than 300, upgrade to LSP w/MC Utilities/Systems Redundancies.
Biomedical Eng. (equip. & wheelchair repair)	-	X	X	Default designation is LSP. Follow Designation of the facility that it supports, up to LSP w/MC Utilities/Systems Redundancies.
Canteen-Cafeteria	-	X	X	Default designation is LSP. Follow Designation of the facility that it supports, up to LSP w/MC Utilities/Systems Redundancies.

Facilities	Possible Designations			Notes
	MC	LSP w/MC Utilities/ Systems Redundancies	LSP	
Central Energy/Utility Plant (including chiller and boiler plants)	X	X	X	To be designed to the same level as the highest buildings the Plant serves
Connecting corridor concourses and bridges	X	X	X	Designation and requirements to be determined by the AHJ on a case-by-case basis. [Considerations include but not limited to: exemption from requirements of chapters 3, 6, and 7 when they are not the main entrance or required exit for the connected buildings; follow MC requirements if critical utilities are located inside along the corridor/bridge.]
Consolidated Mail-Out Pharmacy (CMOP)	X	X	-	Default designation is LSP w/MC Utilities/Systems Redundancies. Designation can be upgraded to MC when the need arises. There are a limited number of CMOPs that cannot be duplicated for handling of controlled substances.
Emergency Generator	X	X	X	To be designed to the same level as the highest buildings the Generator serves

Facilities	Possible Designations			Notes
	MC	LSP w/MC Utilities/ Systems Redundancies	LSP	
Laundry	-	X	X	Default designation is LSP. Consider upgrading to LSP w/MC Utilities/Systems Redundancies based on factors such as regional workload, likelihood of natural disasters/hazards, and community availability of laundry services. Such upgrade can be determined at the VAMC & VISN level without additional approval from VHA-VACO or CFM.
Medical Equipment Storage	X	X	X	To be designed to the same level as the highest buildings the Medical Equipment Storage serves
Medical Gas Storage	X	X	X	To be designed to the same level as the highest buildings the Medical Gas Storage serves
Medical Records Storage	X	X	X	Medical Records Storage areas that are not standalone central storage facilities shall match the building designation of the most critical function of the building they are within.
OIT - Campus Support Center (CSC)	X	X	-	Follow designation of the highest level of a supported entity on the campus.

Facilities	Possible Designations			Notes
	MC	LSP w/MC Utilities/ Systems Redundancies	LSP	
OIT - Mission Support Center (MSC)	X	X	-	Default designation is LSP w/MC Utilities/Systems Redundancies. To be elevated to MC when supporting mission-critical production environment that directly supports patient care.
Outpatient Care (including Ambulatory Care, OPC, CBOC, HCC, multi-specialty, primary care, etc.)	X	X	X	Default designation is LSP. Refer to the list of VHA Strategic Planning Categories (Table 1-7) for determination of Designation. If the designation is raised due to services provided, request to lower the designation can be submitted for review/approval when there is identified alternate VA site of care.
Rehabilitation Medicine - Inpatient (Blind, PT/OT)	X	X	-	To be designed to the same level as the highest building the facility serves (e.g., hospital, CLC, etc.)
Spinal Cord Injury/Disorders Center (SCID Center) - inpatient	X	X	-	To be designed to MC level for Acute and LSP w/MC Utilities/Systems Redundancies for long-term. To be designed to the same level as the highest building the facility serves (e.g., acute, CLC, etc.)
Sterile Processing Service	X	X	X	To be designed to the same level as the highest buildings the Sterile Processing Service serves

Facilities	Possible Designations			Notes
	MC	LSP w/MC Utilities/ Systems Redundancies	LSP	
Temporary Buildings	X	X	X	Physical security requirements to be determined by AHJ on a case-by-case basis.
Warehouse		X	X	Default designation is LSP. Designation must be upgraded to LSP w/ MC Utilities/Systems Redundancies when storage includes caches (all-hazards emergency cache, pharmacy cache), controlled and sensitive material/substances deemed critical to continuity of operation.
Water Tower, Utility Supply Storage Structure or structures supporting utilities	X	X	X	To be designed to the same level as the highest buildings the structure serves

1.4.1.5 Exempt Facilities: These facilities are exempt from the requirements of this manual.

Table 1-6 Exempt Facilities
Accessory Non-Building Structure
Fisher House with 24 or fewer units
Greenhouse (Freestanding)

Table 1-6 Exempt Facilities
Maintenance Storage (Non-biomedical Equipment)
Miscellaneous structure/facility not otherwise identified
Parking Garage
Non-occupied structures (including flagpoles)
Sheds and relocatable buildings
Toilets (Outhouse)
Waste Storage (Non-hazardous)

1.4.1.6 VHA Strategic Planning Categories / Designations: Table 1-7 provides the designations based on the services listed in the VHA Strategic Planning Categories:

Table 1-7 VHA Strategic Planning Categories/Designations:

VHA Strategic Planning Categories	Physical Security & Resiliency Designations		
	MC	LSP w/MC Utilities/Systems Redundancies	LSP
Amb Medical: Audiology and Speech			x
Amb Medical: Cardiology			x
Amb Medical: Dialysis	x		
Amb Medical: Digestive/GI/Endoscopy - Office Visit			x
Amb Medical: Digestive/GI/Endoscopy - Procedure		x	
Amb Medical: EEG/Neurology			x

VHA Strategic Planning Categories	Physical Security & Resiliency Designations		
	MC	LSP w/MC Utilities/Systems Redundancies	LSP
Amb Medical: Endocrine/Metabolic and Diabetes			x
Amb Medical: NonSurg: All Other			x
Amb Medical: NonSurg: Allergy & Immunology			x
Amb Medical: NonSurg: Dermatology			x
Amb Medical: NonSurg: Infectious Diseases			x
Amb Medical: NonSurg: Nephrology			x
Amb Medical: NonSurg: Rheumatology			x
Amb Medical: Oncology - Office Visit			x
Amb Medical: Oncology - Procedure		x	
Amb Medical: Pulmonary/Resp Care			x
Amb Medical: Rehab Medicine			x
Amb Mental Hlth: Homeless			x
Amb Mental Hlth: Intensive Community Mental Health Recovery Services (ICMHR)			x
Amb Mental Hlth: Mental Health Clinic - All Others			x
Amb Mental Hlth: Mental Health Clinic - Psychotherapy			x
Amb Mental Hlth: MH RRTP Outpatient			x
Amb Mental Hlth: MH RRTP Residential Stay		x	
Amb Mental Hlth: Psychology Clinic - All Others			x

VHA Strategic Planning Categories	Physical Security & Resiliency Designations		
	MC	LSP w/MC Utilities/Systems Redundancies	LSP
Amb Mental Hlth: Psychology Clinic - Psychotherapy			x
Amb Mental Hlth: Substance Abuse Clinic			x
Amb Mental Hlth: Work Therapy			x
Amb Surg: Cardiovascular and Thoracic Surgery	x		
Amb Surg: Colon Rectal Surgery	x		
Amb Surg: ENT	x		
Amb Surg: General and All Other Surgery	x		
Amb Surg: Neurological Surgery	x		
Amb Surg: Obstetrics & Gynecology	x		
Amb Surg: Plastic Surgery	x		
Amb Surg: Urology	x		
Amb Surg: Eye Clinic	x		
Amb Surg: Orthopedics	x		
Amb Surg: Podiatry	x		
Amb: Dental - Basic			x
Amb: Dental - Major	x		
Amb: Dental - Minor			x

VHA Strategic Planning Categories	Physical Security & Resiliency Designations		
	MC	LSP w/MC Utilities/Systems Redundancies	LSP
Amb: Geriatrics			x
Amb: Laboratory and Pathology		x	
Amb: Nuclear Medicine		x	
Amb: Primary Care			x
Amb: Radiation Therapy			x
Amb: Radiology *Note: Default designation is LSP. The designation can be upgraded to match the designation of the supported facility(s)/function(s).*			x
Amb: Recreational Therapy			x
Amb: Urgent Care	x		
Blind Rehab - inpatient		x	
Blind Rehab - outpatient			x
CLC - Long		x	
CLC - Short		x	
Home Hospice Care (Administrative Program)			x
Home Respite Care (Administrative Program)			x
Home Telehealth			x
Home-Based Primary Care			x
Homemaker/Home Health Aide Programs			x

VHA Strategic Planning Categories	Physical Security & Resiliency Designations		
	MC	LSP w/MC Utilities/Systems Redundancies	LSP
Inpt Mental Hlth: General Compensated Work Therapy/Transitional Residence (Gen CWT/TR)		x	
Inpt Mental Hlth: PRRP, PRRTP, SARRTP & Dom		x	
Inpt Mental Hlth: Sustained Treatment and Rehab (STAR I II III)	x		
Inpt: Maternity Deliveries	x		
Inpt: Maternity Non-Deliveries	x		
Inpt: Medical	x		
Inpt: Observation Beds (47 hour)	x		
Inpt: Psychiatric	x		
Inpt: Substance Abuse	x		
Inpt: Surgical	x		
Psychosocial Rehabilitation and Recovery Center			x
Purchased Skilled Home Care			x
SCI&D Home Care			x
Spinal Cord Injury - outpatient			x
Spinal Cord Injury Centers - inpatient	x		
VA Adult Day Health Care			x

1.4.1.7 Other Considerations: This section addresses several specific building types and elements.

Low-occupancy housing with 12 occupants or fewer per building are exempt from the requirements of chapters 3, 6, and 7.

Physical security and resiliency requirements for temporary buildings must be determined on a case-by-case basis by the AHJ for overseeing implementation of physical security and resiliency requirements for the facility.

Buildings of type V construction (specifically light-frame wood or cold-formed steel framing structure) are exempt from specific blast-resistant design requirements for the Building Envelope and the Structural System. See Chapters 6 and 7, and Chapter 1 Annex for additional information.

1.4.2 Veterans Health Administration Criteria for Facilities and Services

The default physical security and resiliency designations are provided for various VHA facilities in section 1.4.1; however, there can be situations where these default designations may not be appropriate due to the site conditions, size, location, or other factors of the specific project. A request to deviate from the default designation (such as, from MC to LSP, or vice versa) may be made using the process to request deviation from baseline requirements as described in section 2.3 Exceptions and Deviations.

When the VHA facility or service ***provides direct patient care***, any deviation from the default designations (MC or LSP) must be based, at a minimum, on the patient care space and risk categories of NFPA 99, *Healthcare Facilities Code*, when applicable to the services provided in the facility. For reference, an excerpt of NFPA 99 may be found in the Chapter 1 Annex; however, NFPA 99 be reviewed and complied with in full. A risk assessment considering the respective patient care/risk category must be included in the request for deviation to lower the designation of a VHA facility or service. See Chapter 1 Annex for additional information.

1.4.3 Veterans Benefit Administration Criteria for Facilities and Services

The default physical security and resiliency designation for VBA facilities and services are LSP. For VBA leased facilities, including build-to-suit, new construction, and lease in an existing facility; see section 1.4.6 VA Leased Facilities.

1.4.4 National Cemetery Administration Criteria for Facilities and Services

National Cemeteries include facilities, both enclosed and open-air structures, and utilities. While physical security and resiliency of NCA facilities and utilities is important, their unique nature and functions make many physical security and resiliency requirements less likely to be applicable in cemeteries than in VHA or VBA facilities. Table 1-2 lists the applicable

requirements for each NCA facility type. Request for exceptions can be made in accordance with section 2.3 Exceptions and Deviations.

Table 1-8 National Cemetery Administration Criteria and Requirements

NCA Facility Type / Service	PSRDM Applicable Requirements	Notes
Administration buildings: • Visitor information • Public restrooms	Section 3.2 Standoff Distance Section 3.6.2.1 Parking Section 6.3.1.1 Glass Chapter 10 Security Systems Appx A1-A3 Security Door Types Appx B Security System Application Matrix	Section 3.6.2.1 does not apply to NCA staff parking. Sufficient lighting must be provided for the operation of security systems in accordance with section 3.8 Site Lighting; such lighting must be mounted on the building exterior (not on poles or fences).
Lodges: • Residential • Non-residential	Chapter 10 Security Systems Appx A1-A3 Security Door Types Appx B Security System Application Matrix	None
Maintenance buildings: • Employee buildings • Workshops • Storage for vehicles and equipment	Chapter 10 Security Systems Appx A1-A3 Security Door Types Appx B Security System Application Matrix	Provide security fencing to maintenance yard adjacent to maintenance buildings. Sufficient lighting must be provided for the operation of security systems in accordance with section 3.8 Site Lighting. Such lighting must be mounted on the building exterior (not on poles or fences).
Columbarium: • Walls and courts • Open-air structure	None	None
Committal shelter: • roofed, open at sides • storage closet • open-air structure	None	None
Water supply: • systems • pump stations • deep wells • reservoirs	Chapter 10 Security Systems Appx B Security System Application Matrix	Provide security fencing to control access.
Fuel supply: • stations • tanks	Chapter 10 Security Systems Appx B Security System Application Matrix	Provide security fencing to control access.

NCA Facility Type / Service	PSRDM Applicable Requirements	Notes
Site	Section 3.3 Perimeter Barrier	Where site conditions allow: perimeter or boundary fencing beyond the entrance area is preferred but is a site-specific decision for NCA; the entire cemetery of hundreds of acres may not be fenced when it is first established but incrementally as it is developed.

NOTE: All relevant requirements of Appendix A are listed in the National Cemetery Administration section of that appendix; relevant requirements of Appendix B are listed under Cemetery in that appendix.

1.4.5 VA Owned Facilities

All facilities that are owned and operated by VA must follow the requirements of this manual. These baseline physical security and resiliency requirements apply to new buildings, additions, and existing facilities undergoing renovations and alterations. Table 2-1 Project Scopes/Requirements provides direction in the applicability of requirements for a wide range of project scopes.

1.4.6 VA Leased Facilities

The implementation of physical security for leased facilities is to comply with the Interagency Security Committee (ISC) Risk Management Process. Leased facilities are not required to comply with physical security and resiliency requirements in this manual. For further information, please contact the Office of Real Property within the Office of Construction & Facilities Management.

1.5 Planning, Budgeting, and Programming for Physical Security and Resiliency

When establishing a design and a budget for a MC or LSP project, it is essential that physical security and resiliency are fully integrated into the program, rather than being an added requirement. When physical security and resiliency are treated as add-ons to an otherwise complete project, the costs for implementation will be significantly higher and/or the results less effective. As such, it is essential to establish the physical security and resiliency goals within the capital investment project application phase of the project and to ensure that the budget is set to reflect the physical security and resiliency requirements within the program goals.

1.5.1 Planning for Physical Security and Resiliency

Physical Security and resiliency must be incorporated in the Facility Master Plan (or equal) conducted by each VA facility. VHA conducts a Hazard Vulnerability Assessment (HVA) on all facilities; VBA risk assessments are completed by Office of Administration and Facilities Physical Security Specialist and VA Police; NCA risk assessments are conducted by the VA Police. The findings of risk and vulnerability assessments, prepared by the VA Police, Emergency Management Committee (EMC), or other, must be incorporated into the FMP.

Physical security and resiliency planning within the FMP is required to implement the standards of this manual. See Chapter 2 for the objectives and details of physical security and resiliency planning, risk analysis, and hazard vulnerability assessment.

1.5.2 Risk Assessment of VA Facilities

The risk assessment, mission impact assessment, and evaluation of the physical security and resiliency requirements for each project must be performed by qualified professional specialists/subject matter experts. Mission impact assessments are required to inform facilities/Veterans Integrated Service Networks (VISN) when utility redundancies are needed in direct support of continued operations of facilities. Chapter 2 provides direction on the use and coordination of risk assessment and other vulnerability assessments with physical security and resiliency requirements for a specific project.

It is not possible to eliminate all risk to a facility, and projects may face resource limitations. Cost effective risk management is a requirement of every project; therefore, physical security and resiliency must be fully integrated into the program from inception. Lack of funding alone is not the cause to neglect complying with any physical security and resiliency requirements.

During the planning phase of a new facility or alterations/renovations of an existing facility, the existing VA assessment programs and tools[1] must be used to inform security planning and risk assessment. Security planning begins with a risk assessment to determine project- or site-specific requirements or the need for modifications to the baseline physical security and resiliency design requirements due to unique project conditions. The risk assessment is to be conducted during the project planning stage, and its outcome must be incorporated into the development of project scope and budget.

1.5.3 Value Management of Baseline PSRDM Requirements

A Value Management (VM) study was conducted for the 2015 Physical Security Design Manual (PSDM) in early 2016. The goal of the VM study was to identify the most lifecycle cost effective

[1] These include the VA Police assessment, VHA Hazard Vulnerability Assessment (HVA), Comprehensive Emergency Management Plan (CEMP, Facility Master Plan (FMP), and other risk or security evaluations.

means of achieving physical security and resiliency for VA facilities. Through function and risk analysis, the VM study validated requirements and strategies to identify alternatives that would achieve the highest possible benefit to cost ratio.

Having vetted the physical security and resiliency requirements in the VM study and during the PSRDM update process, many cost-benefit concerns will not need to be revisited in future project-specific VM studies.

1.6 Introduction to Physical Security and Resiliency Concepts

1.6.1 Crime Prevention through Environmental Design

VA follows the principles of Crime Prevention through Environmental Design (CPTED, see www.cpted.net). CPTED strategies include elements of natural surveillance, natural access control, and natural territorial reinforcement. CPTED promotes the principles that proper design and effective use of the built environment can discourage, reduce, or remove potential crime risks. CPTED must be used to evaluate VA site and building designs to create and enhance the concentric circles or layers of security protection. CPTED is covered in more detail in Chapter 3.

1.6.2 Facilities in Floodplains

As directed by Executive Order (EO) 11988, agencies must adhere to local floodplain regulations, which may be more stringent than Federal regulations. 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 https://www.fema.gov/national-flood-insurance-program/flood-map-information. No new facilities shall be constructed in the 100-year flood plain. Data from recent floods and storms, as well as available future projections, must be evaluated for implementation of flood mitigation measures at the facilities.

1.6.3 Security Operations Requirements

Design decisions for the physical security of VA facilities must be based on the concentric levels of control and protection — both physical and operational — as further described in the Annex to Chapter 3.

Directions on operational procedures can be found in VA Handbook 0730 and are not a part of the PSRDM. The physical security systems are designed to support the operational plan; for example, a mass notification system supports Emergency Operations such as evacuation operations.

1.7 Coordination and Prioritization of Physical Security and Resiliency Requirements with Other Documents

Coordination with other VA documents is required. As VA updates the physical security and resiliency requirements in the PSRDM, it is imperative that VA criteria, standards, specifications, and others be coordinated with the new requirements. The A/E designer of record for a VA project must incorporate the requirements of the PSRDM into the specifications and construction documents for the project. Users of this manual must familiarize themselves with the most current documents on the VA CFM Technical Information Library (TIL) at https://www.cfm.va.gov/til/.

Physical security and resiliency requirements must accommodate environmental and cultural special conditions unique to each site. All construction and renovation/alteration projects at VA facilities must be reviewed during the planning phase to identify and resolve any environmental impacts. VA is to obtain service of qualified profession subject matter expert to conduct the review in accordance with the *National Environmental Policy Act* (NEPA), *National Historic Preservation Act* (NHPA), and related laws and regulations. Where conflicts between physical security or resiliency requirements and special environmental or cultural conditions (including the distinctive qualities of a historic building) are identified, such conflicts must be resolved under NEPA and NHPA, as applicable, in ways that to the extent practicable do not detract from physical security and resiliency objectives.

1.8 Requirements for Subject Matter Specialists

In order to meet the physical security and resiliency requirements of this manual, as appropriate to the scope of the project, the design team must include: (1) a certified physical security specialist with an emphasis on risk and vulnerability assessments, physical security design and CPTED, and anti-terrorism force protection; (2) a control systems cybersecurity specialist with in-depth knowledge of the Risk Management Framework; (3) a certified physical security specialist with an emphasis on Electronic Security Systems; (4) certified information and communications technology (ICT) specialist with an emphasis on networking and cabling; (5) a certified systems integrator specialist with an emphasis on HSPD/PPD-21 integrations; and, (6) a licensed professional structural engineer who has specialized training in blast design and analysis (structural blast specialist).

These specialists must be part of the design team during the concept phase of any project. The résumé of the specialist must be submitted to the VA Project Manager (PM), local facility equivalent, or Contracting Officer Representative for review and approval prior to the concept phase of the project. The qualifications of the firm for whom the specialist works must also be submitted with the résumé. The professional qualifications that all specialists must comply with are found where their respective disciplines are addressed in Chapters 2, 6, 7, and 10 of this manual.

1.9 Information Safeguarding and Dissemination Controls

Executive Order 13556, Controlled Unclassified Information, issued November 4, 2010, establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies.

Information that requires safeguarding or dissemination controls, which may be designated using terms such as Controlled Unclassified Information (CUI), Sensitive But Unclassified (SBU), or For Official Use Only (FOUO), may include items such as design analysis, drawings, CAD and/or Building Information Modeling (BIM) files, studies, and assessments regarding physical security. Such information must be:

- Controlled so that information in electronic and hard copy formats are made available only to individuals who have a legitimate business need to know;
- Safeguarded during use and either properly destroyed or returned to VA after use; and
- Kept from being presented in public forums.

Specific requirements regarding handling of such information must be coordinated with the Contracting Officer or the Project Manager.

Annex to Chapter 1

A-1.4.1.7 Type V Construction

Type V construction may be used where permitted by the International Building Code, The Life Safety Code (NFPA 101), the Guidelines for Design and Construction of Hospitals and Outpatient Facilities, the Guidelines for Design and Construction of Residential Health, Care, and Support Facilities, and the VA Design Guidelines unless the facility or a portion of the facility is classified as Mission Critical (MC). The 2012 edition of the Life Safety Code (LSC) defines an ‘‘Ambulatory Health Care Occupancy’’ as a facility capable of treating 4 or more patients simultaneously on an outpatient basis. Centers for Medicare & Medicaid Services (CMS) regulations at 42 CFR 416.44 require that all ambulatory surgery centers (ASCs) meet the provisions applicable to Ambulatory Health Care Occupancy, regardless of the number of patients served. Hospital outpatient surgical departments are comparable to ASCs and thus should also be required to meet the provisions applicable to Ambulatory Health Care Occupancy Chapters, regardless of the number of patients served.

Buildings that are built as Type V construction (specifically light-frame wood or cold-formed steel framing structure) are exempt from specific the building envelope blast resistant design requirements in Chapter 6 and specific structural requirements in Chapter 7. Refer to these two chapters for further information. The intent is to take advantage of the economies that can be achieved by allowing the use of wood and cold-formed steel framing systems.

A-1.4.2a Systems Critical for the Continuity of Operations of VHA Facilities

The following systems are considered critical for the continuity of operations of the facilities. This alphabetical (not in order of priority) list was established by the VA Critical Hospital Systems and Resiliency Workgroup.

- Building Infrastructure
- Electrical Power
- Fire Protection, Suppression and Alarm Systems
- Fuel Distribution Systems and Fuel Supplies
- Heating, Ventilation and Air Conditioning
- Medical Gases Systems
- Information Technology and Communication
- Security System
- Sewage and Waste Systems
- Transportation

- Water Systems

A-1.4.2b Veterans Health Administration Criteria for Facilities and Services

A-1.4.2b.1 VHA Direct Patient Sites of Care[2] are listed as follows:

1. Inpatient Sites of Care
    a. VA Medical Centers (VAMC)
    b. VA Residential Care Sites (VA Domiciliary or Mental Health RRTPs) (Standalone)
    c. VA Extended Care Sites (Community Living Centers (CLC)) (Standalone)
2. Outpatient Sites of Care
    a. Health Care Centers (HCC)
    b. Multi-Specialty Community Based Outpatient Clinics (CBOC)
    c. Primary Care Community Based Outpatient Clinics (PC CBOC)
    d. Other Outpatient Services (OOS) Sites

A-1.4.2b.2 NFPA 99, *Healthcare Facilities Code,*[3] Applicable Categories: NFPA 99 provides categories for both space and risk in patient care areas, and is excerpted retaining the original NFPA paragraph numbering, in part, below:

> *3.3.136* Patient Care Space. Any space of a health care facility wherein patients are intended to be examined or treated. (FUN)*
> *3.3.136.1* Category 1 Space. Space in which failure of equipment or a system is likely to cause major injury or death of patients, staff, or visitors. (FUN)*
> *3.3.136.2* Category 2 Space. Space in which failure of equipment or a system is likely to cause minor injury to patients, staff, or visitors. (FUN)*
> *3.3.136.3* Category 3 Space. Space in which the failure of equipment or a system is not likely to cause injury to patients, staff, or visitors but can cause discomfort. (FUN)*

[2] VHA Sites of Care Classifications for FY 2016 (VAIQ #7670375), further defined in the Glossary, referencing VHA Site Classifications and Definitions Handbook #1006.02
[3] 2018 edition

3.3.136.4 Category 4 Space. Space in which failure of equipment or a system is not likely to have a physical impact on patient care. (FUN)*
3.3.158 Risk Categories.
3.3.158.1 Category 1. Activities, systems, or equipment whose failure is likely to cause major injury or death to patients, staff, or visitors.
3.3.158.2 Category 2. Activities, systems, or equipment whose failure is likely to cause minor injury to patients, staff, or visitors.
3.3.158.3 Category 3. Activities, systems, or equipment whose failure is not likely to cause injury to patients, staff, or visitors but can cause discomfort.
3.3.158.4 Category 4. Activities, systems, or equipment whose failure would have no impact on patient care.

Based on the NFPA 99 categories, any VA project containing Category 1 space or risk, where "failure is likely to cause major injury or death" must be MC. Spaces and risks which are NFPA 99 Category 2 or 3 must be LSP at a minimum, but may be upgraded to MC. Design and construction of VA-owned Category 4 spaces must comply with LSP requirements; for requirements pertaining to facilities leased by VA, refer to section 1.4.6 VA Leased Facilities.

NFPA 99 Chapter 12 defines Emergency Management Categories 1 and 2 as the following:

Table 12.3 Emergency Management Categories:

Emergency Management Category 1 – Those inpatient facilities that remain operable to provide advanced life support services to injured responders and disaster victims. These facilities manage the existing inpatient load as well as plan for the influx of additional patients as a result of an emergency. (For VHA this constitutes inpatient sites of care).

Emergency Management Category 2 – Those inpatient or outpatient facilities that augment the critical mission. These facilities manage the existing inpatient or outpatient loads but do not plan to receive additional patients as a result of an emergency or do not plan to remain operable should essential utilities or services be lost. (For VHA this constitutes outpatient sites of care).

The designation of each VHA facility, if deviating from the default designation, must be determined by the AHJ during the planning phase of the project. When deviating from the

baseline requirements of the PSRDM, the extent of MC requirements, whether to the facility, service, or entire campus, must also be determined by the AHJ during the planning phase of any project.

2 DIRECTION ON USING THE PHYSICAL SECURITY AND RESILIENCY DESIGN MANUAL

2.1 Scope, Purpose, and Goals

This chapter provides direction to the directors, planners, architects, and engineers on the use and coordination of risk assessment, outcomes from vulnerability assessments conducted by VA Police, facility Emergency Management Committee (EMC), VBA, and NCA, with physical security and resiliency requirements. Both the risk assessment and evaluation of the physical security and resiliency requirements for each project must be performed by qualified professional specialists/subject matter experts. During the risk assessment process, participation and support from VA facility staff with expertise in security management, emergency management, operations, and planning are necessary to ensure site specific conditions and issues are addressed. This chapter provides direction on using a risk assessment to customize physical security and resiliency requirements for a specific project.

The risk assessment identified in this chapter must be used when a reduction or deviation from the baseline requirement(s) or the default designation of this manual is sought or when an alternate means to obtain an equivalent level of resiliency and physical security is desired.

It is not possible to eliminate all risk to a facility, and projects may face resource limitations. Cost effective risk management is a requirement of every project; therefore, physical security and resiliency must be fully integrated into the program from inception. During the project planning phase, a risk assessment can review project- or site-specific conditions and determine the need for deviation from the baseline physical security and resiliency design requirement. The risk assessment must be conducted prior to development of project scope and budget with the outcome incorporated into the project application. During planning for all new projects, the existing VA assessment programs and tools[4] are to be used to inform security planning and risk assessment.

This chapter provides information on conducting a risk assessment, of any VA facility or service, and incorporating information from existing VA assessments and tools. VA Police conduct a vulnerability and risk assessment on every VA facility annually or biannually. VHA uses a Hazard Vulnerability Assessment (HVA); VBA risk assessments are completed by Office of Administration and Facilities Physical Security Specialist and VA Police; there are no comparable assessment tools for NCA. It is important to note there needs to be coordination between the risk assessment and the HVA. Vulnerability is a part of a risk assessment, but an HVA is not a

[4] These include the VA Police assessment, VHA Hazard Vulnerability Assessment (HVA) in accordance with NFPA 99, Chapter 12, 1.5.3, Comprehensive Emergency Management Plan (CEMP, Facility Master Plan (FMP), and other risk or security evaluations.

substitute for a risk assessment. Information from the Police assessment (and the HVA for VHA projects) must be incorporated into each risk assessment

The PSRDM contains the baseline requirements consistent with the identified or perceived risk of crimes against persons and crimes against property as well as natural events (with the exclusion of seismic) at VA facilities. The size, type of facility, vulnerable functions and building systems, and specific threat environment of VA facilities vary significantly. It is recognized that all facilities in all possible situations may not be able to meet all PSRDM requirements. In such cases, the specific PSRDM requirements to be modified or omitted must be determined during project planning stage, using a risk assessment of both the site and facility. Submitted requests for deviations based on the risk assessment will be reviewed by the VA AHJ for overseeing implementation of physical security and resiliency requirements for the facility. See Chapter 2 Annex for additional information.

2.1.1 Physical Security and Resiliency Planning as Part of the Facility Master Plan

As part of the planning phase of new buildings and additions, and for existing facilities undergoing renovations/alteration, security planning must be performed. Security planning must use actual facility data to provide a service- or facility-specific assessment.

- Each VHA VAMC has a facility master plan (FMP); security considerations, including a VHA security master plan,[5] are a key part of the FMP which are needed to implement the requirements of this manual. The physical security and resiliency requirements for VHA facilities must be included in the security master plan.[6]
- Each NCA National Cemetery has a site master plan; security considerations, which should be included in the NCA site plan, are a key part of the risk assessment needed to implement the requirements of this manual.

When a facility does not have a security plan as part of its FMP, then leverage an existing assessment, such as the VA Police assessment or the HVA, when conducting security planning for the project during the project planning phase. Security planning is necessary to enable the efficient integration of new security systems with one another or, for existing sites, to incorporate new into existing systems. For example, the electronic access control systems need to be compatible with existing monitoring systems.

[5] Details of the security master plan are based on the requirements of NFPA 730, Chapter 5.
[6] The continuity risk assessment requirements are guided by the 2016 version of NFPA 1600, Chapter 5.

2.1.2 Requirements for a Certified Physical Security Specialist

The risk assessment (threat/hazard, consequences, and vulnerability analyses), security design, CPTED, and anti-terrorism force protection analysis must be completed by a physical security specialist and structural blast specialist complying with the following requirements. (See section 1.8 Requirements for Subject Matter Specialists)

The physical security specialist must have a minimum of five years' experience in physical security design and must maintain current certification as Certified Protection Professional (CPP) or Physical Security Professional (PSP) from ASIS International (ASIS). The physical security specialist must have demonstrated knowledge and experience conducting risk assessments, applying security strategies, such as the application of CPTED, ballistic and forced entry resistance requirements, and anti-terrorism force protection. The résumé of the specialist must be submitted to the VA Project Manager (PM) for review and approval prior to the concept phase of the project. The qualifications of the firm for whom the specialist works must also be submitted with the résumé.

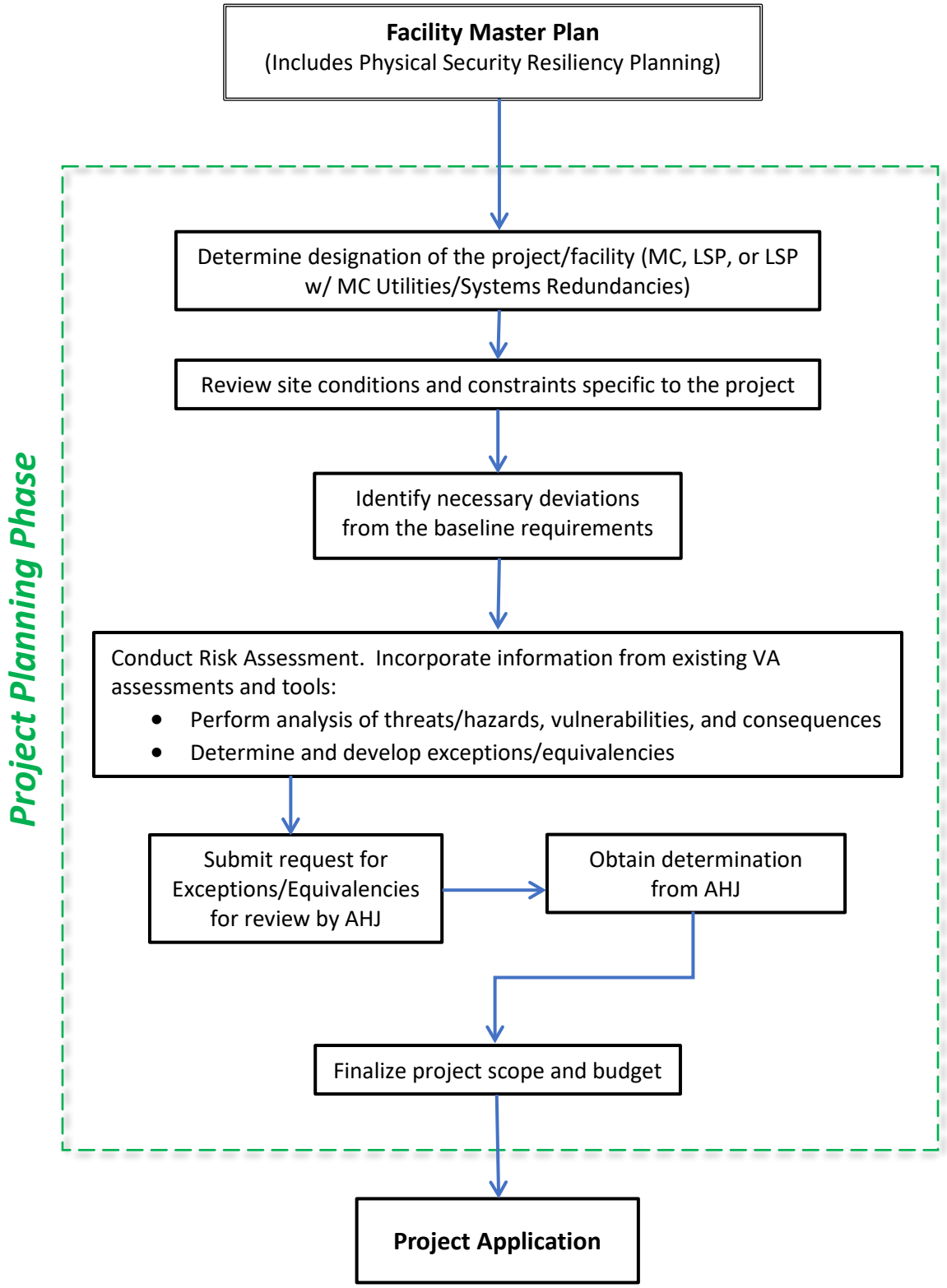
2.2 Risk Assessment of VA Facilities

Risk assessments during the project planning phase must be conducted for all VHA, VBA, and NCA facilities to address site/facility specific conditions and support reduction or deviation from the baseline physical security and resiliency requirements as shown in figure 2-1.

Risk assessments of existing VA facilities show 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 risk targets 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 manmade threats and natural extreme events. Potential impact to the VA facility from the damage/loss of adjacent high-risk facilities must be taken into consideration. The term risk, as used throughout the PSRDM, includes all three factors: (1) threat/hazard, (2) vulnerability, and (3) consequences.

The first task in preparing a risk assessment is to identify the assets and people that need to be protected. Next, a threat/hazard analysis is performed to identify and define the threats and hazards that could cause harm to a building and its occupants. Threats and hazards must be measured against the overall facility and each MC function and system it contains or supports. After threats/hazards and assets are identified, a vulnerability analysis is performed to identify weaknesses. Next, the consequences to the mission that would result from a hazard event or a successfully executed threat are defined. Using the results of the asset's threat/hazard, vulnerability, and consequences analyses, risk is determined. See Chapter 2 Annex for additional information.

Figure 2-1 Deviation/Equivalency Process by Project Specific Risk Assessment



2.2.1 Threat/Hazard Analysis

The PSRDM addresses both manmade threats and natural hazards, requiring a multi-hazard analysis. Consider all manmade threats and natural hazards as possible risks, and then tailor the list to the facility.

Manmade hazards to the site and facility fall into two categories: (1) physical threats to personnel and tangible property, and (2) threats of electronic or computer-based attacks on the information systems that control these critical infrastructures. The deliberations of this chapter involve only physical threats. The most likely event is disorderly conduct or an accidental event, such as an out-of-control vehicle, which rarely cause significant damage or require the facility to shut down. Compartmentalization of spaces, such as having controlled doors between waiting areas and treatment areas assists in limiting the impact of disorderly conduct.

During a multi-hazard analysis, areas of consideration include but are not limited to:

- Administrative headquarter office
- Mass gathering sites, such as lobbies and auditorium
- Childcare/Development Center
- Loading Docks
- Heating/Cooling plant
- HVAC system, including air intakes
- Mailroom
- Caches
- Laboratories
- Pharmacies
- Datacenter/Telephone distribution and main switchgear
- Emergency Department (ED)
- Water supply, including reservoir
- Fuel storage
- Main switchgear
- Liquid oxygen (LOX) storage
- Patient, visitor, and staff parking lots

For facilities generally open to the public (such as those providing health care), there are four main zones of concern: (1) the lobby, where a suspicious person may be challenged; (2) waiting areas outside of access controlled treatment areas; (3) the mailroom, where mail is received for distribution; and (4) the loading dock, or the area where supplies or equipment are received

and held temporarily awaiting distribution. Pay special notice to the Emergency Department (ED).[7]

For facilities not open to the public and having established access control procedures (such as data centers and processing benefits claims), there are three main zones of concern: (1) the lobby and cloakroom, where people await entry into the secure area of the building; (2) the mailroom, where mail is received for distribution; and (3) the loading dock, or the area where supplies or equipment are received and held temporarily awaiting distribution.

Threat analyses must consider the possibility of adjacent threats from nearby non-VA targets and the community in general.

2.2.2 Vulnerability Analysis

There are multiple vulnerability analysis processes across the Department, such as the risk assessment program utilizing the Modified Infrastructure Survey Tool (MIST) and the Hazard Vulnerability Assessment (HVA) process. [8]

In general, the first step in a comprehensive vulnerability analysis is to identify and prioritize the likely manmade threats and natural hazards that the site and facility could face, as in section 2.2.1 Threat/Hazard Analysis. These are typically identified using historical and current data from multiple sources. Based on the list of threats/hazards generated, the general vulnerabilities for the facility are identified.

Determine PSRDM-related vulnerabilities by assessing baseline physical security and resiliency requirements to specific threats/hazards. Assess whether the facility follows design concepts to address potential threats and hazards.

2.2.3 Consequences Analysis

Consequences analysis provides the level, duration, and nature of the loss resulting from an undesirable event. Consequence is commonly measured in four ways: human, economic,

[7] Emergency Departments and ED environs were the most common site (29%), followed by the parking lot (23%) and patient rooms (19%) for hospital-based shootings in the United States between 2000 and 2011; see Gelen, G.D.; Catlett, C.L; Kubit, J.G., Hsieh, Y-H. Hospital-Based Shootings in the United States: 2000- 2011. Annals of Emergency Medicine, Volume 60, No. 6: December 2012. Available at: http://www.annemergmed.com/article/S0196-0644(12)01408-4/abstract

[8] VHA's Hazard Vulnerability Assessment (HVA) process is not applicable to VBA or NCA. Reference NFPA 99, Chapter 12, 1.5.3 for HVA process within VHA.

mission, and psychological, but may also include other factors such as impact on the environment.[9]

- Human consequences include direct impacts (numbers of people affected, fatalities, injuries) and indirect impacts that may arise due to strains on health services. The infliction of mass casualties is an acknowledged goal of many terrorist organizations. Recovered terrorist preoperational surveillance reports include considerable details on the times of day the target population is at its highest and do not distinguish between tenants and visitors. From a consequence perspective, the potential for mass casualties is a major consideration. Thus, the facility population factor is based on the peak total number of personnel in the space, including employees, onsite contract employees, patients, and visitors. This number should not include such transient influxes in population as an occasional conference (or similar event), unless the facility is intended for use in such a manner (such as a conference center) and the population is part of normal business.
- Economic consequences encompass the net economic cost, including both direct (loss of goods, buildings, infrastructure) and indirect (loss of business, increased demand for public services) costs.
- Mission consequences are important, as the value of a facility to the U.S. Government is based largely on the mission of the facility, particularly as it may relate to essential functions and other important business of the Department. As vital as it is for VA to perform these activities, it is equally attractive to adversaries to disrupt important government missions.
- Psychological consequences are important because of the potential negative effect of an undesirable event occurring at a prominent Federal facility. Attacks at certain government facilities, particularly those perceived to be well-protected and central to the safety and well-being of the United States could result in a loss of confidence in the U.S. Government domestically or internationally.

2.3 Exceptions and Deviations

After the risk assessment has been completed and it has been determined that the facility cannot comply with certain requirements of the PSRDM, request for deviation must be submitted to the respective AHJ (as defined in section 1.3 Administration and Enforcement) for review following the procedures of this section. For VHA facilities, requests must be submitted to the Healthcare Environment and Facilities Programs Oversight Committee on Physical

[9] Based on para 4.4 of ISC Risk Management Process, Aug 2013

Security and Resiliency, who provides oversights and guidance on engineering issues related to the physical security and resiliency of VHA facilities and their operation.

2.3.1 Exceptions

When a determination is made at the local level, that due to mission, function, location, or regional responsibility a facility should be upgraded from LSP to MC (or downgraded from MC to LSP), or when an exception/deviation from a specific physical security and resiliency requirement is sought, a request must be submitted — during the project planning phase before development of scope and budget — and approved by the AHJ who is responsible for overseeing implementation of the facility's physical security and resiliency requirements.

2.3.2 Procedures for Exceptions and Deviations

The local facility may initiate the deviation (variance) request process. The request must be submitted to the AHJ for review and approval.

2.3.2.1 Exception/Deviation Requests must include a narrative with justification for the request; to the extent applicable, include the following information:

- Building category.
- Default physical security and resiliency designation and/or baseline requirements from which deviation(s) occur.
- Physical limitations on implementation imposed by existing conditions.
- Programmatic limitations imposed by implementation of PSRDM requirements.
- Alternative method of achieving equivalency/equal level of protection or a schedule for phased implementation of requirements as part of risk mitigation strategy (VHA only).
- Cost of implementation of baseline requirements with a comparison cost of the proposed equivalency.
- Funding sources.
- Impact of exception/deviation on design schedule, construction schedule, and future operations.
- Detailed effects on HVA and CEMP (VHA only) and Emergency Operations Plan (EOP).

2.3.2.2 Review and Approval Procedures for waiver or exceptions/deviations must be as follows:

- Obtain concurrence from the AHJ responsible for overseeing implementation of physical security and resiliency requirements for the facility; follow the process

for obtaining such concurrence as established by each respective Administration — VHA, VBA, or NCA.

- For Major Construction projects, forward a copy of the final AHJ determination to the Office of Facilities Planning within CFM.

2.4 Application of Requirements in Common Project Scopes

Table 2-1 provides a list of common project scopes, most likely scenarios, and applicability of baseline physical security and resiliency requirements. Additionally, a uniform message regarding applicability of baseline physical security and resiliency requirements is included for each discipline in the chapters that follow.

Table 2-1 Project Scopes/Requirements

	Project Scope	Baseline Physical Security and Resiliency Requirements
1	Entire new campus	Comply with requirements for new construction for the entire campus and buildings.
2	New building(s) on an existing campus [Note: Design and addition of new building or structure must not degrade or increase risks to existing buildings and infrastructure.]	Comply with requirements for new construction for the new building(s). Campus level requirements, such as those associated with entrance to the campus, campus perimeter barrier, utilities, etc., are not required, except when included during planning of the project. Stand-off distance requirements are applicable for the new building(s).
3	Addition (horizontal expansion) to an existing building	Comply with requirements for new construction for the building addition.
4	Alteration/renovation (≥50% of area of existing building)	Comply with requirements for "Alteration/Renovation of Existing Facilities" for the entire building.
5	Alteration/renovation (<50% of area of existing building)	Comply with requirements for "Alteration/Renovation of Existing Facilities" only for the area being altered or renovated.
6	Alteration/renovation (≥50% of area of one single floor of an existing building)	Comply with requirements for "Alteration/Renovation of Existing Facilities" for the entire floor.

Project Scope		Baseline Physical Security and Resiliency Requirements
7	Alteration/renovation (<50% of area of one single floor of an existing building)	Comply with requirements for "Alteration/Renovation of Existing Facilities" only for the area being altered or renovated.
8	Alteration/renovation (≥50% of a functional area)	Comply with requirements for "Alteration/Renovation of Existing Facilities" for the entire functional area.
9	Alteration/renovation (<50% of a functional area)	Comply with requirements for "Alteration/Renovation of Existing Facilities" only for the area being altered or renovated.
10	Renovation or addition to a building that adds or changes a functional area (refer to Table 1-7), including particularly additions or changes of high value/high risk.	Consult with AHJ to identify requirements.
11	Phased projects or series of projects	When a total effort is being constructed in phases or as a series of phases, the requirements in the PSRDM must be incorporated so that when all phases or sub-projects are completed, the final design and construction of the altered/renovated building must comply with the PSRDM.
12	Site modifications (such as reconfiguration of roads, parking lots, addition of a parking structure, etc.)	Comply with requirements associated with site (primarily in Chapter 3). Comply with stand-off distance around existing buildings even when the project scope does not include alteration/renovation of existing buildings.
13	Perimeter fence: Replacement	Comply with requirements for perimeter barrier in Chapter 3.
14	Non-bearing Exterior Wall/Façade: Complete replacement of Façade	Comply with Chapter 6 building envelope requirements for new construction.
15	Fenestration: Windows replacement upgrades in which the building exterior walls are not replaced	Comply with requirements of 6.3.1.1 Glass and 6.3.1.2 Glazing.

Project Scope		Baseline Physical Security and Resiliency Requirements
16	Fenestration: Glass replacement upgrades and "storm window" upgrades interior to existing façade (for example, Historic)	Comply with requirements of 6.3.1.1 Glass and 6.3.1.2 Glazing.
17	Fenestration: For renovations of a building in which glazing is not replaced	Comply with requirements of section 6.3.2.1.
18	Structure: Addition of a new story to an existing multi-story building originally designed without progressive collapse prevention	For the addition, comply with Chapter 6 Building Envelope requirements. Chapter 7 requirements are not applicable. If the vertical expansion is two or more stories, the applicable requirements are to be determined on a case-by-case basis by the AHJ.
19	Replacement of specific building system(s) such as electrical, mechanical, plumbing, telecom, security systems, etc.	When alterations/renovations involve changes to the building systems, that do not involve the building interior, the local facility, with concurrence by the region/network and approved by the AHJ must determine whether the work is ≥50% of the building system. When the work is ≥50% of the building system, or when the total work of independent concurrent or sequential projects within a 5-year period is ≥ 50% of the building systems, comply with requirements for "Alteration/Renovation of Existing Facilities" for the entire building system. When the work is <50% of the building system, comply with requirements for "Alteration/Renovation of Existing Facilities" only for the portion of the building system being replaced.
20	Replacement of critical equipment (such as a boiler, chiller, emergency generator, etc.) within a building system	Comply with applicable requirements in Chapter 8 Utilities and Building Services and Chapter 9 Building Systems for replacement of the critical equipment. When the scope does not include alteration/renovation of the building structure enclosing the critical equipment, upgrading of the building structure to comply with the PSRDM is not required.

Annex to Chapter 2

A-2.1 Background: VA Requirements as Compared to Other Federal Agencies

The applicability of the VA PSRDM is comparable to the *Risk Management Process for Federal Facilities, An Interagency Security Committee (ISC) Standard*. Both apply to new buildings and those identified to undergo a certain type of alteration/renovation or major modernization.

The ISC Standard requirements apply to new buildings and buildings undergoing renovation or major modernization. For existing buildings, the criteria are applicable in three situations: (1) the existing building has deferred or delayed security measures; (2) an existing building or space is to have a change in building occupancy type (for example, a warehouse is converted to office space); or (3) the addition is 50 percent or more of the gross area of the existing building. In all cases, the ISC requires a risk assessment during the planning phase.

The VA PSRDM requirements apply to new construction, whether free-standing structures, additions, or alterations/renovations. Direction on applicability is found in each section of the PSRDM.

The process in the VA PSRDM is comparable to the ISC Standard. The steps in the process are compared below:

- The ISC process starts with determining a Facility Security Level (FSL) which range from Level 1 (lowest risk) to Level 5 (highest risk), based on several factors such as mission criticality and facility population. Similarly, the PDRSM process starts with determining criticality and the facility's default physical security and resiliency designation as a MC or LSP based on the requirement to continue operation during a natural or manmade extreme event.
- The next step in the ISC process is to identify the facility's baseline Level of Protection (LOP). The LOP relates directly to a set of baseline protective measures, one for each of the five facility security levels. The baseline LOP must be implemented unless a deviation is justified by the risk assessment. Similarly, the VA PSRDM has baseline requirements for MC facilities and for LSP facilities.
- The next step in the ISC process is to identify and assess risk. A certain risk assessment methodology is not mandated, but ISC requires an analysis of threat, vulnerability, and consequences to specific undesirable events identified by the ISC.[10] In the VA PSRDM process, only when deviation from the baseline requirement is sought is a risk assessment required. VA has an existing assessment program and tools (such as the VHA's HVA, Police assessment, and CEMP) that are used to inform security planning and

[10] Para 5.1.2, The Risk Management Process: An ISC Standard Integration of the Physical Security Criteria, Aug 2013

risk assessment. Risk assessment during the project planning phase is required to analyze the threat/hazard, vulnerability, and consequences of specific undesirable events.

- The next step in the ISC process is to determine the necessary LOP. When the assessed risk of an undesirable event is higher or lower than the facility's baseline LOP, protective measures are to be added or eliminated to align the LOP with the assessed risk. In the VA process, when an assessed threat/hazard is higher or lower than the facility's PSRDM baseline requirements, based on the risk assessment protective measures may be added or eliminated to align the requirements with the level of assessed risk.
- The final step in the ISC process is to implement protective measures and/or accept risk; determine if the baseline LOP or necessary LOP is achievable. If so, put requirements in project design. If not — due to physical limitations, restrictions, or other — consider alternate locations and/or document and accept unmitigated risk. The VA PSRDM process is the same: if achievable, include in the project design requirements, if not, consider alternate solutions through the exception/deviation process.

A-2.2 Risk-Based Protective Design

Despite a wide range of terrorist threats, including chemical-biological and cyber-attacks, explosions remain the most insidious, requiring the least sophisticated materials and expertise to assemble and deploy. Without arousing any suspicion, the principal components of an explosive device may be obtained at a variety of retail outlets. For this reason, VA requires the blast resistant protective design of VA facilities. These provisions recognize the risks and hazards associated with explosive events and prescribe different levels of protection based on the nature of the structure and its criticality.

The effectiveness of the PSRDM and the impact on the overall design is a balance between the cost of protective measures and the cost of regrets. The most beneficial protective measures typically involve the design of anti-shatter facade systems and the hardening of structures to resist the effects of progressive collapse; however, the strategies differ for the design of new structures and the upgrade of existing facilities.

Risk management requires an evaluation of the range of threats and vulnerabilities of the facility in response to the postulated threats. While risk is inevitable, the resources that are best expended to mitigate the hazards may be quantified. This process starts with a Threat Assessment, which evaluates the potential threat scenarios. Once the maximum credible events are defined, a Vulnerability Assessment evaluates the facility's response to these events and identifies the level of hazard associated with the different component responses. In most cases, the vulnerability assessment primarily considers the life safety of occupants; however, for critical facilities, the assessment must consider the continuity of operations, as applicable.

The vulnerability assessment is used to quantify the damages and serve as a basis for developing hazard mitigating upgrades.

Borrowing from seismic risk quantification methods, for which there are defined return periods for different magnitude events, the anti-terrorism risk procedures substitute accessibility to an asset for the likelihood of an event occurrence. This allows an assessment of a given facility's component assets relative to each other or to different facilities, but it does not permit a comparison of anti-terrorist risk to any other form of disaster (natural or manmade). In order to compare risk of different types of hazards, the evaluator must establish a relative likelihood of occurrence for the different hazards. This approach is discussed in FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*. A measure of relative risk may be represented as the product of O (Occurrence), V (Vulnerability), and I (Importance):

Risk = O × V × I

Occurrence (O) is the hazard model used to characterize the likeliness of an initiating event. For blast hazard (and acts of terrorism in general) the events are virtually limitless and depend on several factors such as the intent and resources of the aggressor. Since event occurrence is a function of the characteristics of the target facility, actions that reduce the attractiveness of a target facility and/or deter certain types of events are typically assumed to reduce the likelihood of occurrence.

Vulnerability (V) refers to the damage or fragility model that is used to characterize the outcome or consequences of the event's occurrence. Vulnerability modeling requires the engineering analysis of the facility in order to determine responses for the loads induced by the initiating event. Vulnerability analyses may be performed for the initial state of a structure and may be re-calculated for each upgrade option that is under consideration.

Importance (I) is used to characterize the criticality or the social and economic impact of a facility's operation on the region, the owner, and the society at large. Importance is a necessary component of the risk quantification when a diverse portfolio of facilities is to be evaluated and any sort of prioritization is to take place. The importance of a facility is often considered to be hazard-independent, as it is a function only of the facility's economic and social status.

These calculations allow VA to assess design or mitigation alternatives by comparing expected losses to estimated costs for each alternative. For the purpose of these calculations, the term "loss" includes cost of repair, down-time and casualties. However, a key assumption is that expected damage, down-time and casualties can be estimated for a given building subjected to a given threat scenario. Some decision makers prefer to characterize the various components of performance (such as cost of damage repair, down-time, and casualties) separately while others prefer one characterization of risk that combines all three effects. This can be done by

normalizing each component of risk and combining these values in a weighted average using techniques based on multi-attribute utility theory.

The patterns of past domestic events may not predict the future; nevertheless, it gives valuable insight to the protection against a very low probability but potentially high consequence event. Although each successive major domestic terrorist event exceeded the intensity of the predecessor, VA structures are to be designed to resist a nominal weight of explosive similar to other U.S. Government agency practices.

3 SITE CONSIDERATIONS

3.1 Scope, Purpose, and Goals

This chapter focuses on security design concepts, elements, and site planning strategies that influence the protection of the built and natural environments. See Chapter 3 Annex for additional information.

As stated in Chapter 1, the requirements in this manual apply to new buildings, additions and existing facilities undergoing renovations. Further clarification on applicability to renovation projects is provided in table 2-1 and in the gray box describing alteration/renovation of existing facilities at the end of each major section. A new facility (MC Facility, LSP Facility w/ MC Utilities/Systems Redundancies, or LSP Facility) on an existing campus or an existing facility undergoing renovation does not require the entire campus to be upgraded to the same level. Only the portion of the site occupied by or supporting the facility are required to meet the requirements.

The requirements of this chapter are baseline physical security and resiliency requirements for MC Facilities, LSP Facilities with MC Utilities/Systems Redundancies, and LSP Facilities. LSP Facilities with MC Utilities/Systems Redundancies are to comply with requirements for LSP Facilities. A risk assessment during the project planning phase is allowed to evaluate the deletion or incorporation of other specific requirements (see section 2.3 Exceptions and Deviations). The VA AHJ, defined in section 1.3 Administration and Enforcement, overseeing implementation of physical security and resiliency requirements for the facility will review submitted request for deviation from the baseline requirements of this chapter. When no risk assessment is performed, these baseline requirements apply.

The requirements of this chapter supplement other related VA standards for construction, space and facility planning criteria, design guides, design manuals, specifications, and details, which remain in full force and effect. Specifically, all requirements of VA Handbook 0730, Security and Law Enforcement, Appendix B, (which covers physical security requirements for VA facilities), the VA Fire Protection Design Manual (which covers all VA construction), and ICT standards on the TIL remain in effect.

3.2 Crime Prevention through Environmental Design (CPTED)

VA follows the principles of Crime Prevention through Environmental Design (CPTED) (http://www.cpted.net) in order to influence offender decisions that precede criminal acts by affecting the built, social, and administrative environment. The following CPTED principles must be incorporated into the site design for all VA facilities and sites.

3.2.1 Natural Surveillance

Design the location of physical features, activities, and lighting to preclude hiding spots and maximize visibility of the space and its users. For example, place windows overlooking sidewalks; have open vestibules at building entrances; and, create landscape designs that do not block visibility.

3.2.2 Natural Access Control

Utilize the strategic placement of entrances, exits, fencing, and landscaping to create a perception of risk in potential offenders.

3.2.3 Natural Territorial Reinforcement

Clearly delineate private space to create a sense of ownership where strangers or intruders stand out and are more easily identified. For example, use design element such as sidewalks, landscaping, different paving material, and changes in street elevation to help distinguish between public and private areas.

3.2.4 Target Hardening

Use features that prohibit entry or access, such as perimeter boulders or large rocks, streetscape furniture, art ornamentals, and other perimeter barrier or screening devices.

3.2.5 Alteration/Renovation of Existing Facilities/Sites — CPTED

Requirements for CPTED must be the same as in section 3.2 Crime Prevention through Environmental Design.

3.3 Standoff Distance

Unscreened vehicle must not be permitted to park or travel closer than the minimum standoff distance to any side of a MC or LSP facility. Screened vehicle[11] must not be permitted to park or travel within 5 feet (1.5 m) of any MC or LSP VA facility.

Table 3-1 Standoff Distance

Criteria	Life-Safety Protected	Mission Critical
Minimum Standoff Distance	25 feet (7.6 m)	50 feet (15 m)

[11] A screened vehicle is a motor vehicle that has been examined systematically to determine whether or not a security threat that needs to be mitigated is present. See Glossary.

Criteria	Life-Safety Protected	Mission Critical
Minimum Standoff Distance for Screened Vehicle	Five (5) feet (1.5 m)	Five (5) feet (1.5 m)

These minimum standoff distances are to be provided to the edge of the curb line demarcating the internal roadways and parking within a VA campus. For facilities not located within a campus with internal roadways or parking, the minimum standoff distance is to be provided to the site perimeter fence.

Some facilities require access to areas within the required standoff distances for dropping off or picking up people or loading or unloading packages and other objects. Examples that may require drive-up or drop-off include the medical facility main entrance and lobbies. In these cases, construction of an entrance pavilion, within the standoff distance, that is structurally independent of the facility and provides a protected walkway from the drop-off to the building entrance, may be provided. (See section 4.2 Public Entrances and Lobbies and section 7.2 Blast Resistance.)

3.3.1 Alteration/Renovation of Existing Facilities/Sites — Standoff Distance

Requirements for standoff must be the same as Table 3-1 Standoff Distance.

3.4 Perimeter Barrier

A perimeter barrier[12] assists in controlling and screening authorized entries into secured/protected areas by channeling vehicles and personnel to access control points. It deters casual intruders from penetrating a secured/protected area by presenting a barrier that requires an overt action to enter. It also causes a delay to obtain access to a campus or facility, thereby increasing the probability of detection. Note: In urban areas the wall of a building may be on the perimeter and act as the perimeter barrier.

3.4.1 Perimeter Requirements

A barrier must be established either around the MC or LSP facility, or for the campus perimeter within which the MC or LSP facility is located. The perimeter barrier must clearly mark the site perimeter, provide vehicular/pedestrian access control, identify intentional trespassers, and support campus/facility security operations. The barrier must be consistent with campus

[12] For additional guidance on construction requirements for site security, such as perimeter fences and other barriers, refer to the Uniform Facilities Criteria (UFC) UFC 4-022-02 and UFC 4-022-01 available on the Whole Building Design Guide (WBDG) (http://www.wbdg.org).

architectural elements. For larger sites (with more open space than needed for public gathering areas and operational support areas, such as parking and service yards, around the building), signage may be used to mark the property line or perimeter.

When it is determined that the buildings and the immediate vicinity within a site require a higher standard of barrier than the perimeter of the site, an additional barrier (fence, knee-wall, water or landscape feature) must be provided around the building, to include public gathering[13] and operational support areas.

It is important to note that the perimeter barrier requirements in the PSRDM address physical security and do not address fencing for code or general liability issues. See Chapter 3 Annex for additional information.

3.4.2 Gates

Sufficient gates must be provided to control access to the facility following an emergency event or under high threat conditions, based on the following site conditions: user demand, existing terrain and available space, future development plans, compatible land use and environmental constraints.[14]

Gates, where established, must be of the same or similar design and materials as the adjacent fences. Location of the gates must have standoff from public streets to provide the security force with early warning of approaching pedestrians or vehicles. Gates must be located away from known criminal adjacencies (such as prisons and high crime areas). The roadways adjacent to the gates must provide transitional, non-silhouette lighting and traffic calming features. Gates must be access card operated from the outside or as prescribed by the AHJ. The vehicular gates must be capable of being locked but are not required to be anti-ram rated.

3.4.2.1 Pedestrian Gates: Pedestrian and bicycle gates must be lockable, swing in the outward direction, and be fully accessible to persons with disabilities in width and operation.

3.4.2.2 Vehicular Gates: Vehicular gates must limit opening sizes when possible to decrease open/close cycle time. There is no maximum height for vehicular gates; coordinate gate height with surrounding/adjacent security fencing. Gate width will be at least as wide as the road entering the gate. The operational requirements for the gate must be evaluated to determine which gate type is most suitable. Analysis for all vehicular gates must consider daily peak of vehicular traffic and the operational access

[13] For further information on plaza and public gathering areas see GSA PBS-P100, Facilities Standards for the Public Buildings Service, March 2015.
[14] For additional guidance on gate construction see UFC 4-022-01, 25 May 2005, UNIFIED FACILITIES CRITERIA (UFC) SECURITY ENGINEERING: ENTRY CONTROL FACILITIES/ACCESS CONTROL POINTS.

control requirements for the secured area to determine opening size, gate type, and whether an automatic operator is needed. Follow the requirements of ASTM F2200 for gates used for vehicular traffic that are to be automated. Cantilevered, sliding, or wheel supported gates are considered the best selection for vehicle security gates followed by overhead sliding gates, swing gates, and vertical tilt gates. Areas where snow and ice are prevalent may consider using cantilever or swing gates instead of tracked sliding gates. However, when sliding gates are used, consideration must be given to adding internal heating for gate mechanisms.

The vehicular gates must be capable of being locked but do not have to be anti-ram rated.

3.4.3 Alteration/Renovation of Existing Facilities/Sites — Perimeter Barrier

When included as part of the project scope during the project planning stage, requirements for perimeter barrier are the same as in section 3.4 Perimeter Barrier including 3.4.2 Gates. See Table 2-1 Project Scopes/Requirement for additional information.

3.5 Vehicle and Pedestrian Screening

(Section 3.5 is applicable to MC facilities only)

3.5.1 Guard Houses

MC facilities will establish guard houses at pedestrian and vehicle perimeter entrances to conduct vehicle and pedestrian screening under increased threat conditions. The number, type, and location of the guard houses will be determined through a risk analysis.

- The guard houses must be enclosed and sufficient for protecting guard personnel conducting gate operation, vehicle inspection, and information dissemination.
- Guard houses must be designed to permit the guard to perform duties and must have a secondary means of egress.
- Guard house design must be compatible with the facility architecture and the neighborhood.
- Guard houses must be heated, air conditioned, and lighted to provide an appropriate work environment.
- Guard houses must be provided with power, telephone, intercom, and data.
- Guard houses must be designed to be ballistic resistant, with doors, walls, and windows meeting a UL 752 Level 3 standard and 15-minute forced entry resistance rating.

- Guard houses must be afforded crash protection (from traffic in either direction). Passive barriers such as bollards, reinforced concrete walls or knee-walls, or crash cushions must be used to protect personnel standing on the traffic islands. The maximum height of crash protection barriers will be three (3) ft. (1 m) or the elevation of the guard facility window sills, whichever is less, to avoid conflicts with traffic or guard sightlines.
- Guard houses may be permanent or temporary, relocatable guard shacks; when temporary, relocatable guard shacks are used, each potential location must be furnished with power, telephone, intercom, data, and protected by anti-ram barriers.

3.5.2 Vehicle Screening Area

MC facilities must provide adequate space to accommodate vehicle screening without blocking public rights-of-way.

3.5.2.1 Space and Utilities: The screening area must provide adequate space and utilities to accomplish the following tasks.

- Visual identity check of driver's license.
- Visual inspection of vehicle interior, including luggage compartment, cargo boxes, and trailers.
- Trace element swipes and sensors.
- Space where at least one vehicle may be held for further inspection without blocking access for cleared vehicles to pass.

3.5.2.2 Stacking Space: Stacking space must be provided for vehicles awaiting inspection outside entrances and off public roads.

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

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

3.5.2.4 Parking: Parking to be provided inside the entrance gate for two police vehicles.

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

3.5.3 Alteration/Renovation of Existing Facilities/Sites — Vehicle and Pedestrian Screening

When included as part of the project scope during the project planning stage, MC facilities must meet the requirements of sections 3.5.1 Guard Houses and 3.5.2 Vehicle Screening Area. See Table 2-1 Project Scopes/Requirement for additional information.

3.6 Anti-Ram Rated Vehicle Barriers

Active or passive vehicle barriers must be selected based on the appropriateness of the architecture of the facility and the specifics of the site and natural environment. See section 7.5 Anti-Ram Resistance for details on performance of anti-ram elements.[15]

3.6.1 Active Anti-Ram Rated Vehicle Barriers (Section 3.6.1 is applicable to MC facilities only)

Types of active barriers must be anti-ram rated hydraulic or electric wedges, plate, beam, catch cable system, or retractable bollards recessed into the pavement for a flush condition when not deployed. Barriers may be permanently installed or portable type.

3.6.1.1 Locations: Active anti-ram rated vehicle barriers must be located at required access points that permit vehicles within the minimum standoff distance around the facility. This includes gated access to the loading dock, emergency lanes for first responders, and maintenance access.

3.6.1.2 Structure: See section 7.5 Anti-Ram Resistance for structural requirements of active anti-ram rated barriers.

3.6.1.3 Portable Barriers: Each identified location for use must be provided with necessary utilities (when needed) and configured in such a way that the barriers may be easily put into place when needed.

Portable barriers are to be stored in a secure location, readily accessible by authorized personnel, with lifts and transport devices to permit rapid deployment.

3.6.2 Stationary (Passive) Anti-Ram Rated Vehicle Barriers (Section 3.6.2 is applicable to both MC and LSP Facilities)

Anti-ram rated natural or manmade barriers may be used as a stationary barrier. Landscaping examples include berms, gullies, boulders, trees, and other terrain. Hardscaping examples include benches and planters. Structural examples include walls, bollards, and cables.

[15] For additional reference see *The Site Security Design Guide by the U.S. General Services Administration, Public Building Service*. Washington, DC: GSA, June 2007. https://www.wbdg.org/ffc/gsa/criteria/site-security-design-guide

3.6.2.1 Locations: Anti-ram vehicle barriers must be located at hospital main entrances due to a history of vehicle strikes at these locations.

Anti-ram vehicle barriers must be located at lobby entrances of other building types, cafeterias, child-care play yards, and other gathering areas when at risk from vehicle strikes. The barriers must be walls, stationary bollards, cables, or combination of landscape and hardscape that achieves the required anti-ram resistance.

Anti-ram vehicle barriers must be located at utility connections, emergency power supplies, hazardous-materials storage, HVAC, and external critical telecom and IT resources when at risk from vehicle strikes.

3.6.2.2 Structure: See section 7.5 Anti-Ram Resistance for structural requirements of passive anti-ram vehicle barriers.

3.6.2.3 Accessibility for Persons with Disabilities: Coordinate locations of passive barriers, such as bollards, with accessibility requirements when placed adjacent to or across a path of pedestrian travel and patient transport.

3.6.3 Alteration/Renovation of Existing Facilities/Sites — Anti-Ram Rated Vehicle Barriers (Section 3.6.3 is applicable to both MC and LSP Facilities)

MC and LSP facilities must comply with the requirements of section 3.6 Anti-Ram Rated Vehicle Barriers.

3.7 Parking

Security considerations for parking (lots and structures) must include the safeguards found in this section. Additional safeguards may be established in accordance with the findings of the facility specific pre-design risk analysis.

It is important to note that parking and facility access must comply with the VA accessibility requirements[16] for persons with disabilities. Where access from parking to the facility for patients, visitors, and staff with disabilities is constrained by the required standoff distance, consider provisions to accommodate a shuttle service[17] for persons needing assistance, which may include accessible shuttles with stops or shelters in parking areas and shuttle stop/parking at building entrance(s).

[16] VA Barrier Free Design Guide (PG-18-13) on the CFM TIL at http://www.cfm.va.gov/til/accessibility.asp.
[17] Operated by VA or a Veteran Service Organization (VSO).

3.7.1 Parking Areas

Separate parking areas must be provided as follows:

- Patients and visitors.
- Employees/staff.
- Service/delivery vehicles, where applicable.
- Emergency vehicles, where applicable.

3.7.2 Location

New facilities must not be built with parking in or under the facility. Minimum standoff distances for MC and LSP facilities must be as shown in table 3-1.

3.7.2.1 Surface Parking: Vehicles must not be parked or permitted to travel closer than the minimum standoff distance to any MC or LSP facility.

3.7.2.2 Parking Structures:[18] Above grade parking structure, whether on- or offsite, must not be constructed closer than minimum standoff distance to any MC or LSP facility. Additionally,

- Unscreened vehicles must not be permitted to be parked within or under any VA facility.
- Maximize the visibility into and within the parking structure.
- Enhance natural surveillance and line-of-sight.
- Close off potential hiding places below stairs.
- Avoid dead-end parking areas and areas of concealment.
- Include in the design the ability to completely shut down vehicular and pedestrian access to the parking facility when closed.
- Install two-way emergency communication devices on each level of the structure and in all elevators.

Where underground parking is provided adjacent to (not underneath) buildings required to comply with these requirements, parking may be allowed as close to the buildings as the construction of the building superstructure will allow, based on the required level of protection and the applicable explosive weight. Analysis must show that the soil-structure interaction and any venting into the building will not cause progressive

[18] Guidance based on benchmarking with the International Association for Healthcare Security and Safety (IAHSS), 2012 edition, Security Design Guidelines for Healthcare Facilities and with the ISC, The Risk Management Process for Federal Facilities (RMP).

collapse of the building or damage to inhabited areas of the building beyond the applicable level of protection. Also, ensure there is no venting into inhabited areas of buildings that could result in occupant injuries.

3.7.3 Access

Pedestrian and vehicular access from parking to and from the facility will be as follows:

3.7.3.1 From Vehicle Entrance: Straight-line vehicular approaches to a facility must be avoided. Access roads must be configured to prevent vehicles from attaining speeds in excess of 25 mph (40 km/h).

3.7.3.2 From Parking to Facility: Concentrate pedestrian paths to dedicated entrances and exits. (See Chapter 4 for information on building entrances.)

3.7.4 User Type

In addition to the requirements of sections 3.7.1 Parking Areas, 3.7.2 Location, and 3.7.3 Access, the following are parking and access requirements for physical security defined for specific users.

3.7.4.1 Patients and Visitors: Parking and access for patients, visitors, and the persons transporting them to and from the VA facility must be as convenient as possible to the main entrance, and subject to the requirements of para 3.6.2.1. Patient and visitor parking areas must be monitored by video assessment and surveillance system (VASS). Emergency alert systems, such as emergency phones and call boxes that provide quick access to assistance with a direct line to help will be provided as determined by the facility risk analysis.

3.7.4.2 Emergency Department: Emergency entrance must be provided with a small parking area for emergency patients and space for ambulances as convenient as possible to the emergency entrance, and subject to the requirements of para 3.6.2.1. Ambulances must be permitted to approach the building directly and not be subjected to the standoff distance requirements of this chapter; ambulance drop-off bays/garages must not be located under occupied (inhabited) space of the building.

3.7.4.3 Childcare Parents and Staff: All requirements for maintaining standoff distance between vehicles and the building apply. Child drop-off and pick-up must be visible from the office of the Childcare/Development Center and monitored by SSTV. All vehicular areas, onsite and adjacent offsite, including parking and access roads, must be separated from playground areas by fences designed to prevent children from entering the vehicular areas and anti-ram barriers to prevent vehicles from entering the playground.

3.7.4.4 Vendors: The standoff distance and screening requirements of sections 3.3 Standoff Distance and 3.5 Vehicle and Pedestrian Screening apply. Vendors must use the delivery vehicle entrance and service yard at the loading dock. Parking must be provided for vendors in the service yard as needed.

3.7.4.5 Employees and Staff: Employee and staff parking entrances must be controlled by a card-activated gate. Employee and staff parking areas must be monitored by SSTV. Emergency alert systems, such as emergency phones and call boxes that provide quick access to assistance with a direct line to help, to be provided as determined by the facility risk analysis.

3.7.5 Alteration/Renovation of Existing Facilities/Sites — Parking

Card-controlled access gates to staff parking and other traffic separation measures must be used. Parking in or under a MC or LSP facility must be eliminated, where possible. Where parking must remain in or under a MC or LSP building, all vehicles entering the parking must be screened and maintain the minimum standoff distance for screened vehicles of five (5) feet (1.5 m) as listed in table 3.1.

3.7.5.1 Surface Parking: Vehicles must not be parked closer than the minimum standoff distance (see table 3-1) to any side of a MC or LSP facility. Existing parking within this standoff distance must be eliminated, where possible. Where surface parking must remain within the minimum standoff distance, the parked vehicles must be screened or the MC or LSP facility must be hardened to achieve the performance requirements for the corresponding increase in blast loads. (See Chapter 6 Building Envelope and Chapter 7 Structural System for additional information on the façade and structural hardening requirements.)

3.7.5.2 Parking Structures: Where the parking structure (on- or offsite, above grade) must remain within the minimum standoff distance, the parked vehicles must be screened or the MC or LSP facility must be hardened to achieve the performance requirements for the corresponding increase in blast loads. (See Chapter 6 Building Envelope and Chapter 7 Structural System for additional information on the façade and structural hardening requirements.)

Where underground parking is provided adjacent to (not underneath) buildings required to comply with these requirements, parking may be allowed as close to the buildings as the construction of the building superstructure will allow based on the required level of protection and the applicable explosive weight. Analysis must show that the soil-structure interaction and any venting into the building will not cause progressive collapse of the building or damage to inhabited areas of the building beyond the applicable level of protection. Also, ensure there is no venting into inhabited areas of buildings that could result in occupant injuries.

3.8 Site Lighting

The single most important CPTED security feature is lighting. Provide and maintain minimum illumination levels for pedestrian pathways, bicycle and vehicle routes, parking structures, parking lots, wayfinding, signage, pedestrian entrances, and building services which will increase safety and security for people as well as buildings and site.

3.8.1 General Lighting Requirements

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

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

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

3.8.1.3 Luminance Levels: Illumination levels must comply with the Illumination Engineering Society of North America (IESNA), VA Lighting Design Manual, and local and state governing agencies. For illumination requirements, refer to the VA Lighting Design Manual at https://www.cfm.va.gov/til/dManual.asp.

3.8.1.4 Signage and Wayfinding: Wayfinding must be enhanced by site lighting, including providing improved security by assisting pedestrians and vehicles to locate their destinations expeditiously. For signage and wayfinding criteria, refer to the VA Signage Design Guide on the VA CFM TIL at https://www.cfm.va.gov/til/spclRqmts.asp#SIGN.

3.8.1.5 Environmental Quality: 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.

3.8.2 Lighting Locations

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

3.8.2.1 Site Entrances: Lighting must 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 identification documents.
- To assist guards with visual screening of box trucks, cargo areas, trunks, and trailers.
- To provide illumination of wayfinding and signage.

3.8.2.2 Perimeter Fence: Lighting sufficient to support perimeter SSTV surveillance must 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.

3.8.2.3 Building Entrances and Exits: Lighting at building entrances must support SSTV surveillance and ID functions while providing illumination of surfaces and features for safety.

3.8.2.4 Parking Areas: All parking areas covered and open must be illuminated in support of SSTV and other surveillance without objectionable spill into adjacent areas on- or offsite.

3.8.2.5 Pathways: Pedestrian and bicycle pathways and walks, including bike racks, gates, and other features must be illuminated in support of SSTV and other surveillance, while providing for safety without objectionable spill onto adjacent areas on- and offsite.

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

3.8.2.7 Enclosures: The control systems, delivery connections and access gates to liquid oxygen tanks and other major utilities, such as water tanks/towers, electric utility switchgear,[19] fuel storage and refueling stations must be illuminated in support of SSTV and visual surveillance. Note, the full illumination of a water tower or other large storage tanks is not required.

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

3.8.2.9 Loading Docks and Associated Yards: Loading areas must be illuminated for operations and in support of SSTV and other surveillance and identification needs.

3.8.3 Alteration/Renovation of Existing Facilities/Sites – Site Lighting

MC and LSP facilities must have site lighting installed in accordance with section 3.8 Site Lighting.

[19] Where utility provider does not permit their gear inside a customer building, the outdoor switchgear should be illuminated.

3.9 Landscaping

Landscape plans must be designed to enhance lighting, eliminate places of potential concealment or habitation, and address obstructions to surveillance, intrusion detection systems, and lighting systems.

The area on either side of the perimeter fence must be kept clear of trees, shrubbery, and tall grass that could afford concealment for an intruder. The dimension of this clear zone may vary depending on available land, the asset being protected, and the capability of surveillance systems planned for the site. Where land is available, consider a clear zone of 20 feet (6 m) on the outside and inside of the fence.

3.10 Signage

Avoid signs that identify sensitive areas (such as, air intakes, fuel supply valves, gas or power distribution locations), unless required by other codes or standards.

Annex to Chapter 3

A-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 to deter, prevent, detect, delay, and respond to threats in the protection of assets. The concept of concentric levels of control is to protect the central asset behind layers of security measures such that it is least exposed to the threats. Where a single line of defense might be easily breached, the concentric levels approach offers redundancy in lines of defense that are less likely to be breached.

The First Point of Control, or the outermost level: 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. For rural sites, there may be no value to enclosing a large area that has no facilities or services. Increased levels of screening of persons and vehicles, such as when National Terrorism Advisory System (NTAS) Alerts are issued, must be accommodated at the perimeter without burdening surrounding roads with vehicles waiting to enter the site.

The Second Point of Control: 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.

The Third Point of Control: 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.

The Fourth Point of Control: 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.

The Fifth Point of Control, at the innermost level: Restrict access to restricted areas to a minimum with card-reader access controls, security surveillance television (SSTV) monitors, intrusion detection alarms, and forced-entry and/or ballistic-resistant construction. Restricted access areas may include security control centers, select agent storage, narcotics storage and pharmaceutical caches, and laboratories.

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 standoff 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.

A-3.4 Considerations for Perimeter Barriers

The level of protection afforded by the perimeter barrier will be commensurate with the need to control vehicle access and limit pedestrian access. Higher levels of protection, intended to prevent determined intruders, are achieved using anti-climb fences. Lower levels of protection, intended to guide pedestrians, can be achieved using decorative fencing, chain-link fencing, or knee-walls.[20]

[20] For additional guidance on construction requirements for site security, such as perimeter fences and other barriers, refer to the Uniform Facilities Criteria (UFC) UFC 4-022-02 and UFC 4-022-01 available on the Whole Building Design Guide (WBDG).

4 BUILDING ENTRANCES AND EXITS

4.1 Scope, Purpose, and Goals

This chapter provides physical security and resiliency requirements for public entrances, entrance lobbies, patient drop-offs, and employee/staff entrances at Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA) facilities.

The number of public entrances will be limited to the minimum number required. Veterans, their families, and visitors with mobility impairments shall not be required to travel long distances from parking or drop-off locations to access medical care, benefits, or interment services. Access for people with mobility impairments may be accomplished by construction of an entrance pavilion with a covered drop-off that is structurally independent of the facility, meets standoff requirements, and provides a protected walkway from the drop-off to the building entrance.

Entrance requirements for specific functional areas, such as emergency department, loading dock, and other service entrances are covered in Chapter 5. Specific requirements for security devices and their locations are detailed in Appendix A, Security Door Opening Matrix, and Appendix B, Security System Application Matrix of this manual.

As stated in Chapter 1, the requirements in this manual apply to new buildings, additions and existing facilities undergoing renovations. Further clarification on applicability to renovation projects is provided in table 2-1 and in the gray box describing alteration/renovation of existing facilities at the end of each major section. Requirements modified for LSP facilities are specifically noted.

The requirements of this chapter are baseline physical security and resiliency requirements for MC Facilities, LSP Facilities with MC Utilities/Systems Redundancies, and LSP facilities. LSP Facilities with MC Utilities/Systems Redundancies are to comply with requirements for LSP Facilities listed in this chapter. A risk assessment, during the project planning phase, can evaluate the deletion or incorporation of other specific requirements (see section 2.3 Exceptions and Deviations). The VA AHJ, defined in section 1.3 Administration and Enforcement, overseeing implementation of physical security and resiliency requirements for the facility will review submitted request for deviation from the baseline requirements of this chapter. When no risk assessment is performed, these baseline requirements apply.

The requirements of this chapter supplement other related VA standards for construction, space and facility planning criteria, design guides, design manuals, specifications, and details, which remain in full force and effect. Specifically, all requirements of VA Handbook 0730, Security and Law Enforcement, Appendix B, (which covers physical security requirements for VA

facilities), the VA Fire Protection Design Manual (which covers all VA construction), and ICT standards on the TIL remain in effect.

4.2 Public Entrances and Lobbies

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

4.2.1 Entrances

4.2.1.1 Public Entrances: All public entrances must have a point of physical control for all individuals entering the facility and a screening vestibule that can be used when VA requires individuals entering the building to pass through access control and screening prior to entering the building lobby.

Exception for Life-Safety Protected Facilities: Where the provisions for Public Entrances above cannot be achieved, the primary public entrance will be the main lobby of the facility and other public entrances must be kept to a minimum.

4.2.1.2 Staff Entrances: It is preferable to locate staff entrances independently of main entrance lobbies and to make them convenient to staff parking; provide staff-only entrances with access control, visual monitoring devices, and intrusion detection system.

4.2.2 Screening Vestibules

Screening vestibules are not the same as the typical entrance vestibules with inner and outer doors that served as a thermal barrier. The screening vestibule must have sufficient space and be provided with power, telecommunications, and data connections for installation of access control and screening equipment that can be used should the need arise. Configure access from the drop-off to the lobby through the screening vestibule to prevent circumvention of screening process. Arrange path of travel to prevent vehicular access beyond the standoff distance to the building perimeter. Provide sufficient size to accommodate several people with mobility aids.

The screening vestibule is one of two types: (1) independent of the main building, or (2) part of the main building near the entrance doors. The standoff distance for vehicles is measured to the main building façade whether the entry vestibule is an independent structure or within the main building.

4.2.2.1 Screening Vestibules as a Separate Lobby that is Independent of the Main Building: The preference is for the screening vestibule to be located outside of the main building footprint as a standalone structure, structurally isolated from the protected building, such that any damage to the vestibule will not impact the integrity of the main

building. When the screening vestibule is a standalone independent structure, the standoff requirements of Chapter 3, the façade requirements of Chapter 6, and the structural requirements of Chapter 7 are not applicable to the vestibule; however, laminated glass is to be used for all exterior glazing on the screening vestibule.

4.2.2.2 Screening Vestibule as a Part of the Main Building Lobby near the Entrance Doors: When the screening vestibule shares an internal wall or slab with the main building, the internal wall and slab must be protected from satchel and vehicle-borne explosive devices and must be designed as an exterior wall or slab per the requirements of Chapter 6 and Chapter 7. The blast hardening requirements of Chapter 6 and Chapter 7 do not apply to the exterior wall(s) of the main building lobby so that in case of a blast in the screening lobby, the force of the explosion will vent to the exterior. Standoff distances apply to the exterior walls.

4.2.3 Primary Public Entrances and Lobbies

4.2.3.1 Location: Standoff distances for unscreened vehicles must be in accordance with table 3-1.

4.2.3.2 Doors: Entrance doors to the lobby must be visible to or monitored by the security personnel in the main lobby; security personnel are to have the ability to control door operation from remote location. Blast resistance for doors must be in accordance with Chapter 6.

Exception for Life-Safety Protected Facilities: Security personnel are not required to have the ability to control door operation from a remote location.

4.2.3.3 Access within the Facility: Access from the lobby to elevators, stairways, and corridors that lead to restricted areas must be controlled using electronic access control or mechanical locking devices, limiting access to specific floors and areas that house functions requiring restricted access.

- Install card readers or other electronic access control devices at the entrances to restricted areas; devices to be located at entrances to suites and individual rooms from public corridors.
- Install elevator call (floor selection) buttons requiring use of key cards or other electronic access control to control access to restricted areas.

4.2.4 Access for Emergency Responders

Provide in accordance with Homeland Security (HLS) requirements and the TDM. At a minimum, install a PACS secured House Key Lock Box (HKLB) with standalone voice communications to the Facility's Police Control Room's (PCR) Security Management Control

Center (SMCC) Console whose operation and function is controlled and managed by the Security Management System (SMS). Locate the HKLB at an entrance door approved by the VA PM, OSP NCS O7A2, Security Personnel and Emergency Responders (suggested location is as close to the Facility's Fire Command Center (FCC) as possible). Ensure the HKLB is monitored by the Facility's Security Surveillance Video System (SSTV) that is controlled and managed by the Facility's SMS. Deliver the HKLB with PACS controlled and managed by the SMS. The FCC door must be monitored by the Facility's SSTV System with PACS controlled and managed by the SMCC. Ensure the FCC has an Emergency Responder Communications Box, in an easily available inside location, for homerun voice communications to the Facility's PCR SMCC. Contact OSP, NCS 07A2 (see TDM Paragraph 1.3 for contact information).

4.2.5 Planning, Construction Details, and Materials

4.2.5.1 Structural: Building entrances must be constructed to fail in a way that minimizes hazard to persons inside both MC and LSP facilities and supports continuity of operations of MC facilities after the failure. (See Chapter 6, Building Envelope and Chapter 7, Structural System, for additional requirements.)

- Protection of entrances and lobbies from vehicle ramming must be accomplished outside and in front of the entrance. (See section 3.5 Anti-Ram Rated Vehicle Barriers.)
- Where a covered drop-off area is provided, its supporting structure must be independent of the main building and protected from intentional and unintentional damage by vehicles. Protect supporting columns with anti-ram rated barriers and from explosive devices with architectural or structural finishes that prevent detonation within 6 inches (152 mm).
- Drop-off areas are not allowed beneath the VA facility footprint.

4.2.5.2 Façade: All glazing — both interior and exterior — in the lobby area must be laminated glass.

4.2.5.3 Doors and Hardware: Exterior doors must, in size, operation, and other characteristics, be in compliance with applicable regulatory requirements. Where doors are lockable, they must comply with emergency egress requirements. (Refer to Program Guide (PG-18-14) Room Finishes, Door, and Hardware Schedule, and Appendix A, Security Door Opening Matrix, for additional requirements.)

- Glass for entrance and egress doors must be laminated.
- Entrance doors must be capable of being remotely locked and unlocked from the reception desk in the main lobby, the Security Control Center (SCC), or other designated position.

- 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 must prevent unauthorized access.
- Residential facilities requiring 24-hour access must 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 to include either mechanical or electronic locks.

4.2.5.4 Receptacles: Letter boxes and receptacles for trash and smoking paraphernalia must not be located within 5 feet (1.5 m) of load-bearing elements. Those within 50 feet (15 m) of the building must be designed to prevent depositing of explosive charges or to contain explosions with a W0 charge weight (defined in the Physical Security Design Standards Data Definitions) as directed by the VA PM and coordinated with the structural engineer.

Exception for Life-Safety Protected Facilities: The standoff distance for letter boxes and receptacles for trash and smoking paraphernalia may be reduced from 50 feet (15 m) to 25 feet (7.6 m).

4.2.6 HVAC

Maintain positive pressure in lobbies and entrance areas. (Refer to Chapter 9, Building Systems, for requirements regarding relationship of air intakes to drop-off areas.)

4.2.7 Security

All public entrances require security monitoring. When screening is required 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.

Exception for Life Safety Protected Facilities: When screening is required**,** in lieu of creating a “hard line” in the screening vestibule, provide the means to restrict public access to those areas where screening is available.

4.2.7.1 Security Guard Stations: Guard stations must be located at building entrances available to the public. Guard stations must be located where pedestrian traffic can be monitored and controlled by security personnel. Where guard stations are located

outside, they are to be protected from weather and capable of being secured when not in use.

- Guard stations that are incorporated into an SCC must be separated from public areas with UL 752 Level 3 bullet resistant construction.
- Guard stations that are not incorporated into an SCC must be provided with a desk and capacity to communicate directly with the SCC.
- An intercom must be provided from the front door to the guard station reception desk and SCC.

Exception for Life Safety Protected Facilities: Security guard stations are not required.

4.2.7.2 Screening Devices: At all public entrances provide a screening vestibule with all required connections for temporary installation of metal detectors and package screening equipment and sufficient space for their installation and operation.

- 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.
- Screening devices must accommodate persons with disabilities.

4.2.7.3 Security Devices: SSTV cameras must be provided to monitor activities in the vestibules and lobbies and must be located to provide views of approaching pedestrian and vehicular traffic, drop-off areas, building entrances, and departing pedestrian and vehicular traffic.

4.2.8 Alteration/Renovation of Existing Facilities — Public Entrances and Lobbies

4.2.8.1 Covered Drop-off: Protect columns with anti-ram barriers such as bollards and from explosive devices by installation of architectural or structural finishes that prevent detonation within six (6) inches (152 mm).

4.2.8.2 Vestibules: Where space permits, provide an entrance vestibule of sufficient size to accommodate several people with mobility aids. Configure access from the drop-off to the lobby through the screening vestibule to prevent circumvention of screening process. Arrange path of travel to prevent vehicular access within the standoff distance to the building perimeter.

4.2.8.3 Glazing: All glazing — both interior and exterior — in the lobby area must be laminated glass or fitted with attached anti-fragmentation film.

4.2.8.4 Access within the Facility: Modify existing elevator call buttons to require electronic access control to register calls when elevators open directly into restricted areas; alternatively, construct secure vestibules at elevator lobbies on floors with restricted access.

4.2.8.5 Security Devices: SSTV cameras must be required and located in accordance with section 4.2.7.3 Security Devices.

4.2.8.6 Receptacles: Locate as per section 4.2.5.4 Receptacles.

4.3 Patient Drop-offs

Patient drop-offs must 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 must not be located under occupiable portions of the building or near staff-only entrances. A covered drop-off area that is connected to the primary public entrance by an enclosed walkway may be used; the walkway may be used as a screening vestibule. The drop-off area, canopy, and walkway are not considered part of the protected building structure when they are structurally independent of the building.

4.3.1 Vehicular Access

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

Exception for Life-Safety Protected Facilities: Separation between the building and the drop-offs and staging areas for vehicles may be reduced to 25 feet (7.6 m).

4.3.2 Parking

Parking is not permitted in patient drop-off areas; designated by pavement markings and signage.

4.3.3 Security

Provide SSTV cameras for general surveillance of the area.

4.3.4 Alteration/Renovation of Existing Facilities — Patient Drop-offs

Requirements for patient drop-offs are the same as in section 4.3.

4.4 Building Exits and Life Safety Considerations

Means of egress must not be obstructed by installation of security devices such as guard stations, screening equipment, or other security devices. All exits must comply with applicable codes and regulations.

4.4.1 Site Requirements

Provide an unobstructed and adequately lighted path from each exit to a safe location outside the building in accordance with NFPA 101. Dual light/bulb fixture must be used.

- 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 the anti-ram barriers or other similar devices.

4.4.2 Planning, Construction Details, and Materials

See Chapter 6 for blast requirements for the building envelope and doors.

4.4.3 Security Monitoring

Where exit doors do not also function as access points for the building, provide card reader and door status monitor for authorized users to indicate unauthorized use.

- Provide SSTV 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.

4.4.4 Alteration/Renovation of Existing Facilities — Building Exits and Life Safety Considerations

Requirements for building exits and life safety considerations are the same as in section 4.4.3 Security Monitoring.

5 FUNCTIONAL AREAS

This chapter discusses VA specific spatial functional areas, their relationships, and adjacencies based on physical security and resiliency requirements. These functional areas require enhanced protection when located in a MC Facility, LSP Facility, or LSP Facility w/ MC Utilities/Systems Redundancies.

As stated in Chapter 1, the requirements in this manual apply to new buildings, additions, and existing facilities undergoing renovations. Further clarification on applicability to renovation projects is provided in table 2-1 and in the gray box describing alteration/renovation of existing facilities at the end of each major section. Requirements modified for LSP facilities are specifically noted.

The requirements of this chapter are baseline physical security and resiliency requirements. A risk assessment during the project planning phase is allowed to evaluate the deletion or incorporation of other specific requirements (see section 2.3 Exceptions and Deviations). The VA AHJ, defined in section 1.3 Administration and Enforcement, overseeing implementation of physical security and resiliency requirements for the facility will review submitted request for deviation from the baseline requirements of this chapter. When no risk assessment is performed, these baseline requirements apply.

The requirements of this chapter supplement other related VA standards for construction, space and facility planning criteria, design guides, design manuals, specifications, and details, which remain in full force and effect. Specifically, all requirements of VA Handbook 0730, Security and Law Enforcement, Appendix B, (which covers physical security requirements for VA facilities), the VA Fire Protection Design Manual (which covers all VA construction), and ICT standards on the TIL remain in effect.

Adjacencies and separation requirements for certain functional areas are generally intended to protect against injury or contamination that might result from a blast or release of a hazardous material. They may also be used to protect the integrity of a functional area that must remain operational during and after an extreme event. For those functional areas that store valuable assets such as cash or drugs, adjacency requirements are also intended to protect those assets by making it easier to provide visual monitoring and intrusion detection. For example, Childcare/Development Centers are located in areas where the children can be monitored and protected from predators.

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, remains in full force and effect; the requirements of VA

Handbook 0730 Security and Law Enforcement, Appendix B, as they apply to fiscal services also applies; and, VA Program Guide PG-18-3, Design and Construction Procedures, applies.

5.1.1 Adjacencies

The Agent Cashier must not be located on an exterior wall. The transaction window must face a corridor or other public space, other than the primary public entrance.

5.1.2 Entrances

Access to the Agent Cashier space must be by a door to a corridor which is accessible only to employees of the facility; all doors to the Agent Cashier offices must be provided with audit trail capability.

5.1.3 Construction

The Agent Cashier space must be surrounded by construction that protects it from unauthorized entry.

5.1.3.1 Partitions and Openings: Partitions and teller windows facing spaces with unrestricted access must be UL 752 Level 3 ballistic and 15-minute forced entry resistant construction, including partitions, doors, glazed openings, teller windows, and transaction trays.

- All enclosing walls, floors, and ceilings must be of permanent construction and securely attached to each other; designed in such a manner as to provide visual evidence of unauthorized penetration.
- Partitions and walls must be reinforced, slab-to-slab, with 9-gauge expanded metal; the expanded metal must be spot welded every 6 inches (152 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.
- Pass-through devices must meet the same requirement for ballistics and forced entry protection.

5.1.3.2 Envelope Penetrations: All vents, ducts, and similar openings that enter or pass through an Agent Cashier space must be protected as required by Handbook 0730, Appendix B.

5.1.4 Security

Refer to Appendix B, Security System Application Matrix, for required devices. The items below provide additional guidance on how those devices are to be installed.

5.1.4.1 SSTV: The Agent Cashier space and the transaction window to be monitored by SSTV, and as required by the program.

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

5.1.4.3 Door: Entrance door must be controlled and monitored.

5.1.4.4 Records Storage: Refer to PSRDM section 5.14.

5.1.5 Alteration/Renovation of Existing Facilities — Agent Cashier

Requirements for Agent Cashier areas must comply with section 5.1 Agent Cashier.

5.2 Caches: All-Hazards Emergency Cache and Pharmacy Cache

All-Hazards Emergency Cache: Construction and physical security requirements for All-Hazards Emergency Caches are stated in VHA Directive 1047 as amended; unless more stringent requirements are stipulated below, these Caches must comply with Directive 1047.

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

5.2.1 Adjacencies

Caches located within the main facility must be on a corridor leading to the Loading Dock. The perimeter of the Cache enclosure must be no less than 50 feet (15 m) from the Loading Dock and from the Mailroom. Caches may be located in a separate building from the main facility on the VA facility site, subject to these requirements. They must not be located on an exterior wall and not be directly below a roof unless circumstances require that such a location be used; consult with the AHJ for additional requirements and security measures.

5.2.2 Entrances

Doors and frames to Caches must be opaque hollow metal, controlled as follows:

- Doors from the exterior and the interior must be protected against forced entry and be provided with monitoring devices and electronic access and egress control.
- Refer to PSRDM Appendix A.

5.2.3 Construction

Provide 15-minute forced-entry resistant construction; exterior construction must be reinforced masonry or equivalent.

5.2.3.1 Partitions and Openings: Interior partitions must comply with the following when separating a Cache from other building spaces, including corridors.

- All enclosing walls, floors, and ceilings must be of permanent construction and securely attached to each other; designed in such a manner as to provide visual evidence of unauthorized penetration.
- Partitions and walls must be reinforced, slab-to-slab, with 9-gauge expanded metal; the expanded metal must be spot welded every six (6) inches (152 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.
- When above or below an interstitial space, perimeter walls must extend through such interstitial floors.
- No windows, hatches, access panels, or skylights are permitted in Caches.

5.2.3.2 Envelope Penetrations: All vents, ducts, and similar openings that enter or pass through a Cache must be protected as required by Handbook 0730, Appendix B.

5.2.4 Security

Refer to Appendix B, Security System Application Matrix, for required devices. The items below provide additional guidance on how those devices are to be installed. Entrance doors to the Cache and vault doors, if any, within the Cache to be monitored by SSTV, controlled by physical access control, and monitored by intrusion detection system (both boundary and volumetric).

5.2.4.1 Intrusion Detection: Provide door and lock status sensors and motion detectors in Cache.

5.2.4.2 Access Control: Use card readers to control entry. Cypher locks are not acceptable.

5.2.4.3 Duress Alarm: Provide duress alarm at transaction counter.

5.2.4.4 SSTV: SSTV to be used at entry points, exit points, and service interaction areas.

5.2.4.5 Records Storage: Refer to PSRDM section 5.14.

5.2.5 Alteration/Renovation of Existing Facilities — Caches: All-Hazards Emergency Cache and Pharmacy Cache

Requirements for Cache areas must comply with section 5.2 Caches: All-Hazards Emergency Cache and Pharmacy Cache.

5.3 Childcare/Development Center

This section supplements Program Guide PG-18-9, Space Planning Criteria for VA Facilities, #420 Childcare/Development Center which remains in full force and effect. Childcare/ Development Centers must also meet the licensure requirements of the jurisdiction in which they are located, as well as the requirements of VA Handbook 0730 Security and Law Enforcement, Appendix B, as they apply. Comply with most stringent requirements.

5.3.1 Adjacencies

When located within a portion of a main VA facility, such as a hospital, Childcare/Development Centers must be located on the ground floor away from main building entrance with separate access area for drop-off and pick-up. The Childcare facility must also be remote from ambulatory care, Pharmacy, radiology, prosthetics, supply services, loading docks, mail rooms, agent cashier, fire department, and police operations and holding rooms.

5.3.2 Entrances

Provide a 2-way intercom at door(s) to the reception desk with remote door control from the desk.

5.3.2.1 Entrances: Doors to Childcare/Development Centers, including the main entrance and secondary entrances, must be controlled and monitored; access to be restricted to authorized personnel and guardians.

5.3.2.2 Exits: Exit doors from Childcare/Development Centers must be controlled and monitored.

5.3.2.3 Windows: Windows in Childcare/Development Centers must be protected from forced entry and monitored.

5.3.2.4 Vehicle barriers: Anti-ram vehicle barriers must be provided at main entrance area.

5.3.3 Construction

Enclose outdoor play areas with fences that prevent access by unauthorized persons and prevent children from leaving the designated area.

5.3.4 Security

Refer to Appendix B, Security System Application Matrix, for required devices. All entrances, including drop-off and pick-up areas, playgrounds, and other outdoor areas where children may be while at the Childcare/Development Center to be monitored by SSTV.

5.3.5 Alteration/Renovation of Existing Facilities — Childcare/Development Center

Entrances and security requirements for Childcare/Development Centers must comply with sections 5.3.2 Entrances, 5.3.3 Construction, and 5.3.4 Security.

5.4 Computer Room

This section applies to the Computer Room, as described in ICT standards on the TIL. In addition to the requirements of this section, NFPA 75 *Protection of Electronic Computer/Data Processing Equipment*, and the requirements of VA Handbook 0730 Security and Law Enforcement, Appendix B, must apply. This section provides mandatory supplementary requirements to the ICT standards on the TIL.

5.4.1 Adjacencies

The Computer Room must not be located in a high-risk area and located not closer than 50 feet (15 m) in any direction to main entrance, Loading Docks, personnel and package screening areas, uncontrolled parking, and Mailrooms, and in no case directly above or below such spaces.

5.4.1.1 Elevation: The Computer Room must be above grade and not below the water table, and not in the floodplain as defined in section 1.6.2 Facilities in Floodplains.

5.4.2 Entrances

Entrance doors to the Computer Room and other computer rooms must be controlled and monitored.

5.4.3 Construction

Extend surrounding walls and partitions from slab to slab.

5.4.3.1 Envelope Penetrations: All vents, ducts, and similar openings that enter or pass through the Computer Room to be protected as required by Handbook 0730, Appendix B.

5.4.4 Security

Refer to Appendix B, Security System Application Matrix, for required devices. All doors between the Computer Room and public space must have motion-activated SSTV camera

coverage on the computer room side of the door. The space must be controlled by physical access control and monitored by intrusion detection system (boundary only).

5.4.5 Alteration/Renovation of Existing Facilities — Computer Room

Existing Computer Rooms must comply with the requirements of section 5.4 Computer Room with the exception of the location restrictions. Consult with AHJ for additional requirements or mitigations to provide protection for the space in its existing location.

5.5 Emergency Department

This section supplements Program Guide PG-18-9, Space Planning Criteria for VA Facilities, #256, Emergency Department and Urgent Care Clinic.

5.5.1 Adjacencies

5.5.1.1 Vehicular Access: Only emergency (ambulances, law enforcement, and firefighter) vehicles and private vehicles that have been screened will be allowed within 50 feet (15 m) of the Emergency Department (ED) entrance. No vehicle will be allowed within five (5) feet (1.5 m) of the building structure. Install vehicle barriers as necessary to prevent such access.

5.5.1.2 Functional Adjacencies: Provide direct observation of the waiting room from the guard station and direct access through a controlled and monitored passage.

- Locate adjacent to Police Operations room or a satellite police station.
- Locate at least 50 feet (15 m) from Loading Docks, Mailrooms, main entrance lobbies, and personnel and package screening locations.
- Fixed facilities for patient decontamination (skid systems, smoking shelters that can be converted to include shower heads)

5.5.2 Entrances

Provide separate entrances for ambulatory patients and patients arriving by ambulance. Provide space for screening of pedestrians (See 5.5.4 Security).

5.5.2.1 Exterior Doors: Entrances from the exterior must be monitored.

5.5.2.2 Interior Entry Doors: Doors separating the Emergency (Urgent Care) Department area from the main building must be solid core wood or hollow metal and access controlled and monitored on both sides; doors may have laminated vision panels.

5.5.2.3 Exterior Entrances (Ambulance and Ambulatory): Glazing must be laminated glass or be provided with a shatter-resistant film to minimize injury by broken glass.

5.5.3 Construction

5.5.3.1 Anti-Ram Barriers: Refer to Chapter 3 and Chapter 7.

5.5.3.2 Façade: Refer to Chapter 6.

5.5.3.3 Construction Separation: Separate treatment area and nurses' station from waiting area, triage, and entrances with full height construction. Glazing in this separation must be laminated glass or be provided with a shatter-resistant film to minimize injury by broken glass.

5.5.4 Security

Refer to Appendix B, Security System Application Matrix, for required devices. The items below provide additional direction on how those devices are to be installed. Provide a guard station and direct connection to the Security Control Center (SCC), with capacity to screen patients, visitors, and packages at the ambulatory patient entrance.

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

5.5.4.2 SSTV: Provide SSTV monitoring of ED reception/waiting room and entrance from the exterior.

5.5.4.3 Duress Alarm: Provide duress alarm for receptionist, in areas such as the nurses station, triage, and as required by the program.

5.5.5 Alteration/Renovation of Existing Facilities — Emergency Department

Existing Emergency (Urgent Care) Departments must meet the requirements of section 5.5.2 Entrances, and also replace existing glass with laminated glass or install anti-fragmentation film on existing glass near the ED entrance.

Existing Emergency (Urgent Care) Departments must meet the requirements of section 5.5.4 Security.

5.6 Emergency and/or Standby Generator Room

VA facilities have electrical generators of varying criticality. Generator sets supplying power to the Essential Electrical System (EES) of health care facilities provide emergency power to Life Safety, Critical, and Equipment branches in accordance with codes and standards (e.g. NFPA 70,

Art. 517; and NFPA 99), with requirements of accreditation (e.g. Joint Commission requirements); and with VA policies (e.g. VHA Directive 1028). In some applications, electrical generators need only meet the requirements for "Legally Required Standby System" (e.g. NFPA Art. 700 and 701). In yet other applications, generators are being used for resiliency or (in some limited cases) for energy peak-shaving.

The use and application of a specific generator must be known when determining the level of physical protection to provide.

- Generators providing "Legally Required Standby Power" must be protected at the highest level of the designation being served (i.e., protect as a MC asset if serving a MC facility; protect as an LSP asset if it supports LSP functions).
- Generators not part of the EES that are providing only Standby or Backup power (e.g., to obtain 100% backup power to a facility) must be protected at the level of the function being supported. EXCEPTION: Self-enclosed (weather enclosure), skid-mounted generator sets are NOT required to meet hardening or stand-off distance requirements.
- In no case should the generator be protected at a level higher than the highest designated function being supported (i.e., a generator should not be treated as a MC asset if it *only* supports LSP or exempt facilities).
- Utility "quick connect" receptacles, switchgear, wiring, paralleling gear, transfer switches and associated components must be installed to facilitate temporary replacement of a generator.

See also the requirements in PSRDM Chapter 8, Utilities and Building Services, and Chapter 9, Building Systems. Refer to Chapter 6, Building Envelope, for blast protection requirements.

5.6.1 Adjacencies

Emergency and/or Standby Generators and related switchgear may be located in a separate structure from the main building or within the main building.

5.6.1.1 Elevation: The Generator Room must be above grade and not located in a high-risk area, below the water table, or in a floodplain as defined in section 1.6.2 Facilities in Floodplains.

5.6.1.2 Location in Building: When within a main building such as a medical center, the perimeter of the Generator Room cannot be located closer than 50 feet (15 m) of main lobbies, Loading Dock/receiving area, Mailrooms, or parking and cannot be located above or beneath such facilities.

Exception for LSP Facilities and LSP Facilities with MC Utilities/Systems Redundancies: Separation between the Generator Room and main lobbies, Loading Dock/receiving areas, Mailrooms, or parking may be reduced to 25 feet (7.6 m).

5.6.2 Entrances

5.6.2.1 Exterior Doors: Entrances from the exterior must not open to the Loading Dock service yard. Doors must be hollow metal and access controlled and monitored.

5.6.2.2 Interior Entry Doors: Entrances from the interior of the building must be hollow metal and must be access controlled and monitored.

5.6.2.3 Standby generators within manufactured enclosures must use stock doors which should be oriented, to the extent practicable, to not open towards loading dock, service yard, or other high-risk areas. Door must be monitored (unless technically infeasible).

5.6.3 Construction

5.6.3.1 Interior: The emergency and standby generators and related equipment must be surrounded by walls and partitions that extend from slab to slab.

5.6.3.2 Exterior: When installed outdoors, the emergency and/or standby generators and related equipment must be in a fenced enclosure and protected by passive barriers to prevent damage by vehicles.

5.6.4 Security

Generators operation and status will be monitored in the SCC as well as at the engineering control center. Refer to Appendix B, Security System Application Matrix, for required devices.

5.6.5 Alteration/Renovation of Existing Facilities — Emergency and/or Standby 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 must be performed, and mitigation measures of hardening or relocation be taken.

- Doors must be controlled, and generators be monitored as required by sections 5.6.2 Entrances and 5.6.4 Security.
- Louvered openings serving the generator must comply with requirements of Chapter 6 Building Envelope and Chapter 7 Structural System.

5.7 Energy Center/Boiler Plant

See also the requirements in PSRDM Chapter 8, Utilities and Building Services, and Chapter 9, Building Systems.

5.7.1 Adjacencies

The Energy Center/Boiler Plant may be located within a main building or in an independent building. When in an independent building, see Chapter 3 for site planning requirements.

5.7.1.1 Elevation: The Energy Center/Boiler Plant, including emergency and/or standby generators and switchgear, and engineering control center, and access to fuel tanks, must be above grade and cannot not be located in a high-risk area, below the water table or the floodplain as defined in section 1.6.2 Facilities in Floodplains.

5.7.1.2 Location in Building: When within a main building such as a medical center, the perimeter of the Energy Center/Boiler Plant must not be located closer than 50 feet (15 m) of a main lobby, Loading Dock/receiving area, Mailroom, childcare center, inpatient unit, Police Operations, or Fire or Incident Command Centers and must not be located above or beneath such facilities.

5.7.1.3 HVAC: In hurricane prone areas, louvers must be hurricane and debris impact resistant (refer to section 6.6). Areaways and louver openings serving the energy center/boiler plant must not open to the service yard for the loading dock and mailroom. Refer to Chapter 9 Building Systems for additional requirements.

5.7.2 Entrances

The Energy Center/Boiler Plant must not be entered from the service yard for the Loading Dock and/or Mailroom.

5.7.2.1 Exterior Doors: Doors must be hollow metal and access controlled and monitored.

5.7.2.2 Interior Entry Doors: Entrances from the interior of the building must be controlled and monitored.

5.7.3 Construction

The physical security and resiliency designation of the Energy Plant/Boiler Plant can vary. Refer to Table 1-5 for determination of designation and apply the requirements accordingly.

5.7.4 Security

Refer to Appendix B, Security System Application Matrix, for required devices.

5.7.5 Alteration/Renovation of Existing Facilities — Energy Center/Boiler Plant

Access to the Energy Center/Boiler Plant must be controlled and monitored as required by sections 5.7.2 Entrances and 5.7.4 Security.

Louver openings serving the Energy Center/Boiler Plant must comply with requirements of Chapters 6 and 7.

5.8 Fire Command Center (FCC)

When the Fire Command Center designated for use by emergency responders is provided, this section is applicable.

5.8.1 Adjacencies

Location of the Fire Command Center will be determined with the participation of the facility and emergency responders. It must be easily accessible in case of an emergency and readily identifiable from a distance of at least 50 feet (15 m).

5.8.2 Entrances

Entrance to the Fire Command Center must remain locked at all times; only emergency responders can have access to this room.

5.8.3 Construction

No additional physical security requirements.

5.8.4 Security

No additional requirements.

5.8.5 Alteration/Renovation of Existing Facilities — Fire Command Center

Fire Command Centers must meet the requirements of section 5.8 Fire Command Center.

5.9 Incident Command Center

5.9.1 Adjacencies

When provided, the Incident Command Center (ICC) will be located in an area of the facility (building or campus) that is easily accessible from all other parts of the facility and remote from high risk locations. Sufficient wall surface must be provided for wall-mounted monitors/display, marker boards, etc., to support ICC functions. Where possible, the ICC must have access to natural light and a view of surrounding areas. During normal conditions, without

incidents or other emergencies, the space may serve other functions, such as a conference room.

5.9.2 Entrances

Provide electronic access control at each entrance.

5.9.3 Construction

Surrounding construction must extend from floor slab to underside of slab above.

5.9.3.1 Communications: Communications and data connections must be provided with redundancy so that they can be rerouted when connections are lost.

5.9.3.2 HVAC: Heating, ventilating, and air conditioning systems must remain operational at all times.

5.9.3.3 Electrical and Communications: All circuits, data, communications, and other utilities serving the Incident Command Center must be backed by the standby electrical system. Refer to the VA Electrical Design Manual for specific loads to be connected to the EES. Communications and data connections must be provided with redundancy so that they can be rerouted if connections are lost. Besides on wall surfaces, provide sufficient electrical outlets in the floor under the conference table(s) to avoid having power cords stretching from wall outlets to the conference table.

5.9.4 Security

Incident Command Center must have secure storage facilities for communications devices and operational use supplies outfitted so that equipment is fully charged and ready to use when needed.

5.9.5 Alteration/Renovation of Existing Facilities — Incident Command Center

Incident Command Centers must meet the requirements of section 5.9 Incident Command Center.

5.10 Loading Dock and Service Entrances

5.10.1 Adjacencies

Loading Docks must be adjacent to, but structurally separate from, any VA facility.

5.10.1.1 Prohibited Adjacencies: Loading Docks cannot be located adjacent to or within 50 feet (15 m) of the following.

- Caches
- Central sterile processing and distribution
- Childcare/Development Centers
- Emergency Departments
- Emergency or Standby Generators
- Fire Command Center
- Flammable liquids or gas storage
- Incident Command Center
- Computer Room
- Main electrical switchgear
- Main utility service entrances
- Outdoor air intakes
- Patient care areas
- Pharmacy
- Security Control Center and Police Operations Room
- Water storage — domestic and fire

5.10.1.2 Coordination with Vivarium: Research animals and animal pathological waste must have separate Loading Dock facilities but may be served by the same service yard as the general Loading Dock.

5.10.2 Entrances

Pedestrian doors, stairs, and ramps associated with Loading Docks will be restricted to authorized personnel and be separated from the loading platform by not less than four (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.

5.10.2.1 Exterior Doors: Exterior pedestrian entrance doors and frames must be constructed of heavy-duty hollow metal and must be controlled and monitored.

5.10.2.2 Interior Entry Doors: Doors and frames from the receiving and breakout areas to the interior of the building must be accessed controlled and monitored.

5.10.3 Construction

5.10.3.1 Structural: When located within the main building, structural columns passing through the Loading Dock and floor slabs above it must be structurally hardened in accordance with the requirements of Chapter 7, Structural System.

5.10.3.2 Interior Partitions: The Loading Dock and receiving area must be separated from the corridors and spaces adjoining with walls constructed to meet the requirements of Chapter 7. Doors must be hollow metal construction and must be controlled and monitored.

5.10.3.3 Secured Storage: Provide secure storage areas for hazardous and pathological wastes, flammable storage, and full gas cylinders.

5.10.3.4 HVAC:

- Locate all outdoor air intakes at least 50 feet (15.2 m) horizontally and 30 feet (9.1 m) vertically from parking areas or on roof away from the roof line.
- Air from the Loading Dock and receiving areas shall not circulate to other parts of the building.
- The incoming mail and package screening rooms shall have a cut-off switch to shut off ventilation to the Loading Dock. Air serving the incoming packages and package screening rooms shall not circulate to other parts of the building."

5.10.4 Security

Refer to Appendix B, Security System Application Matrix, for required devices. The items below provide additional direction on how those devices are to be installed.

An area that is of sufficient size to conduct necessary inspections must be provided within the receiving area for inspection and imaging of goods received.

5.10.4.1 Guard Post: When a second guard post is provided for a building, it must 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 must be controlled and monitored.

- If at ground level, provide bollards for protection against vehicle ramming and comply with guard house construction and monitoring requirements as detailed in section 3.5.1.

5.10.4.2 Exterior: Install SSTV 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.

5.10.4.3 SSTV: The Loading Dock, including vehicles parked at the dock, must be monitored by SSTV.

5.10.4.4 Access Control: Dock lift controls and overhead door controls must be secured with a card reader device to prevent unauthorized use for entry.

5.10.5 Additional Requirements

Loading Docks must 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 SSTV.

5.10.5.1 Vehicle Access: Vehicle access to the Loading Dock must be restricted.

- Approaches to Loading Docks must be configured to limit the speed by any type of vehicle to 25 mph (40 kph).
- Where the entrance gate to a service yard is directly from a public right-of-way, deployable anti-ram rated vehicle barriers must be provided on the inside of the gate and 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.

5.10.5.2 Service Yards: The yard must be segregated from other vehicle and pedestrian traffic areas by screen walls.

- Delivery vehicle maneuvering and parking must 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 will be located within the enclosed service yard and under SSTV.

5.10.6 Alteration/Renovation of Existing Facilities — Loading Dock and Service Entrances

Loading Docks may remain in their original locations. Loading Docks must meet the requirements of section 5.10.3.2 Interior Partitions and service yards must be enclosed and meet the requirements of section 5.10.5.2 Service Yards. Loading Docks must meet the following:

5.10.6.1 Inspection Area: An area that is of sufficient size to conduct necessary inspections must be provided within the receiving area for inspection and imaging of goods received.

5.10.6.2 Structural Hardening: See Chapter 7 Structural System.

5.10.6.3 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 must be screened from public view and must be within a controlled access yard or area.

5.11 Mailroom

Adjacencies Mailroom, as used in the PSRDM, includes the suite of rooms for receiving, inspecting, sorting and distribution as well as handling of outgoing mail.

5.11.1 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.

5.11.1.1 Location: Mailrooms within the main building must be located on an exterior wall and may be adjacent to the Loading Dock.

5.11.1.2 Prohibited Adjacencies: Mailrooms cannot be located adjacent to or within 50 feet (15 m) of the following.

- Caches
- Central sterile processing and distribution
- Childcare/Development Centers
- Emergency Departments
- Emergency or Standby Generators
- Energy Center/Boiler Plant
- Fire Command Center

- Flammable liquids or gas storage
- Incident Command Center
- Computer Room
- Main electrical switchgear
- Main utility service entrances
- Outdoor air intakes
- Patient care areas
- Pharmacy
- Security Control Center and Police Operations Room
- Water storage—domestic and fire

5.11.1.3 Functional Separations: Unscreened incoming mail, whether from the U.S. Postal Service or a private carrier such as UPS or FedEx must be housed in a room that is separate from and exterior to outgoing mail.

5.11.2 Entrances

Subject to emergency exit safety requirements, all doors must be locked to prevent entry to the mailroom.

5.11.2.1 Exterior Doors: Exterior entrance doors and frames must be constructed of heavy-duty hollow metal and must be controlled and monitored. Refer to Chapter 6 Building Envelope for additional requirements.

5.11.2.2 Interior Entry Doors: Doors and frames from the Mailroom to the interior of the building must be access controlled and monitored.

5.11.3 Construction

When located within the main building, structural columns passing through the Mailroom and inspection area and floor slabs above them must be structurally hardened in accordance with the requirements of Chapter 7, Structural System.

5.11.3.1 Mailboxes: Mailboxes, when provided, must be in a separate room from the Mailroom and inspection area, and comply with the mounting heights and other regulations of the U.S. Postal Service.

5.11.3.2 Interior Partitions: The Mailroom must be separated from the mailbox room, corridors, and spaces adjoining with walls constructed to meet the requirements of

Chapter 7. Doors must be hollow metal construction and must be controlled and monitored.

5.11.3.3 HVAC:

- The air handling units serving the mail processing areas cannot serve other parts of the building.
- The incoming-mail room and package screening areas must have dedicated exhaust system and must maintain negative air pressure with respect to adjacent spaces. Air must not be recirculated. The exhaust must be filtered to prevent release of toxic elements into the atmosphere.
- Areas housing screened mail and outgoing mail must maintain positive pressure with respect to areas housing unscreened mail. The return air from those areas must not be recirculated.
- The incoming mail and package screening rooms must have a cut-off switch to shut off ventilation to the Mailroom. Air serving the incoming mail and package screening rooms must not circulate to other parts of the building.

5.11.4 Security

Refer to Appendix B, Security System Application Matrix, for required devices. The items below provide additional direction on how those devices are to be installed.

An area that is of sufficient size to conduct necessary inspections must be provided within the receiving area for inspection and imaging of mail received. This may be space shared with the Loading Dock inspection area.

5.11.4.1 SSTV: The Mailroom, including the inspection area and the exterior loading area serving the Mailroom, must be monitored by SSTV.

5.11.5 Additional Requirements

5.11.5.1 Separate Processing Area must include appropriate personal protection equipment (PPE) and disposal instructions for such equipment, as approved by the Centers for Disease Control and Prevention (CDC).

5.11.6 Alteration/Renovation of Existing Facilities – Mailroom

Mailrooms must comply with the requirements of section 5.11 Mailroom.

5.12 Pharmacy

In addition to the requirements of this section, Program Guide PG-18-9, Space Planning Criteria for VA Facilities, #268 Pharmacy Service, *Clinical Series Pharmacy Service VA Design Guide* and the *Primer Series Pharmacy Design Guide,* will remain in full force and effect; the requirements of VA Handbook 0730 Security and Law Enforcement, Appendix B, as they apply to pharmacies apply.

For the purposes of this section, "Pharmacy" refers to the main pharmacy, inpatient pharmacy, and outpatient pharmacy. Coordinate all Pharmacy requirements with those of Pharmacy Caches in section 5.2 Caches: All-Hazards Emergency Cache and Pharmacy Cache.

5.12.1 Adjacencies

Pharmacies cannot be immediately adjacent the Loading Dock or Mailroom or other high-risk areas.

5.12.2 Entrances

The Pharmacy must be accessed by a door to a corridor which is accessible only to employees of the facility. Entrance doors to the Pharmacy must be access controlled and monitored.

5.12.3 Construction

5.12.3.1 Exterior Walls: Construction must be reinforced masonry or equivalent. Exterior walls composed of metal or wood frame must have an interior backing of steel security screen mesh or steel sheet partition.

- Windows or skylights less than 18 feet (5.5 m) above adjacent finish grade, or the roof of a lower abutment, or less than 18 feet (5.5 m) from windows of an adjoining building, or accessible by a building ledge leading to windows of other floor rooms, must have forced entry resistant construction of ¾" (19 mm) #9 10-gauge[21] stainless steel woven security mesh that is securely anchored to the window frame and have intrusion detection alarm that annunciates in the Security Control Center.

[21] SCIF Construction Wall Type B, Suggested Construction for Expanded Metal. TECHNICAL SPECIFICATIONS FOR CONSTRUCTION AND MANAGEMENT OF SENSITIVE COMPARTMENTED INFORMATION FACILITIES VERSION 1.2, IC Tech Spec-for ICD/ICS 705, Office of the National Counterintelligence Executive, April 23, 2012 (https://fas.org/irp/dni/icd/ics-705-ts).

5.12.3.2 Interior Construction: Interior partitions between the Pharmacy and surrounding spaces must be 15-minute forced entry resistant construction and extend from slab to slab.

- All enclosing walls, floors, and ceilings must be permanently constructed and securely attached to each other; they must be designed in such a manner as to provide visual evidence of unauthorized penetration.
- Partitions and walls must be reinforced, slab-to-slab, with 9-gauge expanded metal; the expanded metal must be spot welded every six (6) inches (152 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.
- When above or below an interstitial space, perimeter walls must extend through such interstitial floors.

5.12.3.3 Dispensing Partitions and Openings: Partitions, doors, glazed openings, teller windows, and transaction trays at dispensing windows must be UL 752 Level 3 ballistic construction and 15-minute forced entry resistant construction.

5.12.3.4 Envelope Penetrations: All vents, ducts, and similar openings that enter or pass through a Pharmacy must be protected as required by Handbook 0730, Appendix B.

5.12.4 Security

Refer to Appendix B, Security System Application Matrix, for required devices. The items below provide additional direction on how those devices are to be installed.

Provide SSTV monitoring of Pharmacy dispensing area, vault entrance, and controlled substance storage.

5.12.4.1 Intrusion Detection: Provide door and lock status sensors and motion detectors in Pharmacy. When the Pharmacy is in continuous operation, volumetric intrusion detection is not required.

5.12.4.2 Access Control: Pharmacy entry and narcotic vaults must be controlled via card readers. Mechanical cypher locks cannot be used.

5.12.4.3 Duress Alarm: Provide duress alarm at patient transaction counter and patient/pharmacist consult areas, and as required by the program.

5.12.4.4 SSTV: SSTV must be used at entry points, exit points, service interaction areas and windows, and waiting areas.

5.12.4.5 Records Storage: Refer to PSRDM section 5.14.

5.12.5 Alteration/Renovation of Existing Facilities — Pharmacy

Pharmacies must comply with the requirements of section 5.12.4 Security.

5.13 Police Operations Room and Holding Room

This section supplements the following documents which must remain in full force and effect: Program Guide PG-18-9, Space Planning Criteria for VA Facilities, #279 Police Service, and VA Handbook 0730 Security and Law Enforcement that is in effect at the time the PSRDM is published.

5.13.1 Adjacencies

5.13.1.1 Police Operations Room: 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 department, or main lobby and located to enable appropriate response and deployment to respond to a security related event.

5.13.1.2 Holding Room: Located within or adjacent to the Police Operations Room; an additional Holding Room may be located within or adjacent to a perimeter screening facility.

5.13.1.3 Desirable Separations: Domiciliary, substance abuse, and Veterans assistance facilities cannot be located near the Police Operations Room.

5.13.2 Entrances

5.13.2.1 Police Operations Room: Doors must be from a corridor used only by staff and must be controlled and monitored.

5.13.2.2 Holding Room: Doors and frames must be heavy gauge hollow metal steel construction and door hardware must be protected with 15-minute forced entry resistant construction, meet the ballistic resistance requirements of UL 752 Level 3 and be controlled and monitored.

5.13.3 Construction

5.13.3.1 Police Operations Room: When the Police Operations Room is adjacent to or opens onto areas occupied by unscreened public, such as main lobbies, elevator lobbies, Emergency Departments, and public corridors, all construction, including partitions from slab to slab, doors, windows, and other openings separating the unit from such spaces, must be UL 752 Level 3 ballistic-resistant with 15-minute forced entry resistant construction.

5.13.3.2 Holding Room: Construction of the Holding Room must be protected with 15-minute forced entry resistant construction and meet the ballistic resistance requirements of UL 752 Level 3 and as follows:

- Walls constructed of reinforced masonry extended to the underside of the structure above; gypsum board and steel stud construction cannot be used.
- Door frames must be grouted solid and anchored into the masonry walls.
- An observation window consisting of reflective glass protected by clear polycarbonate must be provided.
- The interrogation table must be firmly anchored to the floor and to one wall, or firmly anchored to the floor.
- Shackle hasps must be anchored to wall construction and be capable of resisting pullout of not less than 1000 pounds (228 kg).
- Provide anti-ligature construction.
- Vandal resistant products must be used within the space; all exposed fasteners must be tamper resistant.
- Construction and materials must eliminate opportunities for detainee to inflict self-injury and improvise weapons that could be used to harm others.

5.13.3.3 HVAC: Heating, ventilating, and air conditioning systems must remain operational at all times.

5.13.3.4 Electrical and Communications: All circuits, data, communications, and other utilities serving the Police Operations Room must be backed by the emergency/standby electrical system. Refer to the VA Electrical Design Manual for specific loads to be connected to the EES.

5.13.4 Security

Refer to Appendix B, Security System Application Matrix, for required devices. The items below provide additional direction on how those devices are to be installed.

SSTV surveillance of the entire Holding Room must be provided through an opening glazed with transparent polycarbonate in a steel frame firmly anchored to the wall. When requested by the VA PM, the SSTV camera will be covert and use lenses made for the purpose.

5.13.4.1 Records Storage: Refer to PSRDM section 5.14.

5.13.5 Alteration/Renovation of Existing Facilities — Police Operations Room and Holding Room

Police Operations Rooms and Holding Rooms that open directly to other parts of the building, including corridors and elevator lobbies, partitions and control doors must be constructed to separate the lobby as required by sections 5.13.2 Entrances, 5.13.3 Construction, and 5.13.4 Security.

5.14 Records Storage and Archives

Records Storage rooms must 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 must comply with the requirements of the PSRDM section 5.4 Computer Room.

5.14.1 Adjacencies

Records Storage and Archives rooms must not be located nearer than 50 feet (15 m) in any direction from main entrance lobbies, Loading Docks, Mailrooms, and other high-risk areas and in no case directly above or below such spaces.

5.14.2 Entrances

Entrances to archival storage spaces, including book stacks, computer main frames, and valuable or historical records and collections must be controlled and monitored. Emergency egress doors from archival storage spaces must be controlled and monitored and have motion-activated SSTV camera coverage of the egress side of the door with all device monitors at a central location within the archival or library area.

5.14.3 Construction

No additional physical security requirements.

5.14.4 Security

Refer to Appendix B, Security System Application Matrix, for required devices.

Archives for rare and valuable artifacts and documents must be provided with intrusion detection and SSTV. SSTV will not record protected health information. The intrusion detection system must provide boundary and volumetric protection. This space must be controlled via a card reader.

5.14.5 Alteration/Renovation of Existing Facilities — Records Storage and Archives

Records Storage and Archive facilities must comply with sections 5.14.2 Entrances and 5.14.4 Security.

5.15 Research Laboratory and Vivarium

This section supplements Program Guide PG-18-9, Space Planning Criteria for VA Facilities, #278 Research and Development, which will remain in full force and effect. The most current requirements of VHA Handbooks 1200.8 and 1200.6 and BSL Research Lab Physical Security Inspections requirements will remain in effect. The requirements of Laboratory Security and Emergency Response Guidance for Laboratories Working with Select Agents (CDC Biosafety in Microbiological and Biomedical Laboratories (BMBL) most current Edition) apply to facilities storing and handling select agents. (Select agents are as defined in Title 42, CFR, Part 73, including pathogens and toxins regulated by both HHS and USDA and non-overlap select agents of HHS.) Veterinary Medical Unit Vivarium spaces must comply with AAALAC accreditation requirements. The requirements of VA Handbook 0730 Security and Law Enforcement, Appendix B, also apply.

5.15.1 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.

5.15.1.1 Shared Occupancy: When located within a building with other occupancies, the Research Laboratory must be located on a corridor restricted to authorized employee use.

5.15.1.2 Select Agents: Laboratories and other facilities using select agents must not be located closer than 50 feet (15 m) from public lobbies, Mailrooms, Loading Docks, or other functional areas identified in Chapter 5.

5.15.1.3 Animal Facilities: The distance between Research Laboratories housing animals and patient care and residential facilities must be maximized to ensure that noise and odors do not reach those receiving services.

5.15.2 Entrances

Research Laboratory and Vivarium entrances must be located away from public areas.

5.15.2.1 Exterior Doors: Entrances to the Research Laboratory and Vivarium from the exterior of a building must be controlled and monitored.

- Entrance doors to Vivariums must be UL 752 Level 3 ballistic resistant and 15-minute forced entry resistant.
- Emergency egress doors from Research Laboratory and Vivarium spaces must be access controlled and monitored. The door must be covered by SSTV camera (recording only) from the Vivarium side and must be UL 752 Level 3 ballistic resistant and 15-minute forced entry resistant.
- Entrances used for delivery of animals and toxic chemicals must be in discreet locations and monitored by SSTV.

5.15.2.2 Interior Entry and Emergency Egress Doors: Entrances to the Research Laboratory and Vivarium from other than Laboratory or Vivarium uses of a building must be controlled and monitored and must be UL 752 Level 3 ballistic resistant and 15-minute forced entry resistant.

- Emergency egress doors from Laboratory and Vivarium spaces must be controlled, monitored, and covered by SSTV camera (recording only) from the Laboratory or Vivarium side.
- Doors to rooms containing select agents must be biometric access controlled and monitored.
- All Research Laboratory and laboratory “neighborhood” doors from public corridors accessible to all building occupants (such as those used for emergency egress) must be electronic access controlled and monitored.
- All doors from public corridors to shared support rooms such as cold rooms, dark rooms, instrument rooms, autoclave rooms, ice machines, and other equipment must be electronic access controlled and monitored.
- Doors to any room used to store radioactive waste, ongoing experiments using radioactive materials, or similar use of radioactive materials must be electronic access controlled and monitored.
- Doors to irradiator facilities must be electronic access controlled and monitored.
- Entries to the containment area for BSL-3 facilities must be electronic access controlled and monitored.
- Doors between “dirty” corridors and “clean” corridors must be provided with a sensor and alarm at a central point in the Research Laboratory or Vivarium, as

well as a local alarm and annunciator, when such door is left open longer than 18 seconds.

5.15.2.3 Elevator Entrances: Control of elevator access opening directly into the Vivarium must be by card reader device in the elevator cab, or, where the elevator is dedicated to Vivarium use, at any landing from which the elevator can be called. The elevator entrance door at the Vivarium must be monitored by a SSTV camera in the space looking at the entrance.

5.15.3 Construction

5.15.3.1 Exterior Walls: Construction must be reinforced masonry, or equivalent. Exterior walls composed of metal or wood frame must have an interior backing of steel security screen mesh or steel sheet partition.

- Windows or skylights less than 18 feet (5.5 m) above adjacent finish grade or the roof of a lower abutment, or less than 18 feet (5.5 m) from windows of an adjoining building, or accessible by a building ledge leading to windows of other floor rooms, must have forced entry resistant construction of ¾" (19 mm) #9 10-gauge stainless steel woven security mesh that is securely anchored to the window frame and must have an intrusion detection alarm that annunciates in the Security Control Center.

5.15.3.2 Interior Construction: Interior partitions between the Research Laboratory and Vivarium and surrounding spaces must be 15-minute forced entry resistant construction and extend from slab to slab.

- All enclosing walls, floors, and ceilings must be permanently constructed and securely attached to each other; they must be designed in such a manner as to provide visual evidence of unauthorized penetration.
- Partitions and walls must be reinforced, slab-to-slab, with 9-gauge expanded metal; the expanded metal must be spot welded every six (6) inches (152 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.
- When above or below an interstitial space, perimeter walls must extend through such interstitial floors.

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

- Walls, floor, and ceiling must be permanently constructed and securely attached to each other.

- All construction must be designed in such a manner as to provide visual evidence of unauthorized penetration.
- Partitions and walls must be reinforced, slab-to-slab, with 9-gauge expanded metal; the expanded metal must be spot welded every six (6) inches (152 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.

5.15.3.4 Envelope Penetrations: All vents, ducts, and similar openings that enter or pass through a Research Laboratory or Vivarium must be protected as required by Handbook 0730, Appendix B.

5.15.3.5 HVAC: Air serving the BSL-3 laboratory, vivarium, radioactive storage, select agent storage, and laboratories shall not circulate to other parts of the building.

5.15.3.6 Power: All equipment, including mandated services and systems (e.g. refrigerators, freezers, vivarium environmental controls) in the Research Laboratory and Vivarium, must be backed up by the emergency/standby electrical system and UPS equipment.

5.15.4 Security

Refer to Appendix B, Security System Application Matrix, for required devices. The items below provide additional direction on how those devices are to be installed.

5.15.4.1 SSTV: BSL-3 Laboratories and Vivariums must have SSTV coverage of internal laboratory spaces which will be monitored by personnel within the containment area

- SSTV cameras must be placed to monitor any Loading Dock or other animal receiving area when not already monitored as a part of a general loading/receiving area as provided in this chapter.
- All SSTV coverage of access to areas surrounding the containment area must be monitored in the SCC.

5.15.4.2 Intercom: An intercom must be provided at each entrance door to a designated office or workstation in BSL-3 Laboratories or Vivariums.

5.15.4.3 Biometric: In conjunction with an access control card reader, a biometric identity verification device must be provided at the entrance to the BSL-3 anteroom. When the biometric device is placed at the door from the anteroom to the BSL-3 Laboratory, it must be functional for personnel in biosafety garments using contactless method to verify identity (such as, iris or facial recognition not hand geometry or fingerprint device).

5.15.4.4 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"), must only be permitted by written authorization of the VA PM with concurrence from the Chief Officer, VHA Office of Research Oversight.

5.15.4.5 Alarms: Provide audible local alarms at each door that has an access control device. Provide duress alarms in each BSL-3 Laboratory and Vivarium.

5.15.4.6 Records Storage: Refer to PSRDM section 5.14.

5.15.5 Additional Requirements for Select Agent Storage

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

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

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

5.15.6 Alteration/Renovation of Existing Facilities — Research Laboratory and Vivarium

Research Laboratories (BSL-3) and Vivarium must comply with the requirements of sections 5.15.2 Entrances, 5.15.3.1 Exterior Walls (forced entry resistant security mesh), and 5.15.4 Security.

5.16 Security Control Center

This section addresses the application, monitoring, control, programming, and interface of the Security Control Center (SCC) with all security subsystems: Electronic Security System (ESS), Physical Access Control System (PACS), Intrusion Detection System (IDS), Security Surveillance Television (SSTV), Duress, Security Phones, and Intercom System (DSPI), and Detection and Screening System (DSS). Additional requirements for the equipment (see Chapter 10) must be coordinated with the fundamental planning concepts and criteria associated with the SCC design and security console operating environment covered in this section.

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 must remain in full force and effect.

5.16.1 Adjacencies

The SCC must be readily accessible to authorized personnel, inconspicuous, and located in areas not frequented by the general public, and must contain office space, support space, and monitoring equipment that is not visible to unauthorized personnel. The security consultant must review the proposed location to ensure it is free from other high-risk activities.

5.16.1.1 Fire Command Center (FCC): When an FCC is provided, the SCC must be near the FCC, but not be accessible to persons using the FCC.

5.16.1.2 Police Operations Unit: The SCC may be connected to the Police Operations unit, but the two areas must be served by separate entrances and each area must be fully functional without requiring access to the other.

5.16.1.3 Back-up SCC: Where provided must be at a remote location from the primary SCC and meet the requirements of section 5.16 Security Control Center.

5.16.1.4 Main Lobby: The SCC containing monitoring devices and security personnel cannot be adjacent to the main public lobby.

5.16.1.5 Holding Room: The SCC cannot include a Holding Room.

5.16.1.6 Prohibited Adjacencies: The SCC cannot be located closer than 50 feet (15 m) to a Loading Dock, Emergency Department, critical utilities, Mailroom, or other high-risk operations or functions.

5.16.1.7 Desirable Separations: Domiciliary, substance abuse, and Veterans assistance, and childcare facilities must not be located near the Security Control Center.

5.16.2 Entrances

The SCC must be entered from a corridor beyond the control doors leading out of the main lobby to the building interior. The SCC must have a security vestibule with a mantrap configuration.

Doors to the SCC must be UL 752 Level 3 ballistic resistant and 15-minute forced entry resistant, access controlled, and monitored.

5.16.3 Construction

5.16.3.1 Partitions: The SCC must be fully enclosed with UL 752 Level 3 ballistic construction, including partitions, doors, and glazed openings.

- All enclosing walls, floors, and ceilings must be permanently constructed and securely attached to each other; they must be designed in such a manner as to provide visual evidence of unauthorized penetration.

- Partitions and walls must be reinforced, slab-to-slab, with 9-gauge expanded metal; the expanded metal must be spot welded every six (6) inches (152 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 must be built from floor slab to ceiling slab or construction and sealed to an air-tight condition.

5.16.3.2 Envelope Penetrations: All vents, ducts, and similar openings that enter or pass through a Cache must be protected as required by Handbook 0730, Appendix B.

5.16.3.3 HVAC:

- HVAC serving the SCC must be independent of the system(s) serving the main lobby.
- The air quality and temperature within the SCC must allow for a comfortable work environment for both personnel and the security equipment. Ventilation controls must also be provided on a separate air handling system that provides an isolated supply and return system.

5.16.3.4 Power:

- All equipment in the SCC must be backed by the emergency/standby electrical system and UPS equipment.

- **5.16.3.5 Security System Equipment and Interface:** The SCC must 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 must be identified to support the SCC should it become inoperable. All security subsystems must be fully integrated by either direct hardwiring of equipment or a computer based electronic Security Management System (SMS). The SCC must house all attended equipment primary power sources for each security subsystem, such as DVRs and monitors. Normally unattended equipment, such as servers, must be located in the Computer Room.
  - The SCC and security console must 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 standalone versus shared space requirements with another telecommunication space.

- Equipment locations, such as wall space for new and upgraded security systems equipment must 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 must be addressed.
- All equipment that is rack mounted or installed in a security console must be clearly labeled as to its identification. Labeling, such as in the case of SSTV monitors, may be programmed with a message embedded or programmed on the monitoring screen.

5.16.4 Physical Security

Refer to Appendix B, Security System Application Matrix, for required devices. The items below provide additional direction on how those devices are to be installed.

The SCC must have physical security safeguards. The main entry door must 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 SSTV 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 is prohibited.

5.16.5 Primary and Secondary Locations

The SCC must be located in an area that is within the first level of security defense defined by VA. The SCC must also be located above grade and above any potential flood areas, such as basement (refer also to section 1.6.2 Facilities in Floodplains).

5.16.5.1 Location: The SCC must be located in an area free of background noise influences that could impact equipment and SCC operations. To prevent potential compromise of operations and to ensure continued protection and support of patient and staff health and safety, the SCC must 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.

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

5.16.6 Space Requirements

The size of the SCC is 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 must meet the requirements of PG-18-13, Barrier Free Design Guide, 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 unless more stringent requirements have been established by the Architectural Barriers Act Accessibility Standard (ABAAS). Floor area planning decisions will depend upon the number of console positions, size of the facility, and overall architecture of the ESS. Centralized architecture, where all video recording is located within the security equipment room (SER), will require additional space versus decentralized architecture. As a general rule, the SER will be a minimum of 50 percent of the overall SCC size, at a minimum 90 square feet (8.4 m^2) for a small SCC. Future expansion of the SCC and security console equipment requirements must be anticipated and may be accommodated through use of modular furniture.

5.16.6.1 Configuration: The SCC will have two core spaces, the SCC itself and the security equipment room (SER). The SCC must consist of a monitoring function (for example, ESS monitors, communications devices, fire alarm). The SER must consist of supportive equipment (video storage devices, data transmission systems/media, and others) that is not monitored. Servers will be located within the Computer Room.

- Security equipment room (SER) will serve as the supporting equipment room for the SCC and designed with sufficient space to accommodate 100 percent system growth. The SER layout must follow ICT standards on the TIL. Computer racking must be centered in the room, permitting access doors to be opened on all sides. Maintain minimum required electrical code distances from the UPS and wall-mounted enclosures and devices. Cooling must be maintained throughout power outages.
- Security equipment closet (SEC) must follow VA OIT Design Standards and share space in the Telecommunication Room. SEC must have a defined space and be physically separated per the OIT standard. Where security equipment will be wall mounted, a 0.75-inch (19 mm) fire-rated plywood (or comparable material) must cover the wall. Where security equipment will be rack mounted, provide securable security equipment cabinets. All incoming and outgoing conduit must terminate/originate at metal wire troughs mounted above the security equipment cabinets or racks. All equipment mounting conditions must include dedicated horizontal and vertical wire and cable management systems.

5.16.6.2 Small SCC: A small SCC will contain no more than four security console bays. 150 to 300 square feet (14 to 30 m²) of space must be provided for a small to medium size SCC operation. The small SCC is commonly associated with facilities or campuses with facilities between 150,000 to 300,000 GSF (14,000 to 28,000 m²). The SER must be not less than half the size of the SCC and no smaller than 90 square feet (8.4 m²). Facilities smaller than 150,000 GSF (14000 m²) will be monitored by the VISN SCC.

5.16.6.3 Large SCC: A large SCC will contain no less than five and no more than eight security console bays. For large SCC operating environments, a minimum of 500 square feet (46.5 m²) of space must be provided. The SER cannot be not less than half the size of the SCC and no smaller than 180 square feet (16.7 m²).

5.16.6.4 Back-up or Secondary SCC: Area requirements for a back-up SCC must be based on what ESS systems will be monitored.

5.16.7 Operational Requirements

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

5.16.7.1 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.

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

5.16.7.2 Accessibility: The SCC must be fully accessible to persons with disabilities.

5.16.8 Alteration/Renovation of Existing Facilities — Security Control Center (SCC)

Where the existing SCC does not meet the requirements of section 5.16 Security Control Center, a secondary SCC that complies with the requirements of section 5.16.5.2 Secondary SCC must be provided.

5.17 Storage of Hazardous Materials

For the purposes of this chapter, "hazardous materials" refers to bio-hazard waste, medical gases (liquid and gaseous), fuel, radioactive materials, and select agents. These materials may also be referred to as Hazmat. The requirements of this section are in addition to those stated elsewhere in this manual, other VA design guides, the requirements of regulatory agencies having jurisdiction, and the requirements of VA Handbook 0730 Security and Law Enforcement, Appendix B.

5.17.1 Adjacencies

5.17.1.1 Bio-Hazard Waste: Limit storage of bio-hazard waste to 30 gallons (115 liters) in normally occupied spaces other than trash collection areas. Provide for local collection points on each floor and building-wide collection area near the Loading Dock to allow for pick-up and removal of hazardous wastes from the site. (Note: This is not acceptable for radioactive or select agents or fuel.)

5.17.1.2 Medical Gases: Tank farms must be separated from occupied portions of buildings as required by NFPA 50 and NFPA 99. Portable tanks and manifolded tanks must be located as remotely as possible from exits and exit access corridors.

5.17.1.3 Fuel: Fuel must not be stored or collected awaiting disposal inside any building.

5.17.2 Entrances

Hazardous Materials Storage rooms must be accessed from corridors that are accessible only to employees of the facility.

5.17.3 Construction

5.17.3.1 Exterior Walls: Construction must be reinforced masonry or equivalent. Exterior walls composed of metal or wood frame must have an interior backing of steel security screen mesh or sheet metal partition.

- Windows or skylights less than 18 feet (5.5 m) above adjacent finish grade or the roof of a lower abutment, or less than 18 feet (5.5 m) from windows of an adjoining building, or accessible by a building ledge leading to windows of other floor rooms, must have forced entry resistant construction of ¾" (19 mm) #9 10-gauge stainless steel woven security mesh that is securely anchored to the window frame and must have intrusion detection alarm that annunciates in the Security Control Center.

5.17.3.2 Partitions and Openings: Interior partitions must comply with the following when separating a Cache from other building spaces, including corridors.

- All enclosing walls, floors, and ceilings must be permanently constructed and securely attached to each other; they must be designed in such a manner as to provide visual evidence of unauthorized penetration.
- Partitions and walls must be reinforced, slab-to-slab, with 9-gauge expanded metal; the expanded metal must be spot welded every six (6) inches (152 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.
- When above or below an interstitial space, perimeter walls will extend through such interstitial floors.

5.17.3.3 Envelope Penetrations: All vents, ducts, and similar openings that enter or pass through a Cache must be protected as required by Handbook 0730, Appendix B.

5.17.4 Security

Refer to Appendix B, Security System Application Matrix, for required devices.

5.17.4.1 Records Storage: Refer to PSRDM Section 5.14.

5.17.5 Alteration/Renovation of Existing Facilities — Storage of Hazardous Material

Storage Hazardous Material Storage must comply with section 5.17 Storage of Hazardous Material.

6 BUILDING ENVELOPE

6.1 Scope, Purpose, and Goals

This chapter provides requirements for exterior walls other than load bearing walls; glazed façade fenestration (including windows and doors) and glazed atria; for roof structures, including skylights; and air intakes and exhausts servicing 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. Although the design to resist one extraordinary loading does not necessarily provide adequate protection in response to another extraordinary event, the basic requirements for ductility, redundancy, and robustness will contribute to the occupants' safety in response to a wide range of hazards and unforeseen events.

All building components requiring blast resistance must be designed using established methods and approaches for determining dynamic loads, structural detailing, and dynamic structural response. Designers must apply dynamic methods of analysis to demonstrate compliance with this requirement. Alternative analysis and mitigation methods are permitted, provided that the performance level is attained, and approval is granted by the VA AHJ.

As stated in Chapter 1, the requirements in this manual apply to new buildings, additions, and existing facilities undergoing renovations. Further clarification on applicability to renovation projects is provided in Table 2-1 and in the gray box describing alteration/renovation of existing facilities at the end of each major section.

The requirements of this chapter are baseline physical security and resiliency requirements for MC Facilities, LSP Facilities with MC Utilities/Systems Redundancies, and LSP facilities. LSP Facilities with MC Utilities/Systems Redundancies are to comply with requirements for LSP Facilities listed in this chapter. A risk assessment during the project planning phase is allowed to evaluate the deletion or incorporation of other specific requirements (see section 2.3 Exceptions and Deviations). The VA AHJ, defined in section 1.3 Administration and Enforcement, overseeing implementation of physical security and resiliency requirements for the facility will review submitted request for deviation from the baseline requirements of this chapter. When no risk assessment is performed, these baseline requirements apply.

The requirements of this chapter supplement other related VA standards for construction, space and facility planning criteria, design guides, design manuals, specifications, and details, which remain in full force and effect. Specifically, all requirements of VA Handbook 0730, Security and Law Enforcement, Appendix B, (which covers physical security requirements for VA

facilities), the VA Fire Protection Design Manual (which covers all VA construction), and ICT standards on the TIL remain in effect.

In order to meet the physical security and resiliency requirements of this manual, the design team must include security subject matter experts as per section 1.8 Requirements for Subject Matter Specialists. The qualifications required for the licensed professional structural engineer who has specialized training in blast design and analysis (structural blast specialist) are included in section 6.1.1 below.

6.1.1 Blast Specialist Requirements

At a minimum, the structural blast specialist must be a registered Professional Engineer having a bachelor's degree in structural engineering or a related field and have formal training in structural dynamics and demonstrated experience with the accepted design practices for blast resistant design. The specialist must have a minimum of five years' experience in performing dynamic analysis in blast resistant design. The résumé of the specialist must be submitted to VA for review and approval prior to the concept phase of the project. The résumé must include a minimum of three projects during the previous two years with similar scope to the project being designed. The qualifications of the firm for whom the specialist works must also be submitted to VA for review and approval.

6.1.2 Explosive Weights and Calculation of Blast Loads

The magnitudes of W1, GP1, and GP2 are defined in the Physical Security and Resiliency Design Standards Data Definitions, a document separate from this Manual. It is provided on a need-to-know basis to the structural blast specialist performing analysis and design of VA projects (See Chapter 6 Annex for additional information regarding request of the Data Definitions by subcontractor/vendors). Authorized users can contact the VA Office of Construction and Facilities Management (CFM) to request the document. The Data Definitions is security sensitive and protected/controlled and must be guarded against disclosure.

Unless otherwise specified, for building envelope, the calculated blast loads are defined to be the peak pressures and impulse resulting from the design level threat located at the minimum specified standoff distances at the base of the building and vertical elevation (taking into account building setbacks, etc.), as appropriate, as limited by the GP values where applicable. Horizontal standoff provided in excess of the minimum standoff distances may only be accounted for in the calculation of the blast loading environment when land use agreements by the local VA facility's authority and the AHJ (see section 1.3 Administration and Enforcement) are in effect to prevent relocation of roadways or parking any closer than their current location.

6.1.3 Exempted Structures

Buildings of type V construction (specifically light-frame wood and cold-formed steel framing structure) are exempt from building envelope blast-resistant design requirements in Chapter 6. However, laminated glass must be used for fenestration and atria. For insulated glazing units, the interior light of glass is to be laminated. For existing facilities, a daylight application of 7-mil anti-shatter film must be applied to existing windows.

Exterior stairwells (enclosed or exposed) and covered or enclosed walkways exterior to the building envelope may be excluded from blast-resistant design of LSP and MC buildings when a continuous hardened façade is provided. See Chapter 6 Annex for additional information.

6.2 Non-Load Bearing Exterior Walls

Non-load bearing exterior walls must be designed such that they have some permanent deformation in response to the peak pressures and impulses calculated per section 6.1.2 Explosive Weights and Calculation of Blast Loads, but no greater than the maximum GP blast loading (Table 6-1). Although negative phase loading should not be considered, the effects of rebound could potentially cause the building envelope to separate from the structure and must be considered as indicated in Table 6-1.

Table 6-1 Threat and Standoff Distance

Criteria	Life-Safety Protected	Mission Critical
Design Level Threat[22]	W1	W1
Standoff Distance (from Table 7-1)	25 ft. (7.6 m)	50 ft. (15 m)
Maximum Blast Load	GP1	GP2
Effects of Rebound	Not Considered	Included

The anchorage and connection of walls into the supporting structure must also be designed to transfer the calculated blast loads. All flexural elements and their connections must be designed and detailed such that no brittle failure mode limits the capacity of the section. Unless the element is designed to remain elastic in response to blast loading, ductile failure modes will be the governing failure mode for flexural elements and their connections and splices. When the elements are designed to resist the calculated blast loads elastically, the

[22] See Chapter 6 Annex for additional discussion regarding the design level threat.

design of non-ductile modes of failure must include a 1.5 factor of safety on the calculated forces.

Acceptable performance must be as defined by the blast load deformation limits in Table 6-2, per Blast Protection of Buildings, ASCE/SEI 59-11, or latest edition.

6.2.1 Tributary Loads from Fenestration

Non-load bearing exterior walls must be able to accept the tributary loads transferred from glazed fenestration and doors in addition to the calculated blast loads applied directly to their surface. The walls must be designed to accept a blast load equal to the maximum capacity of the weakest lite of supported glass (balanced design), but no less than the calculated blast loads (as limited by the GP values) while sustaining deformations no greater than the specified deformation limits (Table 6-2).

Table 6-2 Levels of Protection

Criteria	Life-Safety Protected	Mission Critical
Blast Load Deformation Limits[23]	Heavy Damage	Moderate Damage
Balanced Load Deformation Limits	Heavy Damage	Heavy Damage

6.2.2 Supporting Structure

Non-load bearing exterior walls must span from slab to slab and must not be attached directly to gravity load bearing elements (such as columns and shear walls) unless an advanced dynamic analysis of the load bearing element demonstrates it can accept the maximum blast forces transferred by the members framing into it without compromising its load bearing capacity.

6.2.3 Alteration/Renovation of Existing Facilities — Non-Load Bearing Walls

For building renovations, upgrades, modernizations, or additions in which a non-load bearing exterior wall is being replaced, the replacement wall must comply with the requirements defined in Section 6.2 Non-Load Bearing Exterior Walls. See Chapter 2, Table 2-1 Project Scopes/Requirements, for additional guidance.

[23] Deformation limits are per Blast Protection of Buildings, ASCE/SEI 59-11, or latest edition.

6.3 Fenestration and Doors

6.3.1 Façade Fenestration

All façade fenestration must be designed to the specified performance condition of Table 6-3 in response to the peak pressures and impulses calculated per section 6.1.2 Explosive Weights and Calculation of Blast Loads, but no greater than the maximum GP blast loading (Table 6-1). Although negative phase loading should not be considered, the effects of rebound must be included as indicated in Table 6-1.

6.3.1.1 Glass: All new exterior glazing, including door glazing, must be laminated glass. For insulated glazing units (IGUs) the laminated glass is required only for the inner lite. Glass performance is to be evaluated using a probability of failure of 500 breaks per 1000.[24]

Table 6-3 Glass Performance Levels

Criteria	Life-Safety Protected	Mission Critical
Performance Condition	Fragments must enter the occupied space and land on the floor no further than 10 feet (3 m) from the façade	Glass may crack but must remain in the frame

6.3.1.2 Glazing: Unless demonstrated by analysis that a dry glazed system is adequate, the glass must be restrained within the mullions/frames with a minimum 1/2" bite and a minimum 3/8" wide continuous bead of structural silicone adhesive attaching the inner lite of glass to the frame to allow it to develop its post-damage capacity.

6.3.1.3 Mullions/Frames: The mullions/frames are to be of aluminum and/or steel construction. The mullions/frames must be designed to accept a calculated blast load equal to the peak pressures and impulses applied over their tributary area calculated per section 6.1.2 Explosive Weights and Calculation of Blast Loads, but no greater than the maximum GP blast loading (Table 6-1). The mullions/frames must sustain deformations no greater than the specified deformation limits (Table 6-4) in response to the specified blast loads. The mullions/frames must also be designed to accept a blast load equal to the maximum capacity of the weakest lite of supported glass (balanced design), but no less than the calculated blast loads (as limited by the GP values) while sustaining deformations no greater than the specified deformation limits (Table 6-4). The structural blast engineer must verify that structural properties of mullions/frames

[24] See Chapter 6 Annex for probability of glass failure

used in the blast design calculations are available in mullions/frames from at least three (3) manufacturers, and that the reactions are coordinated with the supporting structure.

For windows with glazing lay-up governed by non-blast requirements (such as, hurricane, forced entry, fabrication, handling, and ballistic), mullions/frames are to be designed for the capacity of the glazing that would be required to meet the blast requirements only. All flexural elements and their connections must be designed and detailed such that no brittle failure mode limits the capacity of the section. Unless the element is designed to remain elastic in response to blast loading, ductile failure modes must be the governing failure mode for flexural elements and their connections and splices. When the elements are designed to resist the calculated blast loads elastically, the design of non-ductile modes of failure must include a 1.5 factor of safety on the calculated forces.

Table 6-4 Façade Frame Deformation Limits

Criteria	Life-Safety Protected	Mission Critical
Blast Load Deformation Limits	L/20 (approx. 6°)	L/40 (approx. 3°)
Balanced Load Deformation Limits	L/14 (approx. 8°)	L/20 (approx. 6°)

6.3.1.4 Supporting Structure: Fenestration mullions/frames must span from slab to slab and cannot be attached directly to gravity load bearing elements (such as columns and shear walls) unless an advanced dynamic analysis of the load bearing element demonstrates it can accept the maximum blast forces transferred by the members framing into it without compromising its load bearing capacity.

6.3.1.5 Alternative Blast Protection Methodologies: Energy dissipating systems that transfer reduced blast forces to the surrounding walls, such as energy absorbing anchors, will be acceptable (this is not a requirement but it is an alternative that may provide a more economical solution) for wall systems that cannot resist the tributary loads transferred from conventional blast-resistant glazing upgrades.

The performance of the energy dissipating system must be demonstrated with acceptable explosive (or shock tube) test data, conducted in accordance with ASTM F1642, current edition. The tested assembly must be demonstrated to VA to be sufficiently similar in glazing layup, mullions, frames, connections, and hardware to that being constructed for the project.

6.3.1.6 Operable Windows: The use of operable windows for blast resistant design is discouraged; however, where operable windows are required, their performance must be demonstrated with acceptable explosive (or shock tube) test data, conducted in accordance with ASTM F1642, current edition, while in the open position. The tested assembly must be demonstrated to VA to be sufficiently similar in glazing layup, mullions, frames, connections and hardware to that being constructed for the project.

6.3.2 Alteration/Renovation of Existing Facilities — Fenestration

6.3.2.1 For renovations in which the glazing is not replaced, use a mechanically anchored or wet glazed attached minimum 7-mil thick anti-shatter film applied to the inside face of the glass (or equivalent) ; performance of the selected system must be demonstrated with glazing hazard calculations or blast test data, which must be of similar sized glass panels and blast load intensity, in accordance with ASTM F1642.

6.3.2.2 Glass replacement upgrades must comply with the requirements of 6.3.1.1 Glass and 6.3.1.2 Glazing.

6.3.2.3 Window replacement upgrades and "storm-window" upgrades interior to existing façade must comply with all the requirements of 6.3.1.1 Glass and 6.3.1.2 Glazing.

6.3.2.4 No upgrades to the frames, mullions, or connections are required for anti-shatter film applications, glass replacement projects, or window replacement upgrades.

6.3.3 Doors

The operable portions of all exterior swing doors of both MC and LSP buildings must be specified using debris mitigating materials such as laminated glass and heavy gauge metal (14-gauge minimum) and must open towards the detonation. The stationary portions of all exterior swing doors must be designed using heavy duty frames and anchorages that are capable of resisting the collected peak pressure and impulse calculated based on section 6.1.2 Explosive Weights and Calculation of Blast Loads, but no greater than the maximum GP blast loading (Table 6-1) while sustaining deformations no greater than the specified deformation limits (Table 6-4). The requirements of section 6.3.1.4 Supporting Structure also apply to exterior doors. The above requirements do not apply to revolving doors, roll-up doors, and sliding doors; however, the glass for these doors must be laminated.

6.3.3.1 Roll-up Doors: Roll-up doors enclosing equipment or mechanical bays are exempt from the hardening requirements. The interior partitions of these equipment or mechanical bays must be reinforced CMU walls that protect the adjacent spaces from infill blast pressures, which correspond to blast loads on exterior walls (Table 6-1), while sustaining deformations no greater than the specified deformation limits (Table 6-2). A

debris-mitigating cable catch system must be installed behind the roll-up door when critical equipment that must remain operational is located within the mechanical bays or when there is occupied space internal to the roll-up door.

6.3.4 Alteration/Renovation of Existing Facilities — Doors

New doors being installed in existing buildings must meet the requirements for the operable portions of doors and their frames/anchorages provided in 6.3.3. When the supporting structure is also being upgraded/replaced as part of the project, modifications required to the supporting structure to meet section 6.3.1.4 Supporting Structure are to be implemented.

6.4 Atria

6.4.1 Atria Enclosures

All vertical, horizontal, and sloped glass surfaces must be designed to the specified performance condition (Table 6-3) in response to the peak pressures and impulses calculated per section 6.1.2, Explosive Weights and Calculation of Blast Loads, but no greater than the maximum GP blast loading (Table 6-1). Although negative phase loading should not be considered, the effects of rebound must be included as is indicated in Table 6-1.

6.4.1.1 Skylights: See section 6.5.3 Skylights.

6.4.1.2 Glass: See section 6.3.1.1 Glass.

6.4.1.3 Glazing: See section 6.3.1.2 Glazing.

6.4.1.4 Mullions: See section 6.3.1.3 Mullions/Frames.

6.4.1.5 Framing: Atria framing members must remain stable and continue to carry gravity loads while sustaining deformations no greater than the specified deformation limits (Table 6-4) in response to the peak pressures and impulses calculated per section 6.1.2 Explosive Weights and Calculation of Blast Loads, but no greater than the maximum GP blast loading (Table 6-1).

6.4.2 Alteration/Renovation of Existing Facilities — Atria

6.4.2.1 For renovations in which the glazing is not replaced, a mechanically anchored or wet glazed attached minimum 7-mil thick anti-shatter film applied to the inside face of the glass (or equivalent) must satisfy the requirements of this section; performance of the selected system must be demonstrated with glazing hazard calculations or blast test data, which must be similar sized glass panels and blast load intensity, in accordance with ASTM F1642.

6.4.2.2 Glass replacement upgrades must comply with the requirements of 6.3.1.1 Glass and 6.4.1.2 Glazing.

6.4.2.3 No upgrades to the frames, mullions, or connections are required for anti-shatter film applications or glazing replacement projects.

6.5 Roofs

6.5.1 Roof Structure

Roof structure (including metal deck, composite deck, concrete slabs, beams, and joists) must be designed to withstand the peak incident pressures and impulses calculated per section 6.1.2 Explosive Weights and Calculation of Blast Loads, but no greater than the maximum GP blast loading (Table 6-1). If the roof structure acts as a diaphragm and contributes to the overall stability of the structure, it must be treated as part of the building's main lateral resisting system, for which Chapter 7 applies. Ray tracing software may be used to calculate a blast loading that considers the presence of parapets, the diffusion of blast waves, and the spatial extent of the roof surface (for example, BLASTX software considers these effects). Although negative phase loading should not be considered, the effects of rebound must be included in the design of blast resistant roof and connections for MC facilities.

Roof structure must be able to accept the tributary loads transferred from glazed fenestration (skylights) in addition to the calculated blast loads applied directly to the surface. The roof structure must be designed to accept a blast load equal to the maximum capacity of the weakest lite of supported glass (balanced design), but no less than the calculated blast loads (as limited by the GP values) while sustaining deformations no greater than the specified deformation limits (Table 6-2). All flexural elements and their connections must be designed and detailed such that no brittle failure mode limits the capacity of the section. Unless the element is designed to remain elastic in response to blast loading, ductile failure modes must be the governing failure mode for flexural elements and their connections and splices. When the elements are designed to resist the calculated blast loads elastically, the design of non-ductile modes of failure must include a 1.5 factor of safety on the calculated forces.

6.5.2 Alteration/Renovation of Existing Facilities — Roof Structure

For upgrades in which an element of the roof structure is being replaced, the replacement element and its connections must comply with the requirements defined in section 6.5.1 Roof Structure. However, when existing roof framing is not replaced or strengthened any replaced decking must be designed to the calculated blast loads (as limited by the GP values), but the deck capacity must be no greater than the capacity of the existing beams that support the deck.

6.5.3 Skylights

Skylight glass for both MC and LSP facilities must be designed to crack but remain in its frame in response to the peak incident pressures and impulses calculated per section 6.1.2 Explosive Weights and Calculation of Blast Loads, but no greater than the maximum GP blast loading (Table 6-1). The blast loading must consider the presence of parapets, the diffusion of blast waves, and the spatial extent of the roof surface.

6.5.3.1 Glass: All skylight glazing is to use laminated glass. For insulated glazing units (IGUs) the laminated glass is required only for the inner lite.

6.5.3.2 Glazing: Unless demonstrated by analysis that a dry glazed system is adequate, the glass must be restrained within the mullions with a minimum 1/2" bite and a minimum 3/8" wide continuous bead of structural silicone adhesive attaching the inner lite of glass to the frame to allow it to develop its post-damage capacity.

6.5.3.3 Mullions/Frames: The mullions/frames are to be of aluminum and/or steel construction. The mullions/frames must be designed to accept the peak pressures and impulses applied over their tributary area calculated per section 6.1.2 Explosive Weights and Calculation of Blast Loads, but no greater than the maximum GP blast loading (Table 6-1). The mullions/frames must sustain deformations no greater than the specified deformation limits (Table 6-4) in response to the specified blast loads. The mullions/frames must also be designed to accept a blast load equal to the maximum capacity of the weakest lite of supported glass (balanced design), but no less than the calculated blast loads while sustaining deformations no greater than the specified deformation limits (Table 6-4). The structural blast engineer must verify that structural properties of mullions/frames used in the blast design calculations are available in mullions/frames from at least three (3) manufacturers, and that the reactions are coordinated with the supporting structure. For glazing lay-up governed by non-blast requirements (such as hurricane, forced entry, fabrication, handling, and ballistic), mullions/frames are to be designed for the capacity of the glazing that would be required to meet the blast requirements only.

6.5.4 Alteration/Renovation of Existing Facilities — Skylights

6.5.4.1 For renovations in which the glazing is not replaced, a mechanically anchored or wet glazed attached minimum 7-mil thick anti-shatter film applied to the inside face of the glass may be used to satisfy the requirements of this section. Performance must be demonstrated with glazing hazard calculations or test data, deemed by VA to be of similar sized glass panels and blast load intensity, in accordance with ASTM F1642, current edition.

6.5.4.2 Glass replacement upgrades must comply with the requirements of 6.5.3.1 Glass and 6.5.3.2 Glazing.

6.5.4.3 No upgrades to the frames, mullions or connections are required for anti-shatter film applications or glazing replacement projects.

6.5.4.4 Skylight replacement upgrades must comply with the requirements of 6.5.3.1 Glass and 6.5.3.2 Glazing.

6.6 Critical Equipment Protection

6.6.1 Penthouses and Screen Walls

All equipment that is identified by VA to be critical must be enclosed in a blast resistant enclosure; however, roof or ground level equipment enclosures may be open above. When the enclosure is not open above, the requirements for section 6.5 Roofs apply. The cladding of critical equipment enclosures must be designed to resist the peak blast pressures and impulses calculated per section 6.1.2 Explosive Weights and Calculation of Blast Loads, but no greater than the maximum GP blast loading (Table 6-1). Acceptable cladding performance must be as defined by the blast load (not balanced design) deformation limits (Table 6-2). Structural performance for critical equipment enclosures must conform to section 6.6.1 Penthouses and Screen Walls. While this may not protect equipment from potential high intensity infill blast pressures, it will protect equipment from the impact of cladding debris. For critical systems requiring assured protection, distributed redundancy is strongly recommended. Distributed redundancy may also be used in lieu of hardening where partial survivability of critical systems is acceptable.

6.6.2 Intakes and Exhausts Servicing Critical Equipment

All air intakes and exhausts for MC facilities and any LSP facility air intakes and exhausts that enter critical equipment spaces must be designed to minimize the blast over pressure applied to critical mechanical or electrical equipment by means of hardened plenums and internal or external structured baffles. The blast pressures and impulses are to be calculated per section

6.1.2 Explosive Weights and Calculation of Blast Loads, but no greater than the maximum GP blast loading (Table 6-1).

The design must deny a direct line of sight from the design level threat located at the standoff distance to the critical infrastructure within. Where direct lines of sight cannot be denied, distributed redundancy is required to support continuous operations.

Deformations of hardened plenums and structured baffles in response to the blast loading must be as defined by the Heavy Damage response limits per Blast Protection of Buildings, ASCE/SEI 59-11, or latest edition. Anchorage of baffles must be designed for the collected blast loads. Baffles must provide an overlap that is equivalent to the space between the baffle and the surrounding wall.

6.6.3 Alteration/Renovation of Existing Facilities — Air Intakes and Exhausts Servicing Critical Equipment

Air intakes and exhausts being replaced as part of a renovation or equipment upgrade must be designed to meet the requirements of section 6.6.2 Air Intakes and Exhausts Servicing Critical Equipment.

6.7 Calculation Methods and Documentation

All blast design and analysis, whether for new or existing construction, must be performed in accordance with accepted methods of structural dynamics. Explosive (or shock tube) testing conforming to ASTM 1642 is required wherever operable windows are used or where the behavior of energy absorbing, or other complex façade systems cannot be characterized by analytical methods. A blast narrative and supporting calculations, signed and sealed by the professional engineer responsible for their preparation, must demonstrate conformance with these requirements.

6.7.1 Design and Detailing

The performance of façade in response to blast loading is highly dynamic and often inelastic. Design and detailing of a blast resistant façade must therefore be based on analytical methods that accurately represent the loads and response. Explosive test data conforming to ASTM F1642, 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.

6.7.2 Blast Loads

Blast loads are developed using the semi-empirical equations of UFC 3-340-01, *Design and Analysis of Hardened Structures to Conventional Weapons Effects,* dated June 2002 (CONWEP).

6.7.3 Dynamic Response

Dynamic structural response analyses must 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 must be in accordance with this document. Where advanced FEM are used, the performance must be demonstrated through interpretation of the calculated results. Dynamic glass response analyses must be performed using window glazing analysis and design software developed by the USG, such as WINGARDPE, SBEDS-W, which are capable of predicting the glass, film, and laminate response when subjected to the blast loading environment.

Annex to Chapter 6

A-6.1.2a Request of Physical Security & Resiliency Design Standards Data Definitions

In addition to the structural blast engineer on the design AE team, subcontractors/vendors (such as curtainwall systems, precast concrete panels, etc.) also need the blast pressures and impulses to design the systems for the building envelope. A vendor can submit request to VA CFM through the VA project manager. If the request is approved, VA will direct the structural blast engineer to provide the computed pressure and impulse (which are based on the specific conditions of the project such as standoff distance, building geometry, or other factors) to the vendor. Without the computed values, the pressure and impulse values in the Data Definitions document alone are not sufficient to provide an appropriate blast resistant design in accordance with this manual.

A-6.1.2b The Explosive Threat, Establishment of the Design Level Threat and the GP Values

The effects of an explosion primarily depend on the weight of explosives, the type of the explosives, and the distance from the point of detonation to the protected structure. Different types of explosive materials are classified as High Energy or Low Energy and these different classifications greatly influence the damage potential of the detonation. Nevertheless, the protective design of structures focuses on the effects of High Energy explosives and relates the different mixtures to an equivalent weight of TNT.

The distance of the protected structure from the point of explosive detonation is commonly referred to as the standoff distance. As the front of the shock-wave propagates away from the source of the detonation at supersonic speed it expands into increasingly larger volumes of air, the peak incident pressure at the shock front decreases and the duration of the pressure pulse increases. Both the intensity of peak pressure and the impulse, which considers the effect of both pressure intensity and pulse duration, affect the hazard potential of the blast loading. When an explosion occurs within an occupied space, the confinement of the explosive by-products produces a quasi-static gas pressure that needs to be vented into the atmosphere. Near contact explosions impose a high impulse, high intensity pressure load over a localized region of the structure, whereas standoff detonations typically produce a lower intensity pressure that may engulf the entire structure.

The building's façade is its first real defense against the effects of a bomb and typically the weakest component that will be subjected to blast pressures, much weaker than the structural elements that support gravity loads or resist lateral pressures. Different weights of explosive threat are therefore considered for the design of the building envelope than for the design of

the building structure. Whereas W0, W1 and W2 are considered for the design of Mission Critical (MC) and Life-Safety Protected (LSP) structural elements, the threat for calculating façade loading for both MC and LSP is W1. The minimum standoff distance for MC is 50-feet and the minimum standoff distance for LSP is 25-feet. At first glance, this may seem counterintuitive; the peak blast load for LSP (W1 at 25-feet) is greater than the peak blast load for MC (W1 at 50-feet). However, the calculated blast loading for the design of the glazed façade elements is limited to GP1 for LSP facilities and limited to GP2 for MC facilities. Therefore, regardless whether the LSP peak blast loading is calculated to have a higher magnitude at the minimum allowable standoff distance than the MC peak blast loading, the limiting magnitude for LSP facilities is lower than for the MC facilities. Furthermore, the GP1 limit extends over a larger area of the building relative to the LSP threat than the GP2 limit relative the MC threat. Therefore, the W1 at 50-feet with a GP2 limit requires a more robust façade for MC facilities than the W1 at 25-feet with a GP1 limit requires for LSP facilities.

Finally, the VA requirements are different from the DoD and ISC standards so that there should not be the assumption that the DBTs, blast loads, standoff distances, and performance requirements for DoD and ISC will satisfy the VA requirements.

A-6.1.2c Design to Resist the Explosive Threat

Although the response of specific glazed components is a function of the dimensions, make-up and construction techniques, the conventionally glazed portions of the façade will shatter and inflict severe wounds when subjected to a W1 explosive detonation at a standoff distance on the order of 200-feet. When a fragment retention film is daylight applied to the inner surface of an existing lite of glass, its resistance to blast pressures will not be increased but the resulting shards will be collected in a single mass. However, when the fragment retention film is applied to the inner surface of the existing lite of glass and attached to the surrounding window frames, the membrane capacity of the film can be developed if the supporting structure is able to withstand the collected loads. When the existing glazed elements are upgraded with an attached fragment retention film, they may be able to withstand the W1 explosive detonation at a standoff distance of approximately 70-feet. The innermost lite of a new insulated glazed façade element must therefore be laminated to restrain glass debris, much as a fragment retention film would protect an existing lite of glass.

Unreinforced masonry block walls are similarly vulnerable to collapse when subjected to the W1 explosive detonation at a standoff distance of 50-feet, however, if these same walls are upgraded with a debris catching system, they may be able to sustain this same intensity explosive detonation at a standoff distance on the order of 20-feet. If the weight of explosives were increased from W1 to W2, the required standoff distances to prevent severe wounds

increases to 300-feet for conventional window glazing,[25] 200-feet for window glazing treated with a fragment retention film, 150-feet for unreinforced masonry block walls and 40-feet for masonry walls upgraded with a debris catching system. Based on these dimensions, it is apparent that substantial standoff distances are required for the unprotected structure and these distances may be significantly reduced using debris mitigating retrofit systems. Furthermore, since blast loads diminish with distance and geometry of wave propagation relative to the loaded surface of the building, the larger threats at larger standoff distances are likely to damage a larger percentage of façade elements than the more localized effects of smaller threats at shorter standoff distances. The blast pressures that may be applied to the roof and subsequent rebound load reversals are likely to exceed conventional design loads. Unless the roof is a concrete deck or concrete slab structure, it may suffer damage.

A-6.1.2d Balanced Design

Building elements store a significant amount of strain energy when they are deformed by a blast event and if the building element does not detach from its supports and fly into the building, it will rebound as it cycles through its dynamic response. In many cases, the damaged building element can be allowed to harmlessly fail during rebound and fall away from the building; however, these building elements can be designed to remain attached though a complete cycle of response. Designing a façade to withstand the effects of rebound will reduce the amount of façade debris that will be deposited outside the building and will maintain a damaged building enclosure. Although this damaged façade will have to be replaced, it may permit a level of continued operation that would not be possible if the damaged façade could fail outside the building. Rebound applies to a variety of building elements including façade, atria, roof cladding.

The façade elements must be designed to provide the required performance in response to the specified blast loading; however, these elements typically possess excess capacity. Many U.S. Government criteria recognize the potential for stronger glass than required to resist the specified blast loading to impose greater reaction forces on the supporting mullions, connections and anchorages. This excess glass capacity could therefore produce a brittle failure of the supporting elements, which might allow the entire window frame to enter the protected space. These U.S. Government criteria therefore require a balanced design in which the framing members are designed and detailed to resist the actual capacity of the glass. In addition to preventing a potentially hazardous failure mode, the balanced design takes full advantage of the actual capacities of all the façade components. Since the balanced design loading exceeds the nominal design loads, a greater extent of damage is permitted for the balanced design loading than for the corresponding actual blast loading.

[25] Glazing refers to the glass make-up, either single pane or insulated double pane, that is used in a window system

A6.1.2e Probability of Glass Failure

Glass strength is variable and is characterized by the number of breaks per thousand, which represents the number of test articles of a given make-up that will fail at a less intense load. Unless the weakest tested strength of glass is specified for design, as is required for conventional wind loads, some of the glass within the façade may fail at a lower intensity blast loading while other lites of glass may withstand higher intensity blast loading. This means some of the glass will collect greater intensity loads that can overload the frames, connections and anchorage. Therefore, the Unified Facilities Criteria (UFC 4-010-01) specifies the mean (500 break per 1000) strength for determining the performance of glass façade in response to blast loading. This strikes a reasonable balance between mitigating glass fragment hazard and preventing component or system failure of the façade system.

A-6.1.2f Thermal Upgrade coordination with Blast Upgrade

When a building is undergoing modernization that includes improving the thermal performance of the façade, it may be possible to achieve the thermal objectives by replacing the glass within the existing frames with an energy efficient insulated glazing unit (IGU). The innermost lite of the replacement IGU would be laminated in order to restrain debris; however, consideration should be given to replacing the framing members to develop the calculated blast loads or (better yet) to develop a balanced design. This issue applies to skylights as well as vertical fenestration.

A-6.1.2g Protection of Exterior Stairwells/Walkways

Exterior stairwells (enclosed or exposed) and covered or enclosed walkways are generally not considered to be routinely occupied. There are typically multiple exterior stairwells in a building, including emergency exit stairwells, and based on the magnitude of explosive threat considered in this design manual, it is unlikely that multiple stairwells would be significantly impacted unless they were very close together. Furthermore, even though these enclosures do not require blast resistant glazing, they may still be usable even if they are littered with broken glass.

7 STRUCTURAL SYSTEM

7.1 Scope, Purpose, and Goals

This chapter provides requirements for blast resistant structures and includes requirements for the prevention of progressive collapse and the hardening of columns, slabs, beams load bearing walls that are required for structural stability, and interior partitions. 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. The requirements in this manual 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. Although the design to resist one extraordinary loading does not necessarily provide adequate protection in response to another extraordinary event, the basic requirements for ductility, redundancy, and robustness will contribute to the occupants' safety in response to a wide range of hazards and unforeseen events.

All building components requiring blast resistance must be designed using established methods and approaches for determining dynamic loads, structural detailing, and dynamic structural response. Designers must apply dynamic methods of analysis to demonstrate compliance with this requirement. Alternative analysis and mitigation methods are permitted, provided that the performance level is attained, and approval is granted by the VA AHJ, defined in section 1.3 Administration and Enforcement.

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

As stated in Chapter 1, the requirements in this manual apply to new buildings, additions, and existing facilities undergoing renovations. Further clarification on applicability to renovation projects is provided in Table 2-1 and in the gray box describing alteration/renovation of existing facilities at the end of each major section.

The requirements of this chapter are baseline physical security and resiliency requirements for MC Facilities, LSP Facilities with MC Utilities/Systems Redundancies, and LSP facilities. LSP Facilities with MC Utilities/Systems Redundancies are to comply with requirements for LSP Facilities listed in this chapter. A risk assessment during the project planning phase is allowed to evaluate the deletion or incorporation of other specific requirements (see section 2.3 Exceptions and Deviations). The VA AHJ overseeing implementation of physical security and resiliency requirements for the facility will review submitted request for deviation from the baseline requirements of this chapter. When no risk assessment is performed, these baseline requirements must apply.

The requirements of this chapter supplement other related VA standards for construction, space and facility planning criteria, design guides, design manuals, specifications, and details, which remain in full force and effect. Specifically, all requirements of VA Handbook 0730, Security and Law Enforcement, Appendix B, (which covers physical security requirements for VA facilities), the VA Fire Protection Design Manual (which covers all VA construction), and ICT standards on the TIL remain in effect.

7.1.1 Explosive Weights and Calculation of Blast Loads

In order to meet the physical security and resiliency requirements of this manual, the design team must include security subject matter experts as per section 1.8 Requirements for Subject Matter Specialists. The qualifications required for the licensed professional structural engineer who has specialized training in blast design and analysis (structural blast specialist) are included in section 6.1.1 Blast Specialist Requirements.

The magnitudes of W0, W1, and W2 are defined in the Physical Security and Resiliency Design Standards Data Definitions, a document separate from the PSRDM. It is provided on a need-to-know basis to the structural blast specialist performing analysis and design of VA projects (see Chapter 6 Annex for additional information regarding request of the Data Definitions by subcontractor/vendors). Authorized users can contact the VA Office of Construction and Facilities Management (CFM) to request the document. Unless otherwise specified, the calculated blast loads are defined to be the peak pressures and impulse resulting from the exterior design level threat located at the minimum specified standoff distances at the base of the building and vertical elevation (considering building setbacks, etc.), as appropriate. Horizontal standoff provided in excess of the minimum standoff distances can only be accounted for in the calculation of the blast loading environment when land use agreements by the local VA facility's authority and the AHJ (see section 1.3 Administration and Enforcement) are in effect to prevent relocation of roadways or parking any closer than their current location.

All interior explosive threats are to be located in the center of the structural bay within which they can be introduced for determining the performance of surrounding structural elements. The interior threat must also be located twelve inches above slabs and 12 inches (0.3 m) from the face of columns and load bearing walls, as noted in Table 7-1. For non-loadbearing interior partitions, the interior threat must be located at the center of the area/room (assumed having shape similar to a square) surrounded by the partitions. In elongated area/rooms, the threat must be reviewed for multiple locations along the long axis of area/room.

Table 7-1 Threat and Standoff Distance

Criteria	Life-Safety Protected	Mission Critical
Exterior Design Level Threat	W1	W2
Standoff Distance	25 ft. (7.6 m)	50 ft. (15 m)
Interior Design Level Threat	W0	W1
Standoff Distance for interior structural elements	12” (0.3 m) above slab at center of each bay	12” (0.3 m) above slab at center of each bay
Standoff Distance for columns and load bearing walls	12” (0.3 m)	12” (0.3 m)

7.1.2 Applicability and Exempted Structures

Buildings of type V construction (specifically light-frame wood and cold-formed steel framing structure) as defined in the International Building Code are exempt from blast resistance and progressive collapse prevention requirements of Chapter 7. However, connections of primary structural members must be designed to develop the flexural capacity of the members. Members must develop their full plastic capacities before they may detach due to connection failure. Balanced design approach as defined in ASCE 59-11 must be used to prevent brittle modes of failure.

7.2 Blast Resistance

Protected structures must be constructed to withstand the peak pressures and impulse due to the exterior design level threat calculated per section 7.1.1 Explosive Weights and Calculation of Blast Loads, and the interior design level threat that may be delivered to loading docks, mailrooms, and main public lobbies to the facility (Table 7-1). These blast loads must be considered concurrent with gravity loads acting on the structure. The structural elements to be designed for the exterior design level threat are those that are a part of or exterior to the building envelope. Additionally, structural elements that are to be designed for the interior design level threat are those within vulnerable interior spaces. This can include columns and slabs that are part of a building overhang or columns that are flush with the exterior façade of the building. This can also include columns and slabs within loading docks that separate this vulnerable space from adjacent occupied spaces.

The design of MC buildings must 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.

The design of life-safety protected buildings must also prevent progressive collapse; however, the building damage may not be economically repairable and the space in and around damaged area may not be usable and may not be fully functional after cleanup and repairs

Where columns and load bearing walls within loading docks, mailrooms, and main lobbies to the facility are accessible to a close contact interior design level threat, a nominal standoff distance of 12" will be assumed.[26]

7.2.1 Priority for Protection

Essential to mitigating progressive collapse, the priority for blast resistance must be given to critical elements which are exposed to the exterior or interior design level threat. Design of secondary structural elements, primary nonstructural elements, and secondary non-structural elements must minimize injury and damage (see Chapter 7 Annex for additional information). In all cases, consideration must be given for both the positive load phase and the subsequent effects of rebound. The priority depends on the relative importance of structural or non-structural elements in the following order.

7.2.1.1 Primary Structure: Primary structural elements are the essential parts of the building's resistance to catastrophic failure, including columns, load bearing walls, girders, and structural members that comprise the main lateral resistance system, including applicable roof beams and girders. Special attention must be given to the lateral resistance and global stability of the structure in response to the specified blast loads. Acceptable performance will be as defined by the blast load deformation limits (table 7-2) per Blast Protection of Buildings, ASCE/SEI 59-11, or latest edition.

7.2.1.2 Secondary Structure: Secondary structural elements are all other load bearing members, such as floor and roof beams and slabs that do not comprise the main lateral resistance system. For contact detonations, breach of slab and failure of floor beams must be acceptable in the bay containing the detonation. For all other threat scenarios, acceptable performance is defined by the blast load deformation limits (table 7-2) per Blast Protection of Buildings, ASCE/SEI 59-11, or latest edition.

[26]For contact detonation, the blast intensity is significantly reduced with additional inches of standoff distance. The center of the explosive itself takes up inches as does the column cover; 12" is a reasonable nominal value.

Table 7-2 Levels of Protection

Criteria	Life-Safety Protected	Mission Critical
Blast Load Response Limits for Primary Structure[27]	Moderate Damage	Superficial Damage
Blast Load Response Limits for Secondary Structure[28]	Heavy Damage	Moderate Damage

7.2.1.3 Primary Non-structural (Non-façade Elements): Primary non-structural elements and their attachments that are essential for life-safety systems or elements that can cause substantial injury if failure occurs, including overhead heavy suspended mechanical units or fixtures weighing more than 31 lbs. These elements (excluding distributed systems such as suspended ceilings or piping networks) must be anchored with lateral ties capable of resisting lateral motions associated with the building's calculated blast induced base shear. Mountings must also be designed for forces required by other criteria such as seismic standards.

7.2.1.4 Secondary Non-structural: Secondary non-structural elements are all elements not covered in primary non-structural elements, such as partitions, furniture, and light fixtures. A positive means of attachment of these elements to the building structure and design arrangements that will minimize debris following in-structure shock motions are required.

7.2.2 Vertical Structural Element Protection

Columns and load bearing walls must be hardened or isolated to resist the appropriate flexural and direct shear effects resulting from the calculated blast loads, which are defined to be the peak pressures and impulse resulting from the exterior and interior design level threat (Table 7-1) to which they may be exposed. Acceptable performance must conform to the blast load response limits for primary structure (Table 7-2).

7.2.3 Wall Protection

Non-load bearing interior walls separating high risk interior spaces (loading docks, mailrooms, and main public lobbies) must be designed to resist the calculated blast loads, which are defined to be the peak pressures and impulse resulting from the interior design level threat (Table 7-1) that may be delivered to these spaces (see 7.1.1 for standoff distance

[27] Deformation limits are per Blast Protection of Buildings, ASCE/SEI 59-11, or latest edition.
[28] Ibid

requirements). Wall breach/spall in response to contact detonations is acceptable. Walls must be of reinforced masonry or concrete construction. Acceptable performance is defined by the blast load response limits for secondary structure (Table 7-2).

All blast resistant wall elements and their connections must be designed and detailed such that no brittle failure mode limits the capacity of the section. Unless the element is designed to remain elastic in response to blast loading, ductile failure modes will be the governing failure mode for flexural elements and their connections and splices. When the elements are designed to resist the blast loads elastically, the design of non-ductile modes must include a 1.5 factor of safety on the calculated forces. Doors within these walls must adhere to the requirements of section 6.3.3 Doors.

7.2.4 Screen Walls and Penthouse Structure

The structure providing lateral resistance for non-load bearing screen walls and penthouses that enclose critical equipment must be designed for the calculated blast loads, which are defined to be the peak pressures and impulse, resulting from the exterior design level threat located at the minimum standoff distance (Table 7-1) and corresponding vertical elevation and building plan dimensions, as appropriate. Acceptable performance is defined by the blast load response limits for secondary structure (Table 7-2).

The cladding of critical equipment enclosures must comply with the requirements of section 6.6 Critical Equipment Protection, and doors are to follow the requirements of section 6.3.3 Doors.

7.2.5 Buried Utilities and Buried Equipment

The location and site conditions of buried utilities/equipment must be evaluated to ensure there is adequate protection against the calculated blast load when the utilities/equipment provide services to Mission Critical Facilities. [Note: Utilities and equipment may be remote from Mission Critical Facilities but still provide services to them.] Unless certain conditions listed below are met, a blast analysis is required to demonstrate that the buried utilities/equipment are at least 12" from the edge of the calculated true crater caused by the W2 design level threat. If the 12” requirement is not met, mitigation measures must be implemented to protect the buried utilities/equipment. When conditions (e.g. vehicle access control, paving, distance, etc.) vary along the path of a buried utility, a separate evaluation must be performed for each differing section. Blast analysis and mitigation measures are not required if one of the following conditions is met:

- The buried utility/equipment is in a location only accessible to screened vehicles. [Note: Locations only accessible to screened vehicles must have vehicular access control such as gates with card access devices, or remote release with operation by authorized

personnel. Examples include loading dock service yards or designated staff parking areas.]

- The buried utility/equipment is at or adjacent to a normal path of travel along which parking is not allowed. [Note: Normal path of travel is a paved public roadway serving visitors and staff where vehicles are not allowed or expected to be parked. Areas where vehicles may park (e.g. designated and un-official parking areas, temporary parking, etc.) and unpaved access roads (e.g. gravel, grass, etc.) are considered outside the normal path of travel.]
- The buried site utility has redundancy in accordance with Section 8.3 Site Distribution of this Manual such that the utility service can be rerouted when there is a break in the utility.
- The location of the buried utility/equipment and the area where an unscreened vehicle may park are continuously paved with asphalt or concrete with a minimum thickness of 3 inches.
- The buried utility/equipment is encased in concrete.
- The buried utility/equipment is located and kept no less than 8'-6" (horizontal distance) from where unscreened vehicles may park. [Note: If the area where unscreened vehicles may park within 8’-6” of the buried utility/equipment has mixed surface or underground materials (e.g. part pavement, part lawn, part gravel, part clay, etc.), this evaluation process and the blast analysis (if necessary) is to be based on the weakest material (e.g. unpaved area, softest soil, non-exempt paved area less than 3” thick, etc.)
- The utility/equipment is buried deeper than 5’.

7.2.6 Detailing of Hardened Elements

All hardened elements and their connections must be designed and detailed such that no brittle failure mode limits the capacity of the section. Unless the element is designed to remain elastic in response to blast loading, ductile failure modes will be the governing failure mode for flexural elements and their connections and splices. When the elements are designed to resist the blast loads elastically, the design of non-ductile modes must include a 1.5 factor of safety on the calculated forces.

7.2.7 Alteration/Renovation of Existing Facilities — Column Protection

In MC buildings, columns in spaces the public can access prior to screening from explosive devices must be hardened to resist the interior design level threat (Table 7-1). In MC buildings, perimeter columns that are exterior to the building envelope and freestanding must satisfy structural hardening requirements of section 7.2.2 Vertical Structural Element Protection.

In LSP buildings, protect columns in interior spaces the public can access prior to screening from explosive devices by either structural hardening or the installation of architectural or structural finishes that prevent detonation within 6 inches (152 mm). In LSP buildings, perimeter columns that are exterior to the building envelope and freestanding must be protected by either structural hardening or the installation of architectural or structural finishes that prevent detonation within 6 inches (152 mm).

7.3 Design for Global Stability of the Structure

7.3.1 Base Shear

In addition to designing the structural elements of the building for the local flexural and shear effects due to the calculated blast loads, the overall stability of the building must resist the global lateral force resulting from a blast. The base shear resulting from the exterior design level threat will be calculated, distributed to the building levels and compared to the base shear resulting from the wind and/or seismic loads; when the blast induced base shear governs, it must be used in the design of the building's lateral system. The blast base shear will be used as an ultimate load.

7.3.2 Base Shear Calculation

The blast base shear, V_b, applied to the building will be calculated using the following equation:

$$\frac{3\,\pi\,I}{2\,T\sqrt{2\,\mu-1}}$$

Where: I = the blast induced impulse on the facing wall

T = the fundamental period of the building

μ = the design ductility

7.3.3 Alteration/Renovation of Existing Facilities — Base Shear Calculation

The overall stability of the building to resist the global lateral force resulting from a blast must be included in designs for existing buildings that are undergoing a seismic upgrade.

7.4 Prevention of Progressive Collapse

7.4.1 Methods

Single-story and two-story structures are exempt from progressive collapse requirements. Buildings with three or more stories[29] must be designed to minimize the potential for progressive collapse using one or more of the following methods (Table 7-3). All perimeter columns and load bearing walls must be designed to prevent progressive collapse (see Chapter 7 Annex for additional information).

7.4.1.1 Tie Force Method in which the structure develops peripheral, internal, and vertical tie forces by providing continuous reinforcement and ductile detailing; this will help prevent collapse following the removal of an interior column.

7.4.1.2 Alternate Path Method, which requires the structure to withstand the threat independent removal of any perimeter column, one at a time, or one bay width of exterior load bearing walls, one at a time, without precipitating a disproportionate extent of damage; the column/wall removal scenarios apply to the full height of the building.

7.4.1.3 Enhanced Local Resistance Methods, in which the shear and flexural strength of the ground floor perimeter columns and walls are increased to provide additional protection by reducing the probability and extent of initial damage.

Table 7-3 Progressive Collapse Mitigation Methods

Criteria	Life-Safety Protected	Mission Critical
Three Stories or More	Tie Force Method	Tie Force Method, Enhanced Local Resistance Method, and Alternate Path Method

7.4.2 Additional Requirements

The requirements of the tie force, enhanced local resistance, and alternate path analysis methods for demonstrating a structure's resistance to progressive collapse must conform to U.S. Government (USG) guidelines, specifically, *Design of Buildings to Resist Progressive Collapse,* UFC 4-023-03 dated 1 June 2013, or latest edition, with the following additional requirements:

[29] Unoccupied stories, such as interstitial mechanical spaces, and mechanical penthouses must not be considered a story for this purpose. Floors below grade (i.e. single and multiple level basements) will be considered a story if there is any space that is designed for human occupancy.

7.4.2.1 The global stability of long narrow buildings must be demonstrated following the removal of an exterior column.

7.4.2.2 In buildings where the slab cantilevers at the perimeter of the building, the first row of inboard columns must be considered in the design to prevent a progressive collapse.

7.4.2.3 Closely spaced columns, either parallel or perpendicular to the façade that are closer than 30 percent[30] of the largest bay dimension, are to be simultaneously removed in the same alternate path analysis; this applies to all structural configurations, including long narrow buildings and internal moment frames with cantilevered beams supporting the façade.

7.4.2.4 All exterior columns of multi-story buildings that are surrounded by a low-rise podium must be considered in the design to prevent a progressive collapse.

7.4.2.5 All columns within courtyards that are directly accessible from the exterior of the building must be designed to prevent a progressive collapse.[31]

7.4.3 Alteration/Renovation of Existing Facilities — Progressive Collapse

In lieu of alternate path analysis, structural hardening/architectural treatment must be implemented per section 7.2.2 Vertical Structural Element Protection.

7.5 Anti-Ram Resistance

7.5.1 Vehicle Barriers

Both active and passive barriers must be tested and certified to be capable of stopping a 4,000-pound (1,800 Kg) vehicle at a speed of 30 miles per hour (48 Km/hr) with a maximum penetration distance of 3.3 feet (1m); see also section 3.5 Anti-Ram Rated Vehicle Barriers.

7.5.1.1 Certification/Testing: Performance of anti-ram element must be demonstrated by means of impact testing or detailed finite element analysis of the vehicle impact; testing is to be performed in accordance with the latest edition of ASTM F2656, ASTM F3016, or DOS SD-STD-02.01.

7.5.1.2 Active Barriers: Active barriers must be electric or hydraulic wedges, bollards, beams, drop arms, or sliding gates.

[30] From the GSA Guidelines
[31] This is intended for a U-shaped building.

7.5.1.3 Passive Barriers: Passive barriers must be walls, stationary bollards, cables, or combination of landscape and hardscape that achieves the required anti-ram resistance.[32]

7.5.2 Alteration/Renovation of Existing Facilities — Anti-Ram Resistance

The requirements of section 7.5.1 Vehicle Barriers apply.

7.6 Calculation Methods

All blast design and analysis, whether for new or existing construction, must be performed in accordance with accepted methods of structural dynamics. A blast narrative and supporting calculations must be submitted at each stage of design; the blast narrative and supporting calculations must be signed and sealed by the professional engineer responsible for their preparation.

7.6.1 Design and Detailing

The performance of structures in response to blast loading is highly dynamic and often inelastic. Design and detailing of blast resistant structures must therefore be based on analytical methods that accurately represent the loads and response. Explosive test data conforming to ASTM F1642, 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.

7.6.2 Blast Loading

Blast loads will be developed using the semi-empirical equations of UFC 3-340-01, *Design and Analysis of Hardened Structures to Conventional Weapons Effects,* dated June 2002 (CONWEP); however, Computational Fluid Dynamics (CFD) methods are required wherever the semi-empirical Kingery Bulmash equations, such as used in the U.S. Army Corps of Engineers software (CONWEP) is no longer valid. Alternatively, it is acceptable to use validated fast running models for close-in/contact detonations to calculate the blast loadings and/or effects on the element. This typically occurs when near contact detonations are considered.

7.6.3 Dynamic Response

Dynamic structural response analyses must 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 must be in accordance with this document. Where advanced

[32] Several DoD documents identify the effectiveness of passive barrier systems; these are based on empirical testing.

FEM are used, the performance must be demonstrated through interpretation of the calculated results.

Annex to Chapter 7

A-7.2.1 Design for Global Stability

The building's lateral load resisting system, the structural frame or shear walls, that resist wind and seismic loads are required to receive the blast loads that are applied to the exterior façade and transfer them to the building's foundation. This load path is typically through the floor slabs that act as diaphragms and interconnect the different lateral resisting elements.

Unlike seismic hazards, which apply base acceleration to the entire building, blast loading is most intense opposite the event and diminishes with distance. As a result, structural damage is typically localized to the columns and bays directly opposite the detonation. Nevertheless, the lateral load resisting system for the building must be checked to make sure global structural stability is preserved. Since it is uneconomical to design a structure to remain entirely within its elastic range in response to an extraordinary loading, limited inelastic deformation is permitted for different structural systems. These inelastic deformations may produce severe cracks to the structural and non-structural elements.

The blast induced base shears may be approximated by treating the fundamental frequency of the entire structure as a single degree of freedom (SDOF) system in response to the total impulse applied to the blast loaded face of the building. The blast induced base shear is then a function of the period of response (T), the applied impulse (I) and the acceptable level of inelastic deformation expressed in terms of global deformation ductility (μ). The global deformation ductility is analogous to the Response Modification Coefficient (R) that is used in seismic design.

$$\text{Blast Induced Base Shear} = \frac{3\,\pi\,I}{2\,T\sqrt{2\,\mu-1}}$$

In addition to the hazard of impact by façade debris propelled into the building or roof damage that may rain down, the occupants may also be vulnerable to much heavier debris resulting from structural damage. Progressive collapse occurs when an initiating localized failure causes adjoining members to be overloaded and fail, resulting in an extent of damage that is disproportionate to the originating region of localized failure. The initiating localized failure may result from a sufficiently sized parcel bomb that is in contact with a critical structural element or from a vehicle sized bomb that is located at a short distance from the structure.

Nevertheless, whether initiated by localized failure or initiated by widespread damage, structural collapse must be prevented. Transfer girders, unreinforced masonry load-bearing walls and precast panelized construction may produce structural systems that are not tolerant of localized damage conditions. The columns that support transfer girders and the transfer girders that are critical to the stability of a large area of floor space are particularly vulnerable

to short standoff explosive events, such as satchels placed in contact with the columns or detonated within vehicles adjacent to the structure. Unreinforced masonry load-bearing walls and panelized precast construction that relies on individual structural panels that may not be sufficiently tied together to resist the collateral large structural deformations associated with an exterior explosive in the vicinity of the building.

Structural elements are classified as primary and secondary based on their influence area. Failure of floor systems which span between girders and column lines are likely to be localized whereas failure of girders, columns and the lateral load resisting system are likely to precipitate more extensive collapse or instability. Greater levels of damage are permitted for secondary structural elements as compared with primary structural elements, particularly when the effects of a specific threat are localized to a single bay of the building.

A-7.4 Prevention of Progressive Collapse

The threat independent prevention of progressive collapse through an alternate load path approach improves the redundancy and resiliency of the building, regardless whether the specified threats are able to cause the postulated initiating damage. The likelihood of catastrophic collapse resulting from a localized failure will be reduced when the structure is designed to withstand the isolated removal of a key structural element or detailed to engage adjacent structural elements in a damage state condition. In many cases, this threat independent approach assumes each floor will be able to bridge over the missing column. This may be achieved using a traditional moment frame system; however, the frame will likely require special ductile connection details that are capable of developing the capacity of the members. Other approaches may introduce trusses or girders at the roof or intermediate floor levels from which the building columns may be hung following the removal of a lower floor column; however, this requires tension splices in every column. Other structural systems may also be used to demonstrate the fault tolerance of a structure.

The alternate load path approach is required for every exterior column up the height of the building as described in Chapter 7, unless VA determines that it may be limited to only the exterior ground floor columns along with the use of a structural system at the exterior of the building that can redistribute gravity loads to adjacent structural elements following the removal of a column or loadbearing wall. The spacing of load redistribution systems up the height of the building are limited to three floors.

Many of the prescriptive tie force methods effectively protect interior structure because it is surrounded by adjacent bays that can develop the large in-plane forces; however, the effectiveness of the tie force methods is limited in the corner bays of buildings. Buildings that are surrounded by low-rise podium structure are to be protected against the removal of an exterior column above the podium. Buildings that are cantilevered from an interior column line

may not require the threat independent alternate load path design when the interior bays are sufficiently recessed within the building footprint; however, they would be subjected to the tie-force design requirements. It may not be feasible to renovate existing buildings to satisfy the alternate load path or tie force design methods; however, a decision by VA to forgo such a structural renovation will be based on an engineering evaluation of the existing structure.

8 UTILITIES AND BUILDING SERVICES

8.1 Scope, Purpose, and Goals

This chapter describes physical security and resiliency requirements for utility systems which include but are not limited to potable water, industrial water, fire protection water, sanitary sewer, storm sewer, natural gas and other fuels, steam, chilled water, liquid oxygen tanks, electrical power, and telecommunications. Site utility entrances may include utility-owned service and metering equipment. These requirements are applicable to MC Facilities and LSP Facilities with MC Utilities/Systems Redundancies. Where requirements are applicable to or modified for LSP Facilities, it is specifically indicated.

As stated in Chapter 1, the requirements in this manual apply to new buildings, additions, and existing facilities undergoing renovations. Further clarification on applicability to renovation projects is provided in table 2-1 and in the gray box describing alteration/renovation of existing facilities at the end of each major section.

The requirements of this chapter are baseline physical security and resiliency requirements. A risk assessment during the project planning phase is allowed to evaluate the deletion or incorporation of other specific requirements (see section 2.3 Exceptions and Deviations). The VA AHJ, defined in section 1.3 Administration and Enforcement, overseeing implementation of physical security and resiliency requirements for the facility will review submitted request for deviation from the baseline requirements of this chapter. When no risk assessment is performed, these baseline requirements apply.

The requirements of this chapter supplement other related VA standards for construction, space and facility planning criteria, design guides, design manuals, specifications, and details, which remain in full force and effect. Specifically, all requirements of VA Handbook 0730, Security and Law Enforcement, Appendix B, (which covers physical security requirements for VA facilities), the VA Fire Protection Design Manual (which covers all VA construction), and ICT standards on the TIL remain in effect.

The system design concepts described herein provide enhanced abilities for continued operations and concurrent maintainability. As such, when these concepts can be implemented at no additional cost or are deemed to be lifecycle cost effective during the holistic design process of a LSP facility, such provisions must be made as project betterments. Refer to the Annex to Chapter 8 for concepts background, intent, and strategies for implementation.

Paramount to all criteria, equipment and services required to keep a facility in operation must not be located in site-specific high-risk areas.

8.2 Utility Entrances

8.2.1 Mechanical

8.2.1.1 Alternate Connections for Steam and Chilled Water: Provide means for the rapid connection of an alternate source, such as a mobile boiler, chiller, or cooling tower, in emergency situations.

8.2.1.2 Water Service: Provide a minimum of two full demand water service connections to the campus feed from either separate source (when cost effective) or two separate connections to a single multi-sourced network. Full demand includes potable, industrial, and fire protection water. Service connections must enter the campus at separate protected (paragraph 8.2.1.3) locations through separate isolation valves. The purpose of this provision is to provide an uninterrupted supply of potable water or permit swift service restoration in the event of a water main break or contamination of one source. When two separate water connections, as described, are not reasonably available for an outside provider, an onsite source, such as a water well with treatment means, must serve as the second source. (See section 8.5 Water and Fuel Storage for onsite water storage requirements). For facilities with only one community-provided source/service connection and where the installation of a water tower or well is infeasible, an alternate source service connection must be provided to serve as the secondary connection for supplemental external source.

Potable water distribution loop and the industrial/fire protection loop must be separated to accommodate improved water turnover and quality in the system. The separation of supply must include an evaluation of line sizing to ensure piping is appropriately sized for actual usage with some expansion but not oversized.

8.2.1.3 Protection of Utility-Owned Service Equipment: To mitigate the risk of flooding[33] of utility-owned service equipment installations must:

- Not be located in the 100-year floodplain or within applicable storm surge (regardless of the facility type). Data from recent floods and storms, as well as available future projections, must be evaluated for implementation of flood mitigation measures to protect the equipment.
- Have equipment above grade such that a localized compartment flood from any source of water cannot occur (examples are higher elevation piped systems, rain, and drainage system backups).

[33] Coordinate with the requirements of section 1.6.2 Facilities in Floodplains.

- Be protected from higher hurricane flood surge (level) for facilities in hurricane prone areas.

For physical protection, this equipment must be located within a building envelope, when possible. When not located within the building envelope, this equipment must be protected in accordance with the requirements of Chapter 6 and located a minimum of 50 feet (15 m) in all directions from high risk areas.[34] Distribution cannot traverse high risk areas to serve downstream spaces. Coordinate with the serving utility.

Additional information may be found in the Annex to Chapter 8.

8.2.2 Electrical

8.2.2.1 Number of Services: Two utility services are required. Services must be from separate utility substations, when the availability of utility sources exists.

8.2.2.2 Separation of Services: Electric service feeders must be underground, located away from other utility services, and located away from high risk areas. Where dual service feeders are utilized, the two feeders must not occupy a common underground raceway system, and the independent raceways must be separated as far apart as is practicable and not less than 50 feet (15m) apart.

8.2.2.3 Protection of Utility-Owned Service Equipment: To mitigate the risk of flooding[35] of utility-owned service equipment, installations must:

- Not be located in the 100-year floodplain or within applicable storm surge (regardless of the facility type). Data from recent floods and storms, as well as available future projections, must be evaluated for implementation of flood mitigation measures to protect the equipment.
- Have equipment above grade such that a localized compartment flood from any source of water cannot occur (examples are higher elevation piped systems, rain, and drainage system backups).
- Be protected from higher hurricane flood surge (level) for facilities in hurricane prone areas.

For physical protection, this equipment must be located within a building envelope, when possible. When not located within the building envelope this equipment must be protected in accordance with the requirements of Chapter 6, located a minimum of 50 feet (15 m) in all

[34] Refer to Glossary for the definition of high-risk areas.
[35] Coordinate with the requirements of section 1.6.2 Facilities in Floodplains.

directions from high risk areas. Distribution cannot traverse high risk areas to serve downstream spaces. Coordinate with the serving utility.

Additional information may be found in the Annex to Chapter 8.

8.2.3 Telecommunications

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

8.2.3.2 Separation of Services: Telecommunications cable pathways must be underground, located away from other utility services, and located away from high risk areas.

Where more than one service is obtained, services must be separated by a minimum distance of 66 feet (20 m).

8.2.3.3 Redundant Service Paths to Entrance Rooms: Entrance Rooms are the separation point between utility-owned and VA-owned equipment. Telecommunications cable pathways must be designed to provide redundant services to the Entrance Room from the street or property line where the interface with the service provider takes place. Redundant service paths must be separated by a minimum distance of 66 feet (20 m) where possible.

8.2.4 Alteration/Renovation of Existing VA Facilities — Utility Entrances

Section 8.2.4 requirements apply only when undertaking a project with appropriate scope to address these issues. These upgrades are not retroactive supplemental requirements to projects of unrelated scope in existing facilities.

Facilities must comply with the redundancy requirements of: sections 8.2.1 Mechanical, 8.2.2 Electrical, and 8.2.3 Telecommunications.

Facilities must relocate existing mechanical and electrical equipment to comply with the requirements of sections 8.2.1.3 Protection of Utility-Owned Service Equipment (Mechanical) and 8.2.2.3 Protection of Utility-Owned Service Equipment (Electrical). Where existing equipment cannot be relocated to within an existing building envelope, protect the equipment with screen walls or barriers that comply with Chapter 6 Building Envelope and Chapter 7 Structural System.

8.3 Site Distribution

8.3.1 Mechanical

8.3.1.1 Steam, Chilled Water, Water, and Fuel System Distribution: Distribution systems must be underground direct buried or located in a structure or above ground but must not be exposed. The systems must be looped or grid distribution systems, such that an interruption at any one point can be isolated and service maintained to the facility. System piping shall not be located in high risk areas, and must include, particularly for fuel systems, enhanced capability to resist external forces such as explosive threat from vehicles.

8.3.1.2 Separation of Sanitary Sewer and Storm Drain Systems: Sanitary sewer and storm drain systems must be separate.

8.3.2 Electrical

Pad-mounted outdoor electrical equipment is not permitted, unless protection equivalent to indoor installation is provided.

8.3.2.1 Separation of Feeders: For the intent of protected redundancy, feeders that form a primary selective pair cannot be located closer than 50 feet (15 m) to each other, must be installed in concrete-encased duct banks, and enter served buildings at different locations. Feeder entry points must maintain a minimum distance of 50 feet (15 m) or greater in all directions from the loading dock, mailroom, or other high-risk areas.

8.3.2.2 Location of Distribution Equipment:[36] All electrical distribution components, such as medium- and low-voltage switchgear and transformers, must:

- Not be located in the 100-year floodplain or within applicable storm surge (regardless of the facility type). Data from recent floods and storms, as well as available future projections, must be evaluated for implementation of flood mitigation measures to protect the equipment.
- Be protected from higher hurricane flood surge (level) for facilities in hurricane prone areas.

8.3.2.3 Manhole and Handhole Covers: Manholes and handholes must be equipped with lockable covers.

[36] Coordinate with the requirements of section 1.6.2 Facilities in Floodplains.

8.3.3 Telecommunications

Section 8.3.3 has been coordinated with the 2016 Telecommunications Design Manual (TDM).

8.3.3.1 Telecommunications Systems Distribution: An underground ring topology must 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 must be based on a 40 percent fill, and there must be a minimum of two spare four-inch (100 mm) conduits between buildings. Conduits must be encased in concrete. Distance between manholes or handholes must not be greater than 400 feet (122 m).

8.3.3.2 Separation of Pathways: Pathways must not be located closer than 50 feet (15 m) to each other; pathways must enter served buildings at different locations and must not be exposed on the building exterior. Quantity and size of conduits will be determined by site design. Telecommunications entry points must maintain a minimum distance of 50 feet (15 m) or greater in all directions from the loading dock, mailroom, or other high-risk areas.

8.3.3.3 Location of Telecommunications Equipment: All telecommunications components other than inter-building cabling must be located 3 feet above the 100-year floodplain, above grade, and within a building envelope.

8.3.3.4 Manhole and Handhole Covers: Manholes and handholes must be equipped with lockable covers.

8.3.4 Alteration/Renovation of Existing VA Facilities — Site Distribution

Section 8.3.4 requirements apply only when undertaking a project with appropriate scope to address these issues; these upgrades are not retroactive supplemental requirements to projects of unrelated scope in existing facilities.

Facilities must provide secured emergency connections for electricity, steam, and all water systems.

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 Chapter 6 Building Envelope and Chapter 7 Structural System.

8.4 Energy Center

8.4.1 Requirements

The Energy Center contains utility production and distribution equipment, as well as incoming services from offsite utility providers, and is responsible for providing utility services during

normal operating conditions as well as during and after manmade and natural 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 from the Energy Center and the facility are typically electricity, steam and condensate return, heating hot water supply and return, and chilled water supply and return. The requirements of this section apply to configurations of centralized plants serving campuses and to decentralized applications of the same types of equipment located in end-use buildings.

8.4.2 Sustained Service

The Energy Center must sustain utility services for a minimum time period of 96 hours.

8.4.3 Standby Electrical System

Refer to 9.3.1 Standby Electrical System.

8.4.4 Long-Replacement-Time Equipment

For equipment that has a long replacement time, provide for additional physical protection and/or installation of redundant equipment (such as, physically separated distributed N+1 strategies) or connections (to facilitate portable temporary plant equipment such as truck mounted air-cooled chillers) that will alleviate extended shutdown time. Examine the added capital expense of options such that the cost of strategies does not exceed 20 percent of the protected base-load equipment.

8.4.5 Alteration/Renovation of Existing VA Facilities — Energy Center

Section 8.4.5 requirements apply only when undertaking a project with appropriate scope to address these issues; these upgrades are not retroactive supplemental requirements to projects of unrelated scope in existing facilities.

Facilities must comply with the requirements of section 8.4.2 Sustained Service, and section 8.4.3 Standby Electrical System.

8.5 Water and Fuel Storage

Designers must base the water and fuel storage needs on the number of people anticipated to be on the site during an event. Additional information may be found in the Annex to Chapter 8.

8.5.1 Requirements

Storage must be provided for potable and industrial water, fire protection, wastewater, and contaminated water, and fuels for use during the period under which offsite utilities are unavailable. At a minimum, water and generator fuel storage must support 96 hours of

operation, and boiler fuel storage must support 10 of the most extreme days of operation in the heating season. Additional information may be found in the Annex to Chapter 8.

8.5.2 Storage Volume Criteria

Designers must adjust potable and industrial water storage criteria and obtain approval from the AHJ as follows:

- Whenever the possibility of natural disasters such as hurricanes, earthquakes, flooding, and fire dictate an increase in the storage volume requirements.
- Separate storage of potable and industrial/fire protection water reserves must be provided for benefits of physical modularity and maintaining potable water quality. A successful mitigation strategy will reduce potable water storage such that the tank retention time during normal use periods is much less than chlorination decay time for the average stored water temperature.
- Potable and industrial water storage can be reduced by implementing water conservation strategies. An Emergency Water Supply Plan (EWSP) must be developed and approved by the AHJ as part of the facility's Emergency Operations Plan (EOP), refer to Chapter 2. The EWSP must be approved in writing at the planning stage of the project. Plans must include strategies and implications similar to the following:
    - Quantify critical medical water consumption, such as for dialysis, sterilization, and when present, once-through water cooled equipment.
    - Quantify food service operations and functions that can be reduced (such as, dishwashing).
    - During a water shortage, area(s) of the facility may be shut down, or showers shut down, or certain fixtures isolated.
    - VA hospitals cannot shut down the air conditioning to buildings to save air conditioning industrial water; some level of air conditioning for dehumidification must be maintained even to unoccupied buildings to prevent mold. Various strategies are available to achieve this performance such as:
        - Raising indoor temperature setpoints to 78-82 deg F (25-28 deg C).
        - Reducing evaporative equipment and boiler make-up demand by increasing cycles of concentration.
        - Utilizing supplemental air-cooled equipment.
        - Utilizing desiccants.

Additional information may be found in the Annex to Chapter 8.

8.5.2.1 Water and Waste-Water: Minimum criteria to be used in determining storage requirements are as follows.

8.5.2.1.1 Potable water: Potable water requirements vary between VA facilities and depend upon the number of persons expected to remain at the facility throughout the emergency. The requirements for potable water storage will be estimated at 40 gallons (150 L)/person/day for 4 days under emergency preparedness plan operations, unless facility calculations approved by the Emergency Management Committee are able to justify reduced consumptions. This calculation applies to one person at the facility 24 hours or 3 people working 8-hour shifts in one day. The director of the facility, in consultation with the area emergency manager, must provide an estimate of the total number of people expected to be on the site, including patients or residents, staff, family members (of patients, residents, and staff), visitors, and potential "refugees." Additional information is found in the Annex to Chapter 8. Additionally, if the facility can demonstrate water supply from a resilient source such as an onsite well or separate utility supplier, a reduction in storage may be requested through the VHA Healthcare Engineering Oversight Committee on Physical Security and Resiliency.

8.5.2.1.2 Industrial water: Industrial water requirements include but not limited to cooling tower and boiler make-up water. Mathematically model the total annual (8,760 hour) water consumption profile with the facility's emergency water conservation measures as noted in the Emergency Operations Plan (EOP) in effect. The industrial water storage requirement is the volume of the greatest 96-hour consumption period. Calculate site-specific industrial water requirements for new facilities needed to keep industrial water system in operation. For existing facilities, obtain metered water consumption data to calibrate models and calculations and then derive new requirements via calculations for new (proposed) construction and operating parameters. Additional information is found in the Annex to Chapter 8.

8.5.2.1.3 Fire protection water: Provide a minimum volume of storage water to fight a single fire for the worst-case scenario on the campus. Include MC Facilities, LSP Facilities with MC Utilities/Systems Redundancies, and LSP facilities in determining the worst-case fire scenario. This quantity represents the volume required exclusively for fire protection and cannot be used to fulfill the requirements for any other water system design volume. The volume of fire protection water cannot be adjusted lower than the calculated requirement.

Facilities must be sprinkler protected throughout. Additional information is found in the Annex to Chapter 8.

Use Table 8-1 to determine minimum storage for non-sprinkler protected facilities and use Table 8-2 for sprinkler protected facilities in calculating the single worst-case fire scenario.

Table 8-1 Non-Sprinkler Protected Facilities

NFPA 13 Hazard	Minimum Flow for Favorable Conditions [a] gpm (L/s)	Minimum Flow for Unfavorable Conditions [b] Gpm (L/s)	Duration [c] minutes	Total Minimum Storage Volume Gallons (Liters)
Light Hazard Patient Buildings, Offices, Quarters	1,250 (79)		60	75,000 (284,000)
Light Hazard Patient Buildings, Offices, Quarters		1,500 (95)	120	180,000 (680,000)
Ordinary Hazard Laboratory Buildings, Shops, Laundries	1,250 (79)		60	75,000 (284,000)
Ordinary Hazard Laboratory Buildings, Shops, Laundries		2,000 (126)	120	240,000 (910,000)
Extra Hazard Warehouses	1,500 (95)		60	90,000 (340,000)
Extra Hazard Warehouses		3,000 (190)	120	360,000 (1,360,000)

a. See VA FPDM 7th Edition section 5.2.A.1 Capacity
b. See VA FPDM 7th Edition section 5.2.A.2 Capacity
c. See VA FPDM 7th Edition section 5.4 Duration

Table 8-2 Sprinkler Protected Facilities

NFPA 13 Hazard	Storage Volume [a] Gallons (Liters)
Light Hazard	24,000 (91,000)[b]
Ordinary Hazard	49,500 (188,000)[c]
Extra Hazard	180,000 (680,000)[d]

a. Densities and areas are from NFPA 13, but the hose stream allowances and durations have been adjusted to address VA requirements.
b. Based on the following: 0.1 gpm/ft^2 over 1500 ft^2 plus 250 gpm hose stream for 60 minutes
(4.1 (L/min)/m^2 over 139 m^2 plus 15.8 L/s hose stream for 60 minutes)
c. Based on the following: 0.2 gpm/ft2 over 1500 ft2 plus 250 gpm hose stream for 90 minutes
(8.1 (L/min)/m2 over 139 m2 plus 15.8 L/s hose stream for 90 minutes)
d. Based on the following: 0.4 gpm/ft2 over 2500 ft2 plus 500 gpm hose stream for 120 minutes
(16.3 (L/min)/m2 over 232 m2 plus 31.5 L/s hose stream for 120 minutes)

For Extra Hazard, the default design demand is 0.4 gpm/ft^2 over 2500 ft^2. However, where the largest demand for the campus is known to be less, the lesser demand can be substituted provided that the hose stream allowance and duration remain 500 gpm and 120 minutes respectively.

Requirements for fire protection water storage are based on the assumption that there will be only one fire at a time. The calculations assume that the water supply from offsite public water provider(s) will not be available. The water supply from onsite water sources, such as groundwater wells, will only be included in the calculations when it can be documented that the water source, pumping facilities, and conveyance system are designed and constructed to provide continued operation during the emergency event.

8.5.2.1.4 Wastewater retention: Wastewater storage requirements must be sized to accommodate “black water” sanitary sewer flows anticipated from the potable water system, based on the same assumptions as the potable water calculations under emergency preparedness plan operations. Use of expandable storage bladders is an acceptable alternative to permanent tanks. Documentation of emergency grey water dumping (such as cooling tower blowdown) strategies for flood prone locations must be reviewed with local regulating authorities, and permitted if required.

A waiver of this requirement may be granted where confirmation that the municipal sewer authority has either (1) not experienced a flood or surcharge in the portion of its network that serves, or is anticipated to serve, the VA facility; or (2) has the ability to receive the facility’s discharge waste volume equal to 4 days under emergency preparedness plan operations. This confirmation of historic experience and capability must be written in the VA facility’s risk assessment. Additional information is found in the Annex to this chapter.

8.5.2.1.5 Contaminated water: The Architect-Engineer designer of record must contact the local water & wastewater utility provider(s) as well as state and/or local authorities to determine if direct discharge of wastewater from patient decontamination operations is allowed or if containment is required. Based on the input from state and local authorities and discussion with VA GEMS and OEM staff either a method for containment must be provided or a discharge approval

letter obtained allowing direct discharge, in compliance with Federal, local and State environmental regulations.

8.5.2.1.5.1. Mass Casualty Decontamination Program Sites. Designated sites that are implementing VHA's mass-casualty decontamination program must include provisions for containment of water contaminated with hazardous material(s) or obtain approval for discharge as noted in 8.5.2.1.5. Determination as to actual provision must be based upon direction from state and local officials as noted above.

8.5.2.1.5.2. Individual Decontamination. Emergency Departments or other VA departments/functions which have individual decontamination units (e.g. the male and female decontamination showers required in Emergency Departments) will be provided with containment provisions for contaminated effluent *if required, as* determined by the AE coordination with state and local officials as noted above.

8.5.2.2 Water Level Monitoring: Water level of a dedicated fire protection storage tank must be remotely monitored in accordance with NFPA 22 and NFPA 72 at a constantly attended location, preferably at the Engineering Control Center (ECC), Boiler Plant, or other 24-hour staffed location. All other water storage tank(s) including those combined with fire protection water must be equipped with water level monitoring through the building control system or the fire alarm system at a constantly attended location, preferably at the Engineering Control Center (ECC), Boiler Plant. In locales subject to freezing, water temperature of above-ground storage tanks must be monitored at a constantly-attended location.

8.5.2.3 Generator Fuel: A peak summer and winter consumption profile measured in gallons per hour must be normalized over a seven-day period; the profile with the greatest consumption must be used to determine generator fuel storage requirements. Boiler and generator fuel storage may be combined as allowed by applicable codes and operational criteria.

8.5.2.4 Boiler Fuel: Facilities using coal as the main fuel normally store a sufficient supply of fuel to meet the normal demands of continuous operation for a period of 15 most extreme days of the heating season. Facilities firing oil as the main fuel must maintain a supply of fuel sufficient to meet the normal demands of continuous operation for a period of 15 most extreme days of the heating season. Plants that generate less than 50 percent of their annual steam demand by natural gas for two consecutive years are to be considered as burning oil only. Facilities firing natural gas as the main fuel, with oil or propane back-up, normally maintain a sufficient supply of

back-up fuel to meet the normal demands of continuous operations for a period of 10 most extreme days of the heating season. (See VHA Directive 1810 Boiler Plant Operations.)

8.5.3 Water Storage Emergency Connection

The water storage system must include emergency connections to allow for a change in supply source or change in delivery points. Develop a site-specific emergency preparedness plan to document water demands and source connections to be utilized under various events. The plan must document water consumption reduction strategies and indicate separate demands for potable and industrial uses. Plan and provide separate supply taps and diversified (multiple/modular) storage for potable and industrial uses (see section 8.5.2 Storage Volume Criteria).

8.5.3.1 Supply Source: Source of water into the facility system. A change in supply source allows the facility to receive water from various planned sources, for example, the public utility, an onsite well, an onsite pond (or lake or river) with piped connection, an onsite pond by mobile pump unit (fire truck), or by tanker truck. The change in sources requires a plan for dealing with a possible difference in source water quality and may require different treatment (for example, filters, softeners, chemical). Potable water distribution loop and the industrial/fire protection loop must be separated to accommodate improved water turnover and quality in the system.

8.5.3.2 Delivery Points: Points of supply into the facility and consumption of water throughout the facility. The emergency management plan must include logistics to accommodate a change in delivery points as: (1) various sources, (2) failure in source delivery point, and (3) reduce consumption and conserve pressure based on the reduced flow or change in booster pumping. Storage tank(s) may be out of service for a variety of reasons and supplies must be capable of a bypass directly to the facility.

8.5.4 Onsite Water Well

Where available and permitted, use an onsite water well as an alternate source for potable, industrial, and fire protection water storage. The water supply from onsite water wells will only be included in the calculations when it can be documented that the water source, pumping facilities, treatment, conveyance system, and storage reservoirs are designed and constructed to provide continued operation during the emergency event and meet the peak water demand criteria listed in section 8.5.2 Storage Volume Criteria. Water buffer tanks are be required to allow a balanced flow through pipelines, maintain pressure in distribution system, and serve as a buffer between the source, treatment plant, and consumer(s). Where water from onsite wells is included in the Emergency Operations Plan, all equipment necessary to operate the

system from source to points-of-use must be powered by the standby electrical system when the normal power system is disabled.

8.5.5 Electrical Power

All electrical equipment necessary to operate stored water and fuel systems must be backed by the standby electrical system. Refer to section 1.4.1 for Physical Security and Resiliency Designations for VA Facilities, and this section for specific utility storage requirements.

8.5.6 Existing Facility – water and Fuel Storage

Sites supporting MC Facilities and LSP Facilities with MC Utilities/Systems Redundancies must comply with the requirements of section 8.5 Water and Fuel Storage.

8.6 Protection of Utilities and Equipment

Protect all water and fuel storage, water/fuel pumping, metering, and regulating equipment with blast-resistant screen walls or barriers that comply with section 6.2 Non-Load Bearing Exterior Walls and section 7.2.4 Screen Walls and Penthouse Structure. At-grade storage or supporting equipment must comply with section 3.3 Standoff Requirements and section 3.6 Anti-Ram Rated Vehicular Barriers. For elevated water towers, fence is acceptable as a barrier and a blast resistant wall is not required. All tanks must remain functional and accessible during emergencies.

Underground storage vaults must be watertight, and tanks secured to prevent buoyancy. When located beneath roadway or surface parking, adequate blast protection must be provided against a potential blast from vehicle above in accordance with section 7.2.5 Buried Utilities and Buried Equipment. Intakes and vents for vaults must be located above grade, above the base flood level elevation, unobstructed, and in areas not subject to flooding.[37] Secure underground storage tanks to prevent buoyancy. Provide electronic security system for access control, intrusion detection, and monitoring of the critical equipment in accordance with Chapter 10.

[37] Coordinate with the requirements of section 1.6.2 Facilities in Floodplains.

Annex to Chapter 8

A-8.1 Scope, Purpose, and Goals

The system design concepts described herein provide enhanced abilities for continued operations and concurrent maintainability; as such, when these concepts can be implemented at minimal additional cost or are deemed to be lifecycle cost effective during the holistic design process of a LSP facility, such provisions are to be made as project betterments.

A-8.2.1.3 and A-8.2.2.3 Protection of Utility-Owned Service Equipment

To mitigate the risk of flooding of utility owned service equipment, installing above the 100-year floodplain reduces the likelihood of rising water from disabling equipment. Constructing equipment enclosures such that any water that does enter the space is able to drain by gravity is important for all spaces regardless of their elevation relative to the estimated flood plain. The intent of this requirement is to be informed of and prevent the recurrence of an event that happened in a federal facility where a main electric room flooded even though the entrance was several feet above a local flood event (Federal Triangle Department of Justice Building, Washington, D.C., 2006). The primary issues were that the floor elevation was lower, the room did not drain, and piping which did not serve the space transited the space. During a short duration, moderately heavy rain event, the exterior storm sewer in the street became surcharged and water backed-up through the building's internal storm piping and at one location, where a cleanout cover had been improperly installed on this 15-inch pipe, catastrophic flows forced the cover off, entered the protected space, and damaged all equipment. The duration of the flood in the street was only a matter of minutes. An estimated 3.5 million gallons of water entered the basement. The adjacent IRS building suffered more extensive damage with water penetration admittance to the perimeter moats, thus creating excessive hydrostatic pressure on lower level window assemblies and their ultimate failure.

A-8.5 Water and Fuel Storage

The director of the facility, in consultation with the area emergency manager, must provide an estimate of the total number of people expected to be on the site, including: patients, residents, staff, family members (of patients, residents, and staff), visitors, potential "refugees", first responders, and additional medical/DEMPS personnel. Standards of the Joint Commission (TJC) require hospitals to address the provision of water and utilities as part of the facility's Emergency Operations Plan (EOP). TJC requires that the EOP state how a hospital will manage utilities during an emergency. In accordance with TJC, the EOP identifies the hospital's capabilities and establishes response procedures for when the hospital cannot be supported by the local community in the hospital's efforts to provide communications, resources and assets, security and safety, staff, utilities, or patient care for at least 96 continuous hours.

A-8.5.1 Requirements

The potable water system must meet the requirements of VHA Directive 1061, *Prevention of Healthcare-Associated Legionella Disease and Scald Injury from Potable Water Distribution Systems*, dated August 13, 2014, and all updated policy requirements.

A-8.5.2 Storage Volume Criteria

Past experience shows that VAMCs are experiencing legionella mitigation challenges with a large, single water storage tank, and the large size being determined in part by high industrial water demands. This situation is exacerbated in warmer climates.

To guide facility managers in the assessment of water storage needs, the Department of Health and Human Services (HHS) along with The Centers for Disease Control and Prevention (CDC), and the American Water Works Association (AWWA) published the *Emergency Water Supply Planning Guide for Hospitals and Health Care Facilities*. The objective of this guide is to help health care facilities develop a robust EWSP and provide a detailed methodology for identifying: current water use, minimum water needs, emergency water conservation measures, and alternative water supplies. The resulting EWSP must be included in the project's basis of design and the facility EOP.

A-8.5.2.1.1 Potable Water

VA commissioned a *Pilot Study of Emergency Power and Water Supply during Natural Disasters* and reviewed water supply requirements at 25 separate medical centers in hurricane prone areas. The study concluded that the minimum potable water requirements during contingency operations ranged from 40 - 50 gallons/person/day. A 20 gal/person/day lower end can be achieved as various emergency operational measures are employed consistent with the resulting project specific EWSP. Regarding the lower end of the range, from the EPA's *Planning for an Emergency Drinking Water Supply* (EPA 600/R-11/054, June 2011): "There are a range of values that are suggested for an emergency water supply (for example, 0.5 gallons per person per day to 5 gallons per person per day) depending on whether water for non-drinking purposes (such as food preparation and hygiene) is included in the estimate. The value of 1 gallon per person per day (USACE 2006) is a plausible planning number, consistent with the Federal Emergency Management Agency (FEMA), EPA, and the Red Cross estimates for drinking, food preparation, and hygiene related to health and safety. [Oxfam (2010) indicates 15 L per person-day. *Water, Engineering and Development Centre* (Reed and Shaw 1999) suggests 3 to 5 L per person-day and FEMA (2004) indicates 1.5 gallon (5.5 L) per person-day.]"

A-8.5.2.1.2 Industrial Water

This requirement was derived from the *Pilot Study of Emergency Power and Water Supply during Natural Disasters*. The study also concluded that it was necessary for the HVAC systems to be in continuous operation, not only to maintain comfortable temperatures for effective patient care and serve critical equipment and process needs, but also to dehumidify the buildings to lessen potentially destructive mold growth caused by loss of power and air conditioning in high humidity climates. Depending upon regional climatic conditions, this may not be the case in all geographic locations.

A-8.5.2.1.3 Fire Protection Water

Densities and areas are from NFPA 13, but the hose stream allowances and durations have been adjusted to address VA requirements.

Installing fire sprinklers in an existing non-sprinkler protected building may be a more cost-effective solution than excessively increasing the amount of water storage.

A-8.5.2.1.4 Wastewater Retention

This requirement was derived from the *Pilot Study of Emergency Power and Water Supply during Natural Disasters* assuming that municipal lift stations and plants would fail during a disaster, and that VA would not allow wastewater (containing biological, radiological, chemical, or heavy metal) to be discharged into the surrounding neighborhood. When the facility's waste drains by gravity to the treatment plant or there is sufficient storage volume in the piping systems, wastewater retention storage may be reduced.

A-8.5.2.1.5 Contaminated Water

The Architect-Engineer designer of record, in coordination with VAMC's Green Environmental Management System (GEMS) Coordinator, must contact the local water & wastewater utility provider(s) as well as state and/or local authorities to determine if direct sanitary sewer discharge of wastewater from medical facility-based First Receivers-Level patient decontamination operations is allowed or if collection and containment is required (examples of patient decontamination systems that may be connected to the sanitary sewer include but are not limited to; mobile patient decontamination systems, skid mounted decontamination units, fixed internal decontamination showers (e.g., those found in Emergency Departments or industrial hazard areas)). Based on the input from State and local authorities, and in coordination with VAMC GEMS and Emergency Management staff, either a method for collection and containment must be provided or an approval letter obtained allowing direct discharge into the sanitary sewer, in compliance with Federal, local and State environmental regulations. NOTE: If approved for direct discharge into the sanitary sewer, wastewater retention requirements in section 8.5.2.1.4 apply.

9 BUILDING SYSTEMS

9.1 Scope, Purpose, and Goals

This chapter describes physical security and resiliency requirements including mechanical building systems (fuels, steam, hot and chilled water), building plumbing systems (potable water, fire protection water, sanitary sewer, and medical, dental and laboratory gases and vacuum systems), building water storage systems (potable and industrial water storage tanks, water wells, pumps, and water purification systems), building electrical power distribution systems, standby electrical systems, uninterruptible power supply (UPS) systems, building telecommunications systems, vertical transport, and pneumatic tube systems. These requirements are applicable to MC Facilities and LSP Facilities with MC Utilities/Systems Redundancies. Where the requirements are applicable to or modified for LSP Facilities, it is specifically indicated. Paramount to all criteria, equipment and services required to keep a facility in operation must not be located in high-risk areas.

As stated in Chapter 1, the requirements in this manual apply to new buildings, additions, and existing facilities undergoing renovations. Further clarification on applicability to renovation projects is provided in table 2-1 and in the gray box describing alteration/renovation of existing facilities at the end of each major section.

The requirements of this chapter are baseline requirements for physical security and resiliency. A risk assessment during the project planning phase is allowed to evaluate the possible deletion or incorporation of other specific requirements (see section 2.3 Exceptions and Deviations). The VA AHJ, defined in section 1.3 Administration and Enforcement, overseeing implementation of physical security and resiliency requirements for the facility will review submitted request for deviation from the baseline requirements of this chapter. When no risk assessment is performed, these baseline requirements apply.

The requirements of this chapter supplement other related VA standards for construction, space and facility planning criteria, design guides, design manuals, specifications, details, and published national policies, which remain in full force and effect. Specifically, all requirements of VA Handbook 0730, Security and Law Enforcement, Appendix B, (which covers physical security requirements for VA facilities), the VA Fire Protection Design Manual (which covers all VA construction), and ICT standards on the TIL remain in effect.

9.1.1 Modularity

Component modularity of major mechanical, electrical, and telecommunications systems is an overarching physical security and resiliency precept, which depends on building systems designed and constructed from interchangeable components. Modularity is also integral to the

VA Hospital Building System (VAHBS).[38] Building systems for facilities must employ the principles of modularity outlined in the VAHBS. The predominant objectives of VAHBS modularity are cost control, improved performance, adaptability, and the provision of a basis for building development and modification. The physical security resiliency benefits of VAHBS modularity include 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 resiliency as well as future expansion.

9.1.2 Security Considerations

Refer to Chapter 5 Functional Areas, Chapter 10 Security Systems, and Appendix A Security Door Opening Matrix, and Appendix B Security System Application Matrix, for construction and security requirements for mechanical, electrical, and telecommunications service spaces.

9.2 HVAC Systems

9.2.1 Requirements

9.2.1.1 Equipment Location: Locate major mechanical equipment above the ground floor, above grade, and in an area not subject to flooding.[39]

9.2.1.2 Water Consumption: Coordinate configuration of HVAC systems consistent with the Emergency Water Supply Plan (EWSP) as described in Chapter 8 Utilities and Building Services of the PSRDM.

9.2.1.3 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, above grade, in an area not subject to flooding.[40] Where looped systems enter the building at two points, the emergency connections need only be installed on one entry.

9.2.1.4 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, standby and/or emergency generators, and other similar systems.

[38] See the Red Book and its Supplement, which describe integrated and modular design for new facilities.
[39] Coordinate with the requirements of section 1.6.2 Facilities in Floodplains.
[40] Coordinate with the requirements of section 1.6.2 Facilities in Floodplains.

9.2.1.5 Entrances and Lobbies: Maintain positive pressure in lobbies and entrance areas.

9.2.2 Intakes and Exhausts

9.2.2.1 Outdoor Air Intakes: All air intakes must 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.

- In addition to the minimum provisions of the International Mechanical Code and local jurisdiction code supplements, locate all outdoor air intakes a minimum of 50 feet (15 m) from areas where vehicles may be stationary with their engines running and similar locations of proximity to noxious discharges, exhaust from other (building) systems and devices, and other unmitigated contaminant sources.
- Locate all outdoor air intakes a minimum of 30 feet (9 m) above finished grade or on roof away from the roof line. Additionally, position bottom of intakes a minimum of one foot (300 mm) or the expected drifting snow depth, whichever is greater, above any building surfaces where water, snow or debris may accumulate.

9.2.2.2 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 standoff distance to the critical infrastructure within. (Refer to Chapter 6.)

9.2.2.3 Hurricane Areas: Louvers in areas prone to hurricanes or wind-debris hazards (in accordance with ASCE 7-10) must 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.

9.2.3 Alteration/Renovation of Existing Facilities — HVAC Systems

Requirements of sections 9.2.1.2 Water Consumption and 9.2.1.3 Emergency Connections apply.

Wind-driven rain and impact-resistant louvers, hardened plenums, and structured baffles, as described in section 9.2.2.3 Hurricane Areas, must be installed in the area undergoing renovation or when major equipment replacement is performed in areas prone to these hazards. (Refer also to Chapter 6 Building Envelope and Chapter 7 Structural System.)

9.3 Electrical Systems

9.3.1 Standby Electrical System

Standby generators are required to provide power for the entire facility load. The standby electrical system consists of generators, switchgear, fuel storage, and distribution equipment necessary to provide standby power to the facility. See also Chapter 5 for functional area requirements for the generators and equipment. The standby electrical system is not the same as the NFPA-required Essential Electrical System (EES), which supplies power to a specifically mandated set of healthcare facility loads. The standby electrical system is in addition to the EES.

It is permissible for the standby electrical system to provide power to the EES when the standby electrical system meets the requirement of the NFPA 99, NFPA 110, and other applicable codes.

Combined heat and power (CHP or cogeneration) may be considered per VA Directive 0055, in addition to the boiler and power generation equipment, because both steam and electricity are required year-round. CHP equipment is considered LSP, though this designation must not compromise protection of facility utilities, structures, and equipment.

9.3.1.1 Standby Generators: Generators for the standby electrical system must be diesel compression engine type, rated as defined by ISO 8528 as Emergency Standby Power or Limited Running Time Power as most applicable to project needs and goals. The standby power system and the EES may be combined when the system as a whole meets NFPA 99, NFPA 110, other applicable codes, and VA criteria. The standby electrical system generators must provide power at the highest practicable voltage level, preferably the medium voltage utility service entrance voltage, and be connected into the normal power electrical system at a point as close as possible to the utility service entrance. The designer is to develop a design based on actual project requirements and conditions, including utility demand data, operational considerations, projected load reductions or growth, emergency community support operations, and applicable codes and VA criteria.

9.3.1.2 Location: Generators, paralleling equipment, and associated fuel and electrical components for the standby electrical system and the EES must be located above grade and above the defined flood elevation[41] and within dedicated, environmentally-controlled structures or rooms. Standby electrical systems must be located a minimum distance of 50 feet (15 m) or greater in all directions from high risk areas.

[41] Coordinate with the requirements of section 1.6.2 Facilities in Floodplains

9.3.1.3 Emergency Connections: Include an exterior emergency quick connection and all associated equipment for the EES at or near the location of the EES distribution equipment.

9.3.2 Uninterruptible Power Supply

Provide uninterruptible power supply (UPS) equipment for critical telecommunications, computer, power quality-sensitive critical equipment and controls, and security systems and equipment. UPS equipment provides power during the time gap between loss of utility power and energization of the EES or standby electrical systems. UPS also provides power for an orderly shutdown of equipment in the event that EES or standby electrical systems do not operate properly.

9.3.2.1 Modularity: Where multiple UPS are used, that they must be of similar size and compatible manufacturer to allow for interchangeability.

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

9.3.2.3 Battery Runtime: Size battery systems for full rated output of duration as defined below; ***individual project needs may dictate a longer runtime***.

9.3.3 Alteration/Renovation of Existing Facilities — Electrical Systems

9.3.3.1 Standby Electrical System: Existing facilities in regions prone to hurricanes (in accordance with ASCE 7-10) and zones of Moderate-High or greater seismicity as designated by VA must comply with section 9.3.1 Standby Electrical System. Facilities outside these areas or zones are encouraged to comply with section 9.3.1 Standby Electrical System.

9.3.3.1 UPS: Existing facilities must comply with section 9.3.2 Uninterruptible Power Supply.

9.4 Telecommunications Systems

Refer to Chapter 5 for functional area requirements.

9.4.1 Entrance Room

The Entrance Room is where all telecommunications services from all service providers are delivered to the building and contains the separation points between utility-owned and VA-owned equipment and cabling.

9.4.1.1 Location: The Entrance Room must be located above grade and above the defined flood elevation, and within a building envelope. In tornado prone areas, a

below-grade location may be considered. The room must be located at least 50 feet (15 m) from high risk areas, must not be located within 25 feet (7.6 m) of an outside wall or delivery area, and must not be located directly below laboratories, kitchens, laundries, toilets, showers, or other areas where water service is provided. Entrance Rooms must be separated from other Entrance Rooms by a minimum distance of 66 feet (20 m).

9.4.1.2 HVAC: The Entrance Room must be provided with generator-backed HVAC service.

9.4.1.3 Power: All equipment in the Entrance Room must be powered from UPS equipment that will provide a minimum of 10 minutes of service at full rated output when only passive equipment is in the Entrance Room. When the Entrance Room contains active equipment, UPS equipment that will provide 10 minutes of service at full rated output is required. If no EES or standby power is to be provided to the Entrance Room, an assessment of the facility must be performed to determine the required UPS battery runtime. In cases where EES or standby power is not available, the UPS operating duration may be increased to 4 hours or more to meet mission needs.

- National Electrical Code Article 708, Critical Operations Power Systems: VHA has determined that facilities which have an Essential Electrical System (EES) have highly reliable electrical infrastructure. The additional cost of complying with National Electrical Code Article 708, Critical Operations Power Systems (COPS), is generally not warranted. However, a VHA facility of regional or national significance may conduct a risk assessment to determine if the power system serving the Entrance Room should be COPS-compliant; final determination will be made by the AHJ.

9.4.1.4 Conduit Pathways: Refer to the Telecommunications Design Manual.

9.4.1.5 Alteration/Renovation of Existing Facilities — Entrance Room

When there is no existing EES or standby power system OR if the existing EES cannot adequately support the equipment in the Entrance Room after the loss of utility power, an assessment of the existing facility must be performed to determine the required UPS battery runtime (i.e. which may be increased to meet mission needs).

9.4.2 Computer Room

The Computer Room contains all the main telephone switching and data processing equipment for the facility.

9.4.2.1 Location: The Computer Room must be located above grade and within a building envelope. The Computer Room must be located at least 50 feet (15 m) from

high risk areas; and must not located directly below laboratories, kitchens, laundries, toilets, showers, or other areas where water service is provided.

9.4.2.2 HVAC: The Computer Room must be provided with generator-backed HVAC service.

9.4.2.3 Power: All equipment in the Computer Room must be powered from UPS equipment that will provide a minimum of 10 minutes of service at full rated output. If no EES or standby power is to be provided to the facility, an assessment of the facility must be performed to determine the required UPS battery runtime. In cases where EES or standby power is not available, the UPS operating duration may be increased to 4 hours or more to meet mission needs.

- National Electrical Code Article 708, Critical Operations Power Systems: VHA has determined that facilities which have an Essential Electrical System (EES) have highly reliable electrical infrastructure. The additional cost of complying with National Electrical Code Article 708, Critical Operations Power Systems (COPS), is generally not warranted. However, a VHA facility of regional or national significance may conduct a risk assessment to determine if the power system serving the Computer Room should be COPS-compliant; final determination will be made by the AHJ.

9.4.2.4 Conduit Pathways: Refer to the Telecommunications Design Manual.

9.4.2.5 Alteration/Renovation of Existing Facilities — Computer Room

When there is no existing EES or standby power system OR if the existing EES cannot adequately support the equipment in the Computer Room after the loss of utility power, an assessment of the existing facility must be performed to determine the required UPS battery runtime (i.e. which may be increased to meet mission needs).

9.4.3 Telecommunications Rooms

Telecommunications rooms distribute telephone, data, and other telecommunications services to work spaces within each telecommunications room's serving zone.

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

9.4.3.2 Power: All equipment in the telecommunications rooms must be powered from UPS equipment that will provide a minimum of 10 minutes of service at full rated output. When a project in which the scope is limited and does not include the upgrade of the existing deficient EES to adequately support the equipment in the telecommunications rooms after the loss of utility power, an assessment of the existing

facilities must be performed to determine the required UPS battery runtime. NOTE: VA, as a Federal agency and AHJ, may designate the telecommunications rooms as a designated critical operations area (DCOA) per NEC Article 708, Critical Operations Power Systems (COPS). When the telecommunications rooms are so designated, NEC 708 may be required for the electrical and other systems serving the telecommunications rooms, including but not limited to upstream electrical distribution equipment.

- National Electrical Code Article 708, Critical Operations Power Systems: VHA has determined that facilities which have an Essential Electrical System (EES) have highly reliable electrical infrastructure. The additional cost of complying with National Electrical Code Article 708, Critical Operations Power Systems (COPS) is generally not warranted. However, a VHA facility of regional or national significance may conduct a risk assessment to determine if the power system serving the Computer Room should be COPS-compliant; final determination will be made by the AHJ.

9.4.3.3 Alteration/Renovation of Existing Facilities — Telecommunications Room

When there is no existing EES or standby power system OR if the existing EES cannot adequately support the equipment in the telecommunications room after the loss of utility power, an assessment of the existing facility must be performed to determine the required UPS battery runtime (i.e. which may be increased to meet mission needs).

9.4.4 Wireless Local Area Network System

Refer to the ICT standards on the TIL.

9.4.5 Portable Radio System

Refer to the Telecommunications Design Manual.

9.4.6 Satellite Radiotelephone System

Refer to the Telecommunications Design Manual.

9.4.7 Public Address System

Refer to the Telecommunications Design Manual.

9.4.8 Distributed Antenna System

Refer to the Telecommunications Design Manual.

9.4.9 Very Small Aperture Terminal Satellite Data Terminal

Refer to the Telecommunications Design Manual.

9.4.10 Alteration/Renovation of Existing Facilities — Telecommunications Systems

Existing facilities must comply with section 9.4 Telecommunications Systems.

9.5 Plumbing Systems

9.5.1 Medical Gases, Vacuum, and Oxygen Systems

Medical gases, vacuum, and oxygen systems must be secured to prevent unauthorized tampering, contaminating, or cross connecting of systems. Provide secured and access restricted emergency connection points for skid-mounted medical air and vacuum equipment and skid-mounted liquid oxygen tank with evaporator and regulators. NOTE: Emergency connection points must include connections for emergency electrical power.

9.5.2 Water Systems, Equipment, and Fixtures

Coordinate configuration of plumbing systems consistent with the Emergency Water Supply Plan (EWSP) as described in Chapter 8 Utilities and Building Services.

9.5.3 Alteration/Renovation of Existing Facilities — Plumbing Systems

Existing facilities must comply with section 9.5 Plumbing Systems.

9.6 Fire Protection Systems

9.6.1 Fire Sprinkler Systems

Facilities must be sprinkler protected throughout.

9.6.2 Alteration/Renovation of Existing Facilities — Fire Protection Systems

Existing facilities must comply with section 9.6 Fire Protection Systems.

10 SECURITY SYSTEMS

10.1 Scope, Purpose, and Goals

This chapter addresses physical security and related resiliency requirements associated with the selection, application, and performance of Electronic Security Systems (ESS). The ESS includes the Physical Access Control System (PACS); Intrusion Detection System (IDS); Security Surveillance Television (SSTV); Duress, Security Phones, and Intercom System (DSPI), commonly referred to as intercommunications system (intercom); the Mass Notification System (MNS); the Security Control Center (SCC); the Patient or Staff Annunciator/Locator System; the Behavioral Health Area System; the Narcotics Storage and Alerting System; and, the Detection and Screening System (DSS).

The requirements provided within this chapter and Appendix A and Appendix B must be used collectively to provide an acceptable level of physical security and resiliency for MC Facilities, LSP Facilities with MC Utilities/Systems Redundancies, LSP Facilities, and sites. Security Systems in existing facilities must meet the same requirements as new facilities.

As stated in Chapter 1, the requirements in this manual apply to new buildings, additions, and existing facilities undergoing renovations. Further clarification on applicability to renovation projects is provided in table 2-1 and in the gray box describing alteration/renovation of existing facilities at the end of each major section.

The requirements of this chapter are baseline requirements for physical security and resiliency. A risk assessment during the project planning phase is allowed to evaluate the deletion or incorporation of other specific requirements (see section 2.3 Exceptions and Deviations). The VA authority having jurisdiction (AHJ), defined in section 1.3 Administration and Enforcement, overseeing implementation of physical security and resiliency requirements for the facility will review submitted request for deviation from the baseline requirements of this chapter. When no risk assessment is performed, these baseline requirements apply.

The requirements of this chapter supplement other related VA standards for construction, space and facility planning criteria, design guides, design manuals, specifications, details, and published national policies, which remain in full force and effect. Specifically, all requirements of VA Handbook 0730, Security and Law Enforcement, Appendix B, (which covers physical security requirements for VA facilities), the VA Fire Protection Design Manual (which covers all VA construction), and ICT standards on the TIL remain in effect. Chapter 10 has been

coordinated with the Telecommunications and Special Telecommunications Systems Design Manual[42] (TDM) dated February 2016.

10.1.1 Veterans Health Administration MC Facilities

The requirements of Chapter 10 apply to all MC facilities, both new and existing. Existing MC facilities under alteration/renovation must be required to meet the same requirements as new facilities. The physical security and resiliency of MC facilities focuses both on protection and safety of people and physical assets, requiring protection of facility systems necessary to maintain operations prior to, during, and after a natural or manmade extreme event or a national emergency.

The integration and monitoring of the ESS, system operation, and space requirements associated with the ESS subsystems are discussed in this section. Security Control Center (SCC) and Security Equipment Room (SER) functional requirements are provided in PSRDM section 5.16 Security Control Center, while operational and system requirements are found within this chapter.

10.1.2 Veterans Health Administration LSP Facilities with MC Utilities/Systems Redundancies, and LSP Facilities

The requirements of Chapter 10 apply to all LSP Facilities with MC Utilities/Systems Redundancies, and LSP facilities, both new and existing. Existing facilities under alteration/renovation are required to meet the same requirements as new facilities.

LSP facilities may or may not include a Security Control Center (SCC). Where an SCC and Security Equipment Room (SER) are required in an LSP facility, the functional requirements provided in PSRDM section 5.16 Security Control Center apply. Where an SCC is not required in an LSP facility, a centralized monitoring function must be provided in order to accommodate security system monitoring requirements (see section 5.16 Security Control Center for further guidance). Operational and system requirements for the SCC are found within this chapter.

10.1.3 Veterans Benefits Administration Facilities

Veterans Benefits Administration (VBA) facilities generally do not have the same level of physical security and resiliency requirements as VHA facilities and can also have other criteria they must meet as lease space tenants (see section 1.4.6 VA Leased Facilities). VBA facilities are generally designated as LSP and require site specific ESS to ensure the desired level of protection is provided based on lease and local requirements. The designer must coordinate

[42] https://www.cfm.va.gov/til/dManual/dmTelecomm.pdf

ESS requirements with the VBA AHJ (see section 1.3 Administration and Enforcement) and VBA leadership in the VBA Office of Facilities and Administration, VBA HQ, Washington, D.C.

- VBA Construction/Operations and Maintenance
- VBA Physical Security
- VBA Emergency Manager
- VBA Safety Manager

Additionally, for VBA facilities, the design team must coordinate with the local emergency and safety managers to ensure the public address system (typically standalone) has a broadcast/microphone located in the Security Control Center (SCC), Integrated Operations Center (IOC), Emergency Operations Center (EOC), building Fire Command Center (FCC); and other ESS or Building Control Systems (BCS) that are activated or deactivated are integrated into the Emergency Notification Plan.

10.1.4 National Cemetery Administration Facilities

National Cemetery Administration (NCA) facilities do not have the same level of physical security and resiliency requirements as VHA facilities. NCA facilities are designated as LSP and may require site specific ESS to ensure the desired level of protection is provided based on local requirements. The designer must coordinate ESS requirements with the NCA AHJ (see section 1.3 Administration and Enforcement) and leadership in the NCA Design and Construction Service, NCACO, Washington, D.C.

- Director, NCA Design and Construction Service
- NCA Emergency Preparedness Coordinator

Additionally, for NCA facilities, the design team must coordinate with the local emergency and safety managers to ensure the public address system (typically standalone) has a broadcast/microphone located in the Security Control Center (SCC), Integrated Operations Center (IOC), Emergency Operations Center (EOC), building Fire Command Center (FCC); and other ESS or Building Control Systems (BCS) that are activated or deactivated are integrated into the Emergency Notification Plan.

10.1.5 Requirements for Subject Matter Specialists

In order to meet the physical security and resiliency requirements of this manual, the design team must include security subject matter experts as per section 1.8 Requirements for Subject

Matter Specialists.[43] The ESS systems must be designed and engineered by qualified Control System Cybersecurity, Information and Communication Technology, and System Integration specialists complying with the requirements listed below.

10.1.5.1 Control Systems Cybersecurity Specialist: The Control Systems Cybersecurity specialist must have a minimum of five years' experience in control system network and security design and must maintain current certification as a Global Industrial Cyber Security Professional (GISCP) or Certified Information Systems Security Professional (CISSP). The Control Systems Cybersecurity specialist must have demonstrated knowledge and experience applying IT and Operational Technology (OT) security strategies such as the application of the NIST security controls, PPD-21 and DHS ISC requirements, exploitation techniques and methods, continuous monitoring, and utility/building control systems design as defined in Chapters 5, 8, 9 and 10. The résumé of the specialist must be submitted to the VA Project Manager (PM) for review and approval prior to the concept phase of the project. The qualifications of the firm for whom the specialist works must also be submitted with the résumé.

10.1.5.2 Registered Communications Distribution Designer (RCDD®): The RCDD® must have a minimum of five (5) years' working experience in:

a) Telecommunications, and Special Telecommunications Systems – FMS functions, operations and management, including additional knowledge of medical, critical, emergency, safety, Disaster Communications, and TIP physical security and classified National Security Agency (NSA) Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST) systems required for VA's operation within the National Command Authority (NCA) Continuance of Government (CoG) and (Contingency of Operations Planning (COOP). The RCDD® must have extensive experience with and helicopter / flight operations and other systems described in CFM's PG 18-10, Telecommunications, and, Special Telecommunications System Design Manual (TDM-2016); and

b) Information and Communication Technology Specialist – for OIT control system network and security design and must maintain current certification to function as The Information and Communication Technology specialist with demonstrated knowledge and experience applying IT and OT security strategies such as the application of the NIST security controls, PPD-21 and DHS ISC

[43] It is acceptable to have one person on the design team who is certified in one or more of these areas; however, one area of certification may not be substituted for any other. The design team must include security subject matter expert(s) certified in all three areas.

requirements, cable network design and installation, project management, data center design, electronic safety and security and outside plant design as defined in Chapters 5, 8, 9 and 10. The résumé s of each specialist must be submitted to the VA Project Manager (PM) for review and approval prior to the concept phase of the project. The qualifications of the firm(s) for whom the specialist works must also be submitted with the résumé.

10.1.5.3 System Integration Specialist: The System Integration specialist must have a minimum of five years' experience in control system network, fire, and security design and must maintain current certification as a Certified System Integrator (CSI), Certified Fire Alarm Designer (CAFD), Certified Service Technician (CST), or Physical Security Professional (PSP). The Information and System Integration specialist must have demonstrated knowledge and experience applying IT and OT security strategies such as the application of the NIST security controls, PPD-21 and DHS ISC requirements, cable network design and installation, project management, data center design, electronic safety and security and outside plant design as defined in Chapters 5, 8, 9, and 10. The résumé of the specialist must be submitted to the VA Project Manager (PM) for review and approval prior to the concept phase of the project. The qualifications of the firm for whom the specialist works must also be submitted with the résumé.

10.2 Coordination with Telecommunication and Other Systems

The ESS design team will also need to collaborate closely with the Building Automation, Fire, RFID, Wi-Fi (not DHS Distributed Antenna System (DAS) for Emergency Responder use only), and other building control systems to ensure end-to-end cybersecurity is provided across the VA domain (both Internet connected and required standalone systems). Additionally, there are some historic building, Federal and National Code compliance, OIT and GSA required guidance and restrictions of use. Please refer to CFM's PG-18-10, Telecommunications, and Special Telecommunications Design Manual (TDM-2016), Chapter 1 – General for descriptions.

10.2.1 Telecommunications Infrastructure Plant

Ensure that all ESS design and construction is Telecommunications Infrastructure Plant (TIP) compliant (Facilities Management Service (FMS) and IT combined, refer to the TDM for additional requirements) and fulfills the OIT Trusted Internet Connection and Continuous Monitoring requirements.

10.2.1.1 Facilities Management Service (FMS) Communications Systems and Equipment: Microprocessor based FMS systems and equipment are outside the purview of OIT and include, but not limited to:

- Two-way and Radio Paging (Emergency and Routine)

  Nurse Call
  Code Blue

- Television

  Master Antenna (MATV)
  Community Antenna (CATV)
  Closed Circuit (CCTV) for education
  Satellite TV (SATV)

- Microwave
- Satellite Radio/Telephone and Radio Entertainment
- Public Address

  Overhead Paging
  Mass Notification
  Intercommunications (Intercom)

- Physical Security Management

  Physical Access Control Systems (PACS)
  Motion Intrusion Detection
  Duress and/or Panic Alarm
  Security Surveillance Television (SSTV)

- Patient, Staff, and Asset Monitoring

  Cardiac/Medical Telemetry
  Patient/Staff Location

- Emergency Management

  Distributed Antenna System (DAS)/Emergency Responder Emergency
  Fire Alarm
  Police
  Disaster

These systems and equipment must be located in the FMS area of the Telecommunications Rooms and the Antenna Equipment Headend Room. Headend,

host servers, or active equipment associated with archiving, packetized storage, or transport of confidential information generated by an FMS system must be located within the FMS designated equipment area of the Computer Room (refer to ICT standards on the TIL for specific requirements) and will be serviced and managed by OIT.

Life-safety systems as defined in TDM section 7.2.6 (i.e. nurse call and code blue, public address, and radio paging) are standalone networks that terminate in an interface cabinet in the FMS portion of the Computer Room. (Refer to TDM Chapter 1 and paragraph 7.2.6).

10.2.1.2 FMS Active Equipment Area: At a minimum, the Computer Room must contain a designated FMS space (refer to ICT standards on the TIL for specific space requirements) for the following FMS active equipment.

- Code One (Blue)
- Emergency Voice Switching Control System
- Energy Management System (or EMCS)
- Fire Alarm
- Nurse Call
- Public Address System (PAS to include overhead paging)
- Security Management (includes duress alarm, motion intrusion detection, and access control)

10.2.1.3 Information Technology Equipment (OIT): Any electronic digital or analog computer, with peripheral support, memory, programming, or other directly associated equipment, records, and activities that supports VA's mission and allows archiving and/or packetized storage and transportation of confidential Veteran, patient, staff, or public information. OIT equipment located within OIT equipment area of the Computer Room and its LAN is not permitted to be the primary media that actively process life safety, public safety and emergency data, nor any FMS systems data unless nationally-recognized testing laboratory (NRTL) UL 1069 and IEC 60950-1/2 Listed and Labeled (refer to Facilities Management Service (FMS) Communications Systems and Equipment and the TDM).

10.2.1.4 Co-located OIT and FMS Systems: Many FMS building systems are now electronically monitored and managed and require non-OIT IT equipment and servers. In the past, these systems were typically located in building mechanical and electrical rooms. Now, environmental, physical, and at times communications security

requirements for server-based FMS systems, mandate that this equipment be co-located with OIT equipment in the Computer Room, Telecommunications Rooms, and Antenna Headend Equipment Room, when specifically, approved and authorized.

10.2.1.5 OIT One-VA Technical Reference Model:[44] The One-VA Enterprise Architecture (One-VA EA) is a comprehensive picture of the VA's operations, capabilities and services, and the business processes and IT capabilities that support them.

10.2.1.6 OIT TRM Technology/Standards List: The OIT TRM Technology/Standard List identifies technologies and technical standards that have been assessed. Each project team must consult the organizations responsible for the target development, desktop, testing and/or production environments to ensure that the intended use of the technologies is supported.[45]

10.2.1.7 VA HSPD-12/PPD-21 Program Management Office: The Office of Personnel Security and Identity Management (PS&IM) is comprised of VA's Personnel Security and Suitability Service (PSS), Security and Investigations Center (SIC), and the HSPD-12 Program Office (HSPD-12) within the Office of Operations, Security and Preparedness (OSP). PS&IM ensures alignment, accountability, and transparency of VA personnel security, suitability, and HSPD-12 programs and provides central coordination and oversight of the Department personnel security, suitability, and identity management infrastructure. The HSPD-12 Program Office provides Departmental policy and guidance, management, communications, training, deficiency requirements, and oversight for identity and access implementation programs, including PIV,[46] Physical Access Control Systems, and Logical Access Control Systems. The PIV Program Office, which falls under OIT, in conjunction with the Office of Human Resources and Administration, has the responsibility for implementing HSPD-12 in the Department.

Homeland Security Presidential Directive 12 (HSPD 12), dated August 27, 2004, *Policy for a Common Identification Standard for Federal Employees and Contractors*, directed the promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors.

Identity, Credential and Access Management (ICAM) is the intersection of digital identities and associated attributes, credentials, and access controls into one comprehensive approach.

Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, released on February 12, 2013, states the Federal government has a responsibility to

[44] https://www.va.gov/TRM/TRMHomePage.asp
[45] https://www.va.gov/TRM/ToolListSummaryPage.asp
[46] https://www.va.gov/PIVPROJECT/ and http://www.idmanagement.gov/identity-credential-access-management

strengthen the security and resilience of its own critical infrastructure against both physical and cyber threats. It further states that "…all Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions."

GSA manages the federal HSPD-12 ICAM program[47] which is responsible for the management of identity information, credentials, and secure access to buildings, networks, and information technology systems.

GSA Schedule 70, Special Item Number (SIN) 132 62 Homeland Security Presidential Directive 12 (HSPD-12) Product and Service Components[48] is used by Federal agencies to implement the requirements of HSPD-12, FIPS-201, and associated NIST special publications. The HSPD-12 implementation components specified under this SIN are:

- PIV enrollment and registration services,
- PIV systems infrastructure,
- PIV card management and production services,
- PIV card finalization services,
- Physical access control products and services,
- Logical access control products and services,
- PIV system integration services, and
- Approved FIPS 201-Compliant products and services.

For vendor list, contact: U. S. Department of Veterans Affairs, Office of Security and Law Enforcement (07B1C), 810 Vermont Avenue, NW, Washington, D.C. 20420.

VA ESS System Integrators and Installers must be GSA HSPD-12 Certified.[49]

ESS components and devices must be ADA 2010 OSHA Section 508 compliant, reference the TDM Section 1.8.1.6.

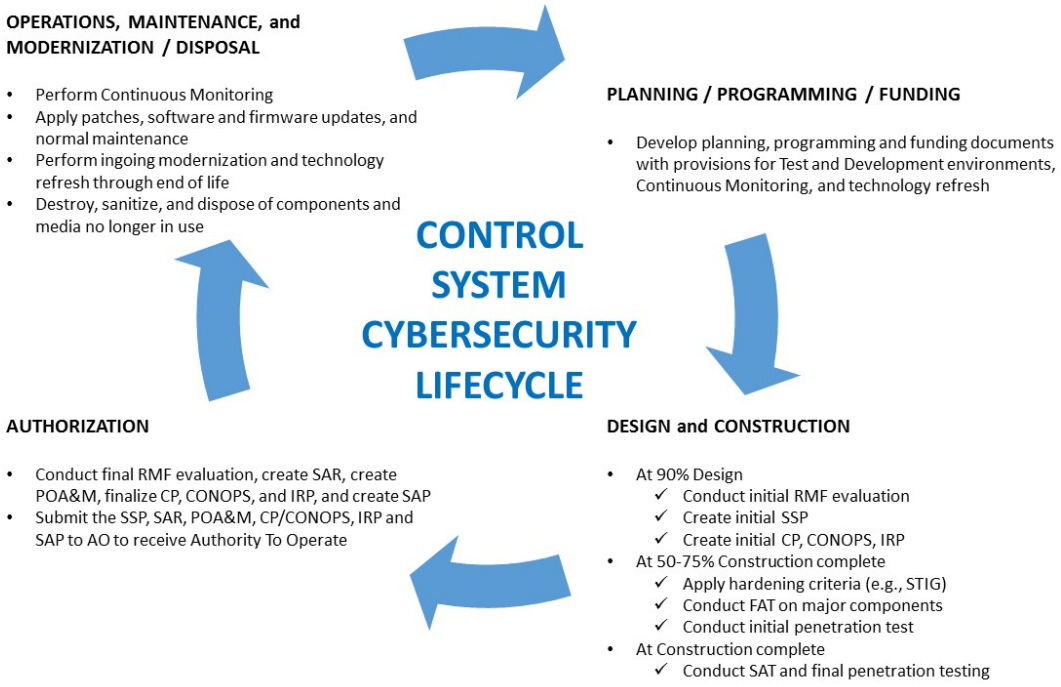
Note: ESS RFID Real-Time Personal Locator systems must comply with VHA/AFGE MOU.

[47] http://www.gsa.gov/portal/content/105233
[48] Homeland Security Presidential Directive 12 (HSPD-12) Product and Service Components
[49] http://elibrary-test.fas.gsa.gov/ElibMain/scheduleList.do;jsessionid=FBBBC4E20232B816ACE9D0E59C0A4B3E.node1?catid=360&famid=3&sched=yes

10.2.2 ESS Cybersecurity Requirements

As long as VA uses outside contractors to design, construct, and operate building control systems, it is vitally important that contractors and vendors become part of the cybersecurity solution, starting with the initial planning and ending with proper disposal of obsolete equipment. Figure 10-1 illustrates the cyber lifecycle of ESS.

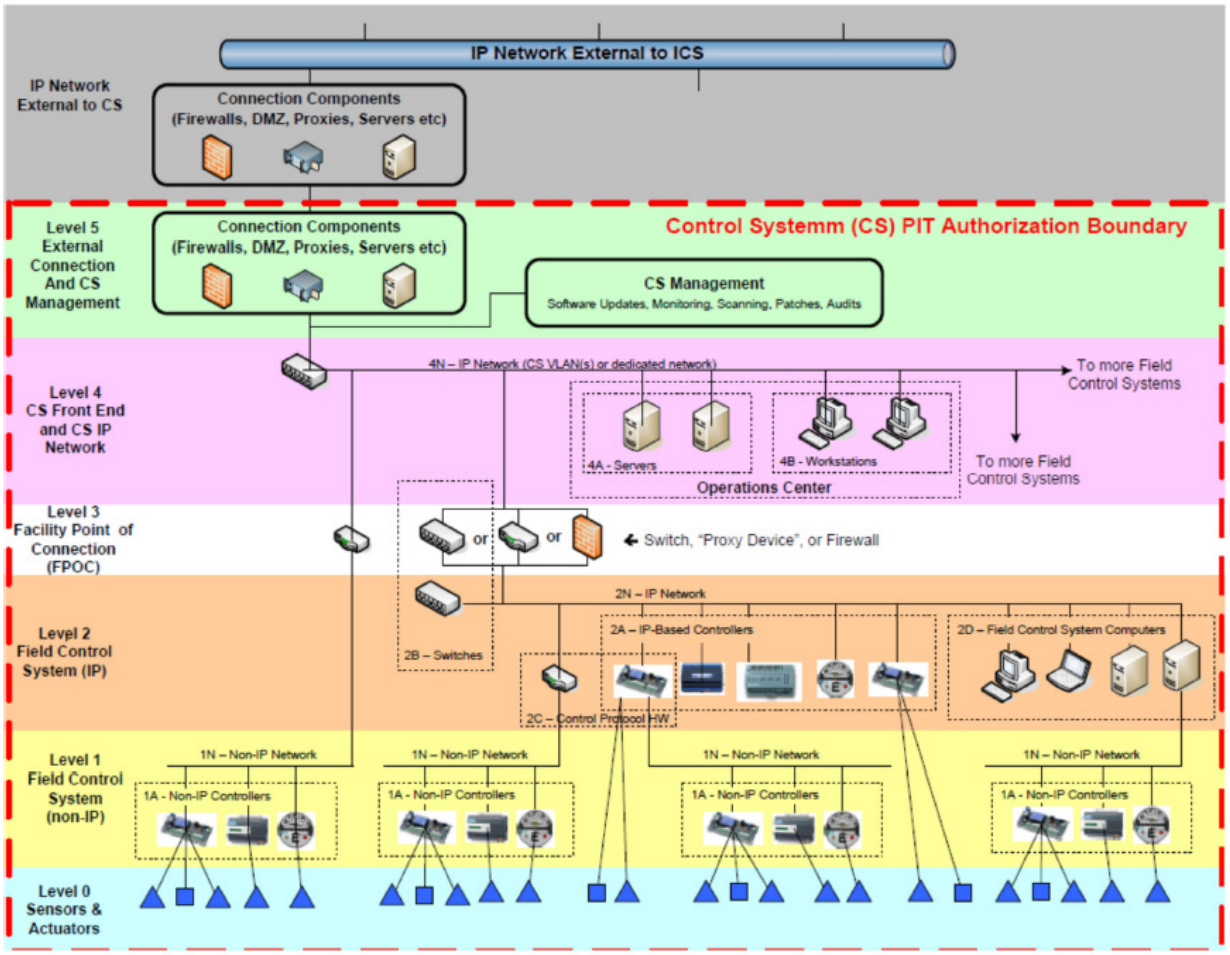
Figure 10-1 ESS Cybersecurity Lifecycle



10.2.2.1 Authorization (to Operate): On an open ESS architecture, where ESS are connected to other VA systems through local area networks (LAN) or wide area networks (WAN), or simply connected to the Internet or extranet, the need to maintain data security is critically important. In these circumstances, ESS must undergo information security authorization processes where the ESS are evaluated to ensure data security is maintained. VA utilizes the National Institute for Science and Technology (NIST) Special Publication 800 series and follows the Risk Management Framework (RMF). The facility OIT End User Operations (EUO) Area Manager (AM) is responsible for the RMF process.

The ESS Reference Architecture is provided in Figure 10-2; additional Plant and Conduit reference diagrams are in the TDM Appendices A and B.

Figure 10-2 ESS Reference Architecture (Adopted from DoD Model)



10.2.3 Trusted Internet Connection/Einstein

The U.S. Government PKI is designed around the Federal Bridge Certification Authority. This innovative approach allows U.S. Federal agencies to operate their own public key infrastructures and interoperate with the public key infrastructures of other agencies in a highly simplified architecture that minimizes cross-certification management and enhances technical interoperability. The Federal Bridge implicitly establishes standards of assurance for its participating members and enhances interoperability standards among PKI product and service vendors.

The ESS PACS, SSTV, and IDS are typically connected via the Trusted Internet Connection (TIC) and federal bridge servers and continuously monitored using the DHS Einstein program. Coordinate with the Office of Information & Technology (OIT) Security Operations to ensure an Interconnection Security Agreement (ISA) is established (when required) during the Factory Acceptance Testing (FAT) phase; contact Security Operations, U. S. Department of Veterans

Affairs, Office of Information & Technology (OIT), 810 Vermont Avenue, NW, Washington D.C. 20420.

10.3 Electronic Security Systems

All systems are required to be standalone networked for identity verification as required by Homeland Security Presidential Directive 12 (HSPD-12), Presidential Policy Directive 21 (PPD-21), and Federal Information Processing Standards 201 (FIPS-201) compliance.

There is a higher need for event correlation and awareness for MC facilities; MC facilities must report up to a regional monitoring center to provide system resiliency and failover.

Integrate all ESS into a common graphic user interface (GUI) to provide comprehensive situational awareness. This includes correlating alarm events with automated video call-up of associated video for remote assessment. Linkages between systems must be logical in lieu of complex hardwired systems using inputs and outputs.

Larger MC or regional systems must consider the use of physical security information management (PSIM) systems to combine large complex subsystems. PSIM systems also provide the ability to monitor multiple security subsystems from multiple manufacturers. Regional monitoring systems are a VA goal and are required. A central interface must be provided for monitoring, reporting, and configuration of all electronic security subsystems; it must provide correlated event monitoring and controls.

The ESS must allow the configuration of alarm monitoring, administrative, asset management, digital video management, intrusion detection, visitor enrollment, remote access level management, and integrated security workstations.

The ESS must have the ability to compose, file, maintain, update, and print reports for either individuals or the system. Examples of systems reports include:

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

All ESS with system clocks must be connected to a time synchronization clock to provide a coordinated time stamp. The time synchronization system must be based on an internal VA utilized time clock or atomic sync.

The ESS must be backed by the standby electrical system and UPS equipment. (Refer to Chapter 9 Building Systems for utility and building system requirements)

10.3.1 ESS Commissioning

ESS systems, subsystems, and software programming must undergo comprehensive acceptance testing. The acceptance test process must be documented using a standard testing process that is implemented and assessed by a qualified independent third party. VA has adopted the *Unified Facility Criteria 04-021-02 Electronic Security Systems 2016 Chapter 9,* as the template document for ESS Commissioning. (Refer to TDM paragraph 1.3 for personnel contact information)

The use of the *Unified Facility Criteria 04-021-02 Electronic Security Systems 2016* procedures is required for initial ESS commissioning and for periodic re-commissioning as directed by VA Central Office. The Contracting Officer (CO) must issue the Test Selection Form (TSF) and a copy of the USACE PVT procedures with the project's scope of work and contract documents. The contractor must complete and submit the TSF based on the project scope of work. The CO will review, adjust as required, and return the approved TSF to contractor. The contractor will in-turn utilize the TSF to modify the USACE PVT procedures to meet the VA contract requirements.

At a minimum, the process must meet the following requirements:

- Demonstrate the functionality of each security device or component.
- Demonstrate performance characteristics consistent with the manufacture's specifications.
- Demonstrate all functionality including software programming, integration of subsystems, and automation of system functions as specified for the particular project.
- Verify that network connections, IT integration, and IT security requirements meet FIPS, NIST, and all other applicable standards.
- Verify that all life-safety integration requirements and functions meet local and national codes and ordinances.
- Demonstrate startup, recovery from failure, and operator training requirements.

10.3.2 ESS Monitoring

ESS monitoring requirements are be based on a robust, multi-tier architecture that provides local, regional, and national alarm monitoring, as well as remote alarm assessment, dispatch, and response. The multi-tier structure provides multiple levels of ESS event visibility that corresponds to the national SSP and includes redundant primary and secondary monitoring capability within regions or in clusters organized geographically (the current VISN model or similar). Implementation of regional and national ESS integration must adhere to standard technical specifications and be incorporated into all new construction, major modernization, or

ESS upgrade. ESS integration into smaller renovation and expansion projects to existing facilities must be analyzed on a case-by-case basis to determine suitability and cost effectiveness. The national SSP and facility-level SMP must identify overall system framework and operational procedures.

10.3.3 ESS Configuration Management

An ESS configuration standard must be established to support effective and efficient monitoring of the ESS. Managing the configuration requires the following:

- Maintain baseline configurations in accordance with technical specifications for systems and security technology set forth by VA Central Office.
- Establish and enforce security configurations for individual applications such as PACS, SSTV, and IDS systems and products employed in facility physical security systems.
- Monitor and control changes to the baseline configurations and to the constituent components of security systems (including hardware, software, firmware, and documentation) throughout the respective system lifecycle. Configuration management can be largely accomplished through updating ESS documentation received during initial project installation.
- The facility Chief of Police, with support from the Chief of Engineering and the CIO, is responsible for tracking and maintaining the baseline configuration of the ESS. The facility Chief of Engineering is responsible for establishing ESS configuration standards to support the Chief of Police for the effective and efficient monitoring of the ESS.

10.3.4 ESS and Room Types (From VHA Program Guide and VHA 730 Appx B)

The ESS Appendix B (Excel worksheet) maps the ESS to exterior and interior spaces and room types. The ESS design team will need to confirm final selection of the various ESS with the Information Systems Owner (Regional Director).

10.4 Physical Access Control System/Electronic Access and Door Control

The Physical Access Control system (PACS) consists of all equipment and information required to verify, identity, and grant or deny access to individuals in accordance with HSPD-12 and PPD-21. Equipment ranges from card readers and locks to the servers and databases required for identity verification and all components and communication in between. All PACS must comply with HSPD-12, PPD-21, NIST SP 800-116, and VA 6500 Directive page 40 Section (4) Physical Security Controls requirements. Each facility must have its own dedicated connection to the

Federal bridge and PACS server. These requirements are established in the VA Master Construction Specifications. MC facilities must have a SCC for monitoring with failover to a regional monitoring center.

VA Federal Bridge servers must be located in the MCR or VA Data Centers.

10.4.1 PACS Hardware

10.4.1.1 Data Gathering Panels must be centrally located within a secure location that prevents panels from being damaged, tampered with, or accessed by unauthorized personnel. Field modules, such as reader modules, may be located on the secured side of a door in an enclosure that is locked or protected with a tamper switch.

10.4.1.2 Entry Control Devices include card readers and biometric verification stations. All entry control devices must be dual authentication card readers (card and pin), FIPS 201 compliant and hardwired to the PACS data gathering panel. Biometric systems have limited application and can only be utilized for secondary authentication into high security areas.

10.4.1.3 Electrified Locks, such as, magnetic locks, strikes, and mortise locks, must be selected based upon life-safety requirements, locking arrangements, and level of security. Utilize request-to-exit devices integrated in the electrified locksets in accordance with NFPA, IBC, and other applicable construction codes. Fail-safe-fail-secure, field selectable locks must be used.

10.4.1.4 Optical Turnstiles, where used in high-traffic access control points such as lobbies, require integrated barriers. Rotary turnstiles are discouraged due to life-safety concerns. Coordinate and accommodate life-safety when planning to use turnstiles.

10.4.2 PACS Credentials and Enrollment Interface

With the development of the HSPD-12 based architecture, credentialing and badge issuance are separate from the PACS. Facility level enrollment station is required; however, credentialing and badge issuance will be accommodated by a separate non-PACS system. The facility level enrollment station will allow the PIV badge holder to be programmed for facility level access permissions. Credential validations must comply with OMD 11.11, FICAM, and NIST SP 800-116, and must use PKI authentication method.

10.4.3 PACS Locations

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

10.5 Intrusion Detection System

The Intrusion Detection System (IDS) consists of all equipment and information required to detect and annunciate potential unauthorized entry into a protected space through an accessible and man-passable opening. An accessible opening as defined by NFPA 730 *Guideline for Premise Security* is within 18 feet (5.5 m) of exterior ground surface within 14 feet (4.3 m) directly or diagonally opposite a window, structure, fire escape, or roof, or 3 feet (0.9 m) or less from an opening, fire escape, ladder, and the like that is in or projecting from the same or adjacent wall and leads to other premises.

A man-passable opening as defined by NFPA 730 is a clear cross section area of 96 square inches (619 cm^2) or more with the smallest dimension exceeding six (6) inches (15.2 cm). IDS sensors include motion detection, glass break, door contacts, and other detection devices. All IDS must meet UL 639 Intrusion Detection Standard. Terminate all IDS sensors on the PACS data gathering panel. Provide an arm/disarm panel in protected spaces. Pharmacies have additional requirements; refer to VA 0730, Appendix B for these requirements. (Refer to TDM paragraph 7.2.8.2)

10.5.1 Planning and Selection Criteria

IDS must provide multiple levels or points of detection as far as possible from an asset to be protected. Determine the type of IDS sensor technology to use based upon the capability of the sensor and environmental factors.

Intrusion devices of different technologies (such as, motion detection, glass break, or magnetic contacts) must be zoned separately. Intrusion devices of like technologies must be wired together, not to exceed three devices, within the confines of clear physical barriers and not to exceed 50 feet (15 m). Devices in the same physical location providing the same purpose must be programmed in alarm groups to support the intrusion zone concept.

10.5.2 Data Transmission System

Sensors and arm/disarm devices must be hardwired and directly connected to the data gathering panel. 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 and VA requirements, including coordination with proper approving authority within VA.

10.5.3 Interior Sensors

10.5.3.1 Door/Window Contacts may be either recessed or surface mounted; the preferred method is to use a recess mounted contact to reduce the ability to defeat the

system and improve aesthetics. Surface mounted switches must be mounted on the protected side of the door.

For high value/high risk, contacts must be a Balanced Magnetic Switch (BMS):

- When double doors or gates require protection, each door must be fitted with a separate BMS.
- When protecting roll-up doors wider than 80 inches (2 m), BMS must be mounted on both sides on the interior side of door.

10.5.3.2 Glass Break Sensors: Windows with security mesh screen do not require glass break sensors. Window construction must mitigate blast or ballistic hazards when selecting sensor technology. Laminated glass thicker than 0.25 inches (0.635 cm) does not require IDS. Glass break sensors must not be used in the absence of PIRs or balanced magnetic switches.

10.5.3.3 Microwave Sensors, where required for security, must use a multiple-beam configuration and only be used when there is a clear line of sight between a transmitter and receiver and where the ground is within the sensor operational specifications. Microwave sensors must not be used near outdoor fluorescent lights.

10.5.3.4 Passive Infrared Sensors: Passive infrared sensor (PIR) must meet the requirements of ANSI/SIA PIR-01, *Passive Infrared Motion Detector Standard - Features for Enhancing False Alarm Immunity*. 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, 45 degrees or curtain, must be determined from a field survey and mounting surface availability. Sensitivity of the sensor must be adjustable to provide the necessary area of protection.

10.5.3.5 Vibration Sensors: Boundary walls to be protected must use vibration detection sensors mounted to the wall to assure detection of attempted penetration before the wall is breached. Vibration sensors must be used in combination with BMS for safes and vaults. Wall mounted shock/vibration sensors must be provided with LEDs to indicate activation and must be mounted to provide a clear view of the LED. Except for unusually small areas, smaller than 10 x 10 feet (3 x 3 meters), sensors zoned together must not cover more than one wall.

10.5.3.6 Video Motion Detection (VMD) cameras and software provide an automated alert, assessment, and response notification capability. VMD is best utilized in conjunction with other sensors (such as PIR, MW, glass break) to verify and validate alerts and alarms. The nuisance alarm rate (NAR) must comply with NFPA 731.

10.5.3.7 Interstitial Motion Detection (IMD) sensors provide an automated alert, assessment, and response notification capability of movement in the interstitial spaces. IMD is best utilized in conjunction with other sensors (such as PIR, MW, glass break) to verify and validate alerts and alarms. The nuisance alarm rate (NAR) must comply with NFPA 731.

10.5.3.8 Seismic/Movement Motion sensors provide an automated alert, assessment, and response notification capability of movement due to seismic/wall/foundation displacement that could occur as a natural or manmade event. Seismic/Movement is best utilized in conjunction with other sensors (such as PIR, MW, glass break) to verify and validate alerts and alarms. The nuisance alarm rate (NAR) must comply with NFPA 731.

10.5.3.9 Underfloor Motion/Water/Heat sensors provide an automated alert, assessment, and response notification capability of underfloor motion and are most often a multi-use sensor or collocated with other sensors and report back via a common transport channel. The nuisance alarm rate (NAR) must comply with NFPA 731.

10.5.4 Exterior Sensors

Exterior intrusion detection systems must be planned for remote VA utility infrastructure lacking physical guard or police force presence. These areas are commonly water towers and water treatment facilities outside the VA established perimeter but may include other assets. Exterior sensors must only be used for perimeter protection when the area to be protected is bordered by a fence or physical barrier. Exterior perimeter detection capability must 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. Facilities that use a fence to define boundaries must address the use and necessity of fence mounted sensors, microwave sensors, or photoelectric beams.

10.5.4.1 Microwave Sensors, where required for security, must use a multiple-beam configuration and only be used when there is a clear line of sight between a transmitter and receiver and where the ground is within the sensor operational specifications. Microwave sensors must not be used near outdoor fluorescent lights.

10.5.4.2 Infrared Sensors, where required for security, must 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 must not be installed where local climatic conditions would cause interference.

10.5.4.3 Fence Mounted Sensors, where required for security, must include tension wire, capacitance, electric vibration, and shock sensors. When using fence mounted sensors, a BMS must be installed at the pedestrian and vehicle access point gates.

10.5.4.4 Video Motion Detection (VMD) cameras and software provide an automated alert, assessment, and response notification capability. VMD is best utilized in conjunction with other sensors (such as PIR, MW, glass break) to verify and validate alerts and alarms. The nuisance alarm rate (NAR) must comply with NFPA 731.

10.5.5 Design and Installation

To ensure proper operation, maximum detection capability, and minimize false alarms, IDS must be installed in accordance with manufacture instructions, 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 must be capable of continuous operation and monitoring through the use of UPS equipment and standby electrical system (see Chapter 9 Building Systems).

10.5.5.1 Locations: Protect all man-passable openings in a building perimeter with contacts. Protect all accessible openings as defined by NFPA 730 with appropriate sensors. (Refer to Appendix A, Security Door Opening Matrix, and Appendix B, Security System Application Matrix, for IDS system component locations.)

10.6 Security Surveillance Television

This section addresses physical security standards for the two basic uses of Security Surveillance Television (SSTV): (1) event assessment and (2) general surveillance. This section describes the selection, application, and performance of the SSTV, which includes cameras, monitors, controlling and recording equipment, and centralized management and operations of the system. (Refer to TDM section 7.2.8.1)

10.6.1 System Uses, Compatibility, and Integration

10.6.1.1 System Uses: SSTV must be used to monitor building entrances, restricted areas, MC asset areas, and alarm conditions. SSTV must be used for surveillance and documentation of defined exterior areas, such as, site and roadway access points, license plates, parking lots, and building perimeter, and interior areas (to include facial recognition systems) from a centralized SCC. (Refer to TDM section 7.2.8.1)

10.6.1.2 System Compatibility: All components of the SSTV must be fully compatible and must not require the addition of interface equipment or software upgrades to ensure a fully operational system.

10.6.1.3 System Integration: The SSTV must be able to be fully integrated with other security subsystems.

10.6.2 Networked versus Standalone

SSTV must be designed and engineered as a standalone system(s).

10.6.2.1 Networked SSTV may be used when VA Networks are Life-Safety Code 101 and NRTL 1069 and IEC 60950-1/2 Listed and Labeled, may be utilized when multiple cameras, monitors, controllers, and recording devices are configured and makeup what is defined as a whole SSTV. All components of the system must be monitored and controlled in the SCC, using either a matrix switcher or a desktop computer. Alternate locations for monitoring cameras may be required in some circumstances.

10.6.2.2 Standalone SSTV must be used for a single application and designated location use only and may compliment the PACS for a specific area. Fixed camera(s) must be positioned in a manner to allow viewing of specific entry control point(s) through the use of a dedicated SSTV monitor located in a common viewing area.

10.6.3 Cameras

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

10.6.3.1 General Requirements: All cameras must meet the following requirements. Cameras must conform to National Television System Committee (NTSC) formatting criteria.

- Cameras must be color and auto-day/night feature to digitally switch from color to black and white at dusk and vice versa at dawn.
- Cameras must be rated for continuous operation.
- Each camera function and activity must be addressed within the system by a unique twenty-character user defined name; the use of codes or mnemonics identifying the SSTV action will not be accepted.
- Cameras must 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 SSTV computer network, a video encoder must be used to convert the signal from the NTSC criteria to Moving Picture Experts Group (MPEG) format.

- All cameras must 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 is discouraged for any long-term application (more than one (1) year period of use) and must not be used for MC assets (see section 10.5.3.3 wireless camera use).

10.6.3.2 Fixed versus Pan/Tilt/Zoom: SSTV cameras may be either fixed or pan/tilt/zoom (P/T/Z).

- Fixed cameras must be the primary means of surveillance to monitor designated access control and monitoring points.
- Fixed cameras must be used to monitor interior building areas; P/T/Z cameras may be used to provide supplemental surveillance coverage of building interiors where necessary.
- P/T/Z cameras must be used and deployed for all site perimeter and exterior building areas.

10.6.3.3 Hardwired versus Wireless (all wireless applications are only allowed after approval by VACO's Spectrum Management and COMSEC Service's Special Communications Team, (SMCS – OSP 007), AHJ as per TDM paragraph 1.3): SSTV cameras classified as hardwired directly connect to a monitoring device using video signal imaging cable. A wireless SSTV 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 Internet protocol (IP) cameras must be the method of installation.
- Hardwired cameras must be connected to the monitoring equipment with continuous wiring used as the media transmission system.
- If approved, and prior to selection of wireless cameras, account for the potential effects on the use of this technology, such as geographical area of coverage, environmental interference, effects on medical systems, and distance from the monitoring location.
- Wireless systems must meet FCC requirements and be approved by VA wireless system approval authority during the design of the system.

10.6.3.4 Color versus Black and White: All SSTV cameras must be color that allows for black and white applications.

- Cameras must be able to switch between color and black and white through a programmable feature built into the camera (auto day/night feature).

- Color must be the primary mode, automatically switching to black and white when light levels drop below normal specifications.

10.6.3.5 Camera Lenses must be used in a manner that provides maximum coverage of the area being monitored and meet the following requirements. Two types of lenses must be used for both interior and exterior fixed cameras.

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

10.6.3.6 Camera Enclosures: All cameras and lenses must be enclosed in tamper resistant housings.

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

10.6.3.7 Camera Installation, Mounts, Poles, and Bases: All camera equipment must be installed to ensure all components are fully compatible as a system. Adhere to the National Electrical Contractors Association Standard, NECA 303-2005, *Installing Closed-Circuit Television (CCTV) Systems*.

- Camera mounts must be installed on approved mounting surfaces structured for weight, wind load, and extreme weather conditions.
- Camera mounts must be installed in a manner that will not inhibit camera operation or field-of-view.
- Where a 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 must be constructed of metal with a concrete base and must be installed and grounded in accordance with the NEC.
- Camera poles must be weather resistant.

- 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, or interfere with the video picture and signal.
- All camera poles and mounts must be installed in locations that will allow for optimum view of the area of coverage.

10.6.3.8 Power Source: All SSTV cameras and mounts must be powered remotely by a UL listed power supply unit (PSU) as follows:

- The PSU must have the ability to power at least four exterior cameras or eight interior cameras.
- A back-up with dedicated power feed from a security system power panel must be provided to the camera and mount; a step-down transformer must also be installed at the camera location to ensure a proper operating voltage is provided to the camera and mount.
- The SSTV must be supported by UPS equipment and standby electrical system (see Chapter 9 Building Systems).

10.6.3.9 Lightning and Surge Protection: With the exception of fiber optic cables, all cables and conductors that act as control, communication, or signal lines must include surge protection when extending beyond the building envelope.

10.6.3.10 Site Coordination: Site and building exterior lighting must be coordinated and installed in a manner that allows the SSTV system to provide positive identification of a person, vehicle, incident, and location.

- Lighting must not provide bright illumination behind the main field of camera view.
- Cameras must 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 that are necessary for operational integrity of the SSTV system.

- SSTV cameras must be installed so that landscaping will not deter from the intended field of view.
    - Cameras must not be mounted in trees, bushes, or any other natural landscape that will in the long term degrade the view or operation of the SSTV system.
    - Cameras must not be installed behind, next to, or on any natural or manmade 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 SSTV system.

10.6.4 Additional Components

10.6.4.1 Monitors must 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).

10.6.4.2 Matrix Switcher/Network Server (controlling equipment) must be used to call up, operate, and program all cameras associated SSTV components. Controlling equipment must have the ability to operate the cameras locally and remotely. A matrix switcher or a network server must be used as the SSTV controller. The controlling equipment must 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. The controlling equipment must be able to perform as an analog-to-Ethernet "bridge," allowing for the control of matrices, multiplexers, and P/T/Z cameras.

10.6.4.3 Keyboards and Joysticks must 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 SSTV camera controls.

10.6.5 Controlling and Recording Equipment

All cameras on the SSTV must 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 must be determined by the size and type of SSTV designed and installed, as well as the extent to which the system is to be used. The following criteria must be followed when choosing a SSTV camera recording device.

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

- The DVR must have a built-in compact disc-recordable (CD-R) or Digital Versatile Disc Recordable (DVD-R) for downloading of the buffer to compact disc (CD) or Digital Versatile Disc (DVD) for back-up.
- The DVR buffer must be cleared, and all information transferred to CD when the buffer is at no greater than 60 percent of capacity.
- CDs and DVDs must be stored in a dry, cool, central location that is secure; recordings must be stored in accordance with VA Police directives.

10.6.5.2 NVR must be used within the SSTV for large or small SSTV system set-ups. The NVR must be used when the SSTV is configured as part of the SMS only. Input to the NVR must 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-IP cameras over to an ethernet cable.
- The NVR must provide for either direct download of data to a computer storage device or CD/DVD; all storage media must be stored in a dry, cool, central location that is secure, and storage media must be held as directed by the VA Police.

10.6.6 Video Motion Detection

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

10.6.6.1 Timing: This feature must 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.

10.6.6.2 Interface with IDS: The video motion detection must be interfaced with the IDS to provide redundancy in the security alarm reporting system.

10.6.6.3 Other System Interface: Cameras must be designed to interface and respond to exterior and interior alarms, security phones/call-boxes, duress alarms, and intercoms upon activation.

10.6.7 Camera Locations

Refer to Appendix A, Security Door Opening Matrix, and Appendix B, Security System Application Matrix, for SSTV component locations.

10.7 Duress, Security Phones, and Intercom System

This section addresses physical security criteria associated with the selection, application, and performance of the duress, security phones or emergency call-boxes, and intercom system (DSPI), also referred to as the intercommunications system, which must be provided as a standalone system (Refer to CFM's TDM paragraph 1.3 for AHJ contact information and TDM Chapter 7 for technical requirements).

10.7.1 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 must be used.)

10.7.1.1 DSPI System Compatibility: All components of the DSPI system must be fully compatible and not require the addition of interface equipment or software upgrades to ensure a fully operational system.

10.7.1.2 System Integration: The DSPI system must be fully integrated with other security subsystems.

10.7.1.3 Accessibility for Persons with Disabilities: DSPI systems must be accessible to persons with disabilities.

10.7.1.4 Security Intercoms: The main components of this security subsystem are the hardwired master intercom and remote intercom stations. Intercom devices must be integrated with the SSTV upon initiation and activation of a two-way conversation. Where wireless systems are used, repeaters must be required. Where a wireless intercom system is used; it must meet FCC wireless transmission standards and VA requirements, including coordination with proper approving authority within VA. Typical locations for security intercoms must 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.

10.7.1.5 Intercom Door Release: Security intercom with remote door release capability must be used for functional areas that require PACS. The security intercom system must 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 must have both an audio and built-in video capability. Video verification of person(s) requesting access at these points must be required.

10.7.1.6 Intercom Master Station must be capable of selectively calling and communicating with all intercom stations individually or system-wide. Master stations must have a "call in" switch to provide an audible and visual indication of incoming calls from remote stations. The master station must 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.

10.7.1.7 Intercom Substation must 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 must automatically transfer to another master station.

10.7.1.8 Multi-intercom Station must have the ability to call or monitor multiple stations individually or as a public address system.

10.7.1.9 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.

10.7.1.10 Push-to-Talk (PTT) Two-Way Communications is the typical type of intercom activation device, which requires a button be pressed in order to transmit conversation over the intercom.

10.7.1.11 Voice Operated Intercom Switching (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 must be used in interior or exterior areas; however, not in areas with high background noise, such as parking garages.

10.7.2 Security Phones and Emergency Call-Boxes

An emergency call-box or telephone system must be used instead of intercoms for a multi-facility environment, a standalone facility with a parking structure, or a site with a requirement to transmit call station communications to another site. Emergency call-boxes must be used in areas such as parking garages/lots, sidewalks, pathways of large campuses, and in isolated areas. (Refer to CFM's TDM paragraph 1.3 for AHJ contact information and TDM Chapter 7 for technical requirements.)

10.7.2.1 Push Button Hardwired: Emergency call-box systems must 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 must initiate a call-in to a pre-programmed master station. Once the button is pushed, hands-free operation must occur.

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

10.7.2.3 Speaker-Handset Stations: Emergency call-box stations must 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.

10.7.2.4 Scream Alert Option: Emergency call-boxes must provide the option that a speaker phone becomes activated when a loud scream is heard. This system must 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.

10.7.2.5 Integration with SSTV Cameras: Emergency call-boxes must provide coverage with SSTV when activated or have a built-in camera video surveillance capability that can be monitored from the SCC upon device activation. (See section 10.5.)

10.7.2.6 Remote Control and Monitoring: Emergency call-box master stations must 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 must provide auto-answer capability to allow VA

Police to monitor and initiate calls. The master stations must have the capability to remotely adjust speakerphone and microphone capabilities and reset the call-box activation from the central monitoring station.

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

10.7.2.8 Outdoor versus Indoor Locations: All emergency call-boxes must 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 must remain easily visible during low light conditions. SSTV and call-boxes must be integrated to provide automatic surveillance and priority monitoring of the caller's location.

- Emergency call-boxes in indoor locations must be easily accessible to the public, clearly marked, and may be wall mounted.
- All emergency call-boxes must be accessible to persons with disabilities.

10.7.3 Duress/Panic Alarms

Duress/panic alarms must 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 and provided as a standalone system (See CFM's TDM paragraph 1.3 for AHJ contact information and Chapter 7 for technical requirements). Upon activation, a silent alarm signal must be sent to a centralized monitoring location that must be capable of continuous operations. Other requirements associated with activated alarms will include all of the following.

- Alarms must be continuously monitored by the SCC.
- Activated alarms must be integrated with SSTV coverage of the area.
- Alarms must be mounted in such a manner as not to be observable and 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.

10.7.3.1 Switch/Push Button Hardwired: The duress/panic alarm system must 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 must identify the location of the alarm by phone extension and area description.

10.7.3.2 Wireless: Before selection and installation of a wireless system a survey must be conducted to determine if a wireless application is appropriate and feasible. Wireless systems must use ultrasonic, infrared, and radio frequency waves to link duress/panic devices with distributed transmitters and receivers. Receivers must be mounted throughout an area or building, as needed, and hardwired to a central monitoring console. Repeaters must be used to ensure full coverage. All wireless systems must conform to FCC and VA standards for wireless communications systems. Authorization from the VA AHJ is required prior to specification and use of wireless devices (Contact VACO's Spectrum Management and COMSEC Service's Special Communications Team, (SMCS – OSP 007), AHJ, for approval. Refer to TDM section 1.3 for contact information).

10.7.3.3 Switch/Push Button Telephone Extension: This system uses an existing telephone line and PBX to transmit a duress alarm. On activation the PBX must 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 must not use automatic voice dialers to 911 or the municipal police department.

10.7.3.4 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, can be used. The use of these devices must 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. Where a wireless pendant device is used, it must meet FCC wireless transmission standards and VA requirements, including use approved by the proper approving authority within VA. The devices must meet the following requirements.

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

10.7.3.5 Locators and Repeaters: The duress/panic alarm devices must be integrated with SCC and SMS software to provide identification and location of the user. Locators must be required for wireless/pendant devices. Where a wireless locator and repeater systems are used, they will meet FCC wireless transmission standards and VA requirements, including use approved by the proper approving authority within VA. Requirements for locators and repeaters are as follows.

- Locators must 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 must 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.

10.7.3.6 Automated Dispatch: Duress/panic alarm devices must automatically announce or provide alarm notification signals to on-site pagers worn by VA Police and other designated personnel, handheld portable radios, cell phones, and landline telephones.

10.7.3.7 Integration with SSTV Cameras and IDS: Duress alarm areas must be covered by SSTV cameras. Once the duress alarm has been activated the SSTV must monitor and record all events associated with the alarm. The IDS will provide monitoring of duress alarm. Refer to section 10.4.

10.7.4 1DSPI Locations

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

10.8 Public Address and Mass Notification System

VA facilities use a standalone public address (PA) system and may not have a Mass Notification System. (Refer to the TDM Chapter 7.)

At joint VA-DoD facilities, the determination on the use of PA/MSN will need to be negotiated by site. DoD uses the UFC 4-021-01 Mass Notification Systems and UFC Design: 4-510-01 Military Medical Facilities, along with the Defense Health Agency World Class Toolkit to develop MSN and PA guidance.

The design team must coordinate with the site OIT, Fire Alarm, and Emergency Manager to ensure system integration with other ESS or BCS are included in other plans, policies, procedures and operations in the SCC, IOC, or EOC.

10.8.1 System Elements and Features

PA/MNS are used for notification of events (manmade and natural hazard) and instructions that can be broadcast across the interior and exterior of the buildings and campus. (Refer to Appendix B, Security System Application Matrix, for locations where PA/MNS may be utilized.)

10.8.1.1 PA/MNS System Compatibility: All components of the PA/MNS must be fully compatible and not require the addition of either software or hardware interface equipment.

10.8.1.2 System Integration: The PA/MNS must be fully integrated with other security subsystems. (Note: Fire alarm systems must NOT be combined with other systems such as building automation, energy management, security, etc.)

10.9 Security Control Center, Integrated Operations Center, Emergency Operations Center

This section addresses the application, monitoring, control, programming, and interface of the Security Control Center (SCC), Integrated Operations Center (IOC), and Emergency Operations Center (EOC) with all security subsystems: PACS, IDS, SSTV, PA/MSN, DSPI, and DSS.

10.9.1 Security Control Center System Equipment and Interface

The SCC will be the central point for all monitoring, controlling, programming, and service for all security systems. Backup and secondary locations and related security equipment and capabilities must be identified to support the SCC should it become inoperable. All security subsystems must be fully integrated by either direct hardwiring of equipment or a computer based electronic Security Management System (SMS). The SCC must house all attended equipment primary power sources for each security subsystem, such as DVRs and monitors. Normally unattended equipment, such as servers, must be located in the Computer Room.

The SCC and security console must 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 standalone versus shared space requirements with other telecommunication space.

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

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

10.9.1.1 Integrated Operations Center System Equipment and Interface: The IOCs must have limited access to security systems, primarily monitoring perimeter SSTV. Future plans for IOCs designated as regional control centers will have additional security access to perform expanded missions or serve as the backup facility to the primary SCC.

10.9.1.2 Emergency Operations Center System Equipment and Interface: When a site does not have an SCC or IOC, the site EOC must have limited access to security systems, primarily monitoring perimeter SSTV. EOCs designated as backup SCC will have additional security access to perform expanded missions. In the majority of lease space, the DHS ISC criteria apply, and security systems are determined by the Facility Security Committee (Designated Official), and emergency management systems are provided by Federal Protective Service (FPS) or contract services.

10.10 Patient or Staff Annunciator/Locator (PAL)

This section addresses physical security criteria associated with the selection, application, and performance of the Patient or Staff Annunciator/Locator system (PAL). (Refer to the TDM section 7.2.8.5.)

10.10.1 System Elements and Features

The PAL system is used to locate patients and staff within the facility. (Refer to Appendix B, Security System Application Matrix, for optional locations where PAL systems may be utilized.)

10.10.1.1 PAL System Compatibility: PAL/Patient Annunciator/Locator (PAN) Antenna Headend (HE) equipment will be located in the Police Control Room (PCR), a dedicated room by the PCR, or the FMS area of a TR closet to the PCR and must be monitored, operated, and controlled by the SMS as approved by AHJ, VACO Spectrum Management and Communications Security (COMSEC) Service (SMCS – OSP 007) during the project design and technical reviews at the beginning and throughout the project.

10.10.1.2 System Integration: The PAL system is complete and separate standalone network that is a UL-2017 compliant and contains the PAN, Telecommunications Infrastructure Plant (TIP) (paragraph 7.2.3) including Telecommunications Outlets (TCO's) and Communications Circulating Grounding System (CCGS) (paragraph 7.2.4) systems and have location ID, connected to the PCR and Emergency Management Control Room (EMCR)'s SCC (and OSP's EMCC if not a part of the EMCR) and be

controlled and operated by the Police Service (add each associated Nurses Station when patient functions are performed).

10.11 Behavioral Health Area (Psychiatric or Mental Health Area)

This section addresses physical security criteria associated with the selection, application, and performance of the Behavioral Health Area systems (BHA). (Refer to the TDM Chapter 9.)

10.11.1 System Elements and Features

BHA systems are used for the safe holding of patients that may cause injury to themselves, other patients, or staff. (Refer to Appendix B, Security System Application Matrix, for optional locations where BHA systems may be utilized.)

10.11.1.1 BHA System Compatibility: All components of the BHA system must be fully compatible and not require the addition of either software or hardware interface equipment.

10.11.1.2 System Integration: The BHA system is a standalone network and must be installed according to VA patient privacy and HIPAA Rules and not connected to additional location(s) unless specifically pre-approved by VACO SMCS (SMCS – OSP 007).

10.12 Narcotics Storage Alerting and Signal System

This section addresses physical security criteria associated with the selection, application, and performance of the Narcotics Storage Alerting and Signal systems (NSAS). (Refer to the TDM Chapter 9.)

10.12.1 System Elements and Features

NSAS systems 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 building entry or delivery. (Refer to Appendix B, Security System Application Matrix, for optional locations where NSAS systems may be utilized.)

10.12.1.1 NSAS System Compatibility: All components of the NSAS system must be fully compatible and not require the addition of either software or hardware interface equipment.

10.12.1.2 System Integration: The NSAS system is a standalone network, must be DEA compliant and completely compatible, and operate with the project provided NSAS vault, cabinet, or container.

10.13 Detection and Screening Systems

Used only where specific site conditions require this level of security, detection and screening systems (DSS) include: X-ray screening machines, walk-through metal detectors (WTMD), hand-held metal detectors (HHMD), a desktop and hand-held trace/particle detectors (also called sniffers and itemizers), and Equipment RFIDs. 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; or to track and inventory valuable equipment and assets. Use of DSS equipment may be considered during periods of elevated credible threat from the National Terrorism Advisory System (NTAS).[50] Each facility will be addressed on a case-by-case basis concerning the use of DSS.

At a minimum, provide power and communications rough-ins for future installation of DSS equipment in the screening vestibule.

10.13.1 System Elements and Features

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 building entry or delivery. (Refer to Appendix B, Security System Application Matrix, for optional locations where DSS may be utilized.)

10.13.1.1 DSS System Compatibility: All components of the DSS must be fully compatible and not require the addition of either software or hardware interface equipment.

10.13.1.2 System Integration: The DSS must be fully integrated with other security subsystems.

[50] Formerly the Homeland Security Alert System (HSAS)

Annex to Chapter 10

A-10.1 VA and Industry Trends

ESS are a hybrid, or converged, system of traditional IT products and Operational Technologies (OT) products that must now be considered an exploit vector that can be used to penetrate into the larger VA network. These hybrid systems contain or transmit Personally Identifiable Information (PII), Protected Critical Infrastructure Information (PCII), Health Insurance Portability and Accountability Act (HIPAA), or Payment Card Industry (PCI) information/data. Examples of systems that may be hybrid, or converged, systems include:

- Access control/alarm systems that use badges/PIV Cards and Active Directory for keyless entry (contain PII).
- Keyless entry/keypad systems that use Active Directory (contain PII).
- Meter data management systems that interconnect with a local utility with real time demand and response (when the meter data is determined to contain PCII).
- Patient Monitoring and Wandering Systems (contain PII, HIPAA).
- Vehicle fueling/charging stations/pumps with credit card swipe (contain PCI).
- Computerized maintenance management systems/work order systems that interconnect with control system back-end controllers and devices (when the system is determined to contain PCII or PII).

The ESS design team must utilize the best practices as outlined in the Department of Homeland Security (DHS) Interagency Security Committee (ISC) *Securing Government Assets through Combined Traditional Security and Information Technology White Paper 2015*. Close coordination with the VA OIT will be required to create the documentation to document Federal Information Security Management Act (FISMA) and Federal Identify, Credential and Access Management (FICAM) compliance.

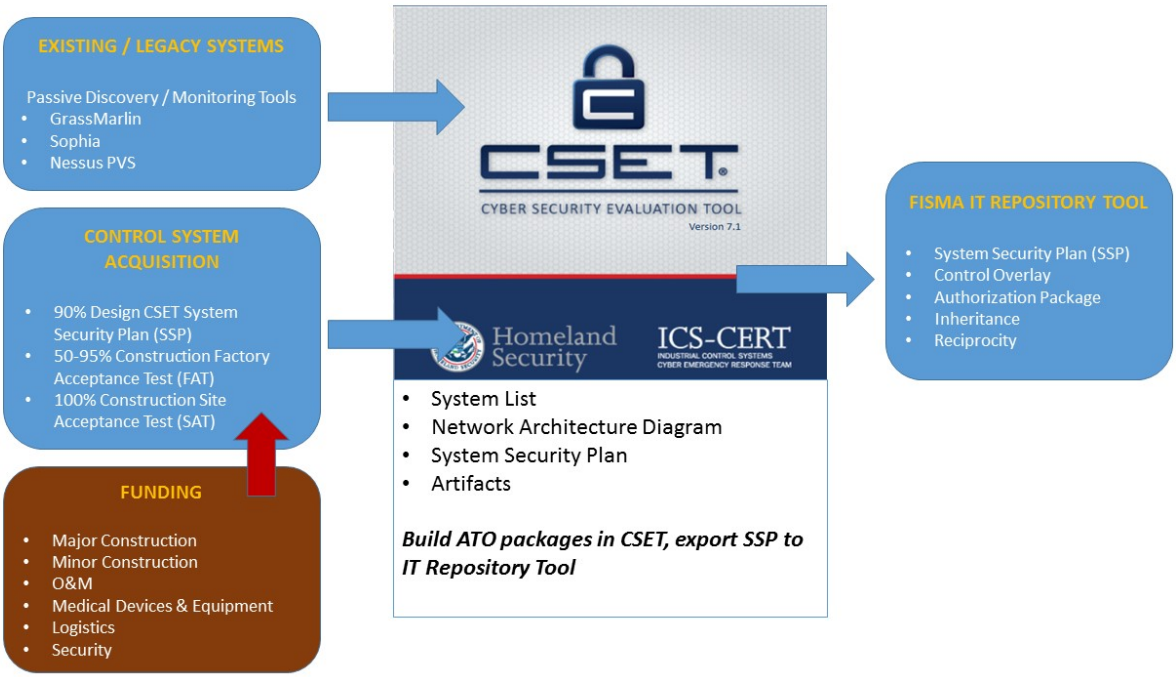
A-10.2 Cyber Security Evaluation Tool (CSET)

The DHS CSET is a useful tool that supports the ESS design, construction and authorization phases of the ESS lifecycle. CSET incorporates NIST, ISO, SANS, and other industry standard references. CSET includes the NIST SP 800-53 R4, NIST SP 800-82 R2, the NIST Cybersecurity Framework, and the Committee for National Security Systems Instruction (CNSSI) 1253 RMF standards and guidelines.

CSET has a plug-in (on initial install of CSET use the custom option) that connects to the National Security Agency-developed GrassMarlin (GM) passive network analysis tool. GM can be used to create an initial network architecture diagram of existing ESS. The CSET tool can be

used during design and construction to develop baseline risk assessments and initial System Security Plans (SSPs). SSPs are published as Word documents that can be copied into the OIT Information Repository tool. CSET and the OIT Information Repository tool relationship is shown in Figure A-10-1.

Figure A-10-1 Relationship of CSET, Component Registry, eMASS, and DITPR



A-10.3 GrassMarlin Passive Network Discovery Tool

In support of a passive means to generate an Industrial Control System network and discover IP devices, NSA has developed the GrassMarlin (GM) tool. GrassMarlin[51] is a software prototype that provides a method for discovering and cataloging Supervisory Control and Data Acquisition (SCADA) and Industrial Control System (ICS) systems on IP-based networks. GM uses a variety of sources to generate this data, including PCAP files, router and switch configuration files, CAM tables, and live network packet captures. The tool can automatically determine the available networks and generate the network topology as well as visualize the communication between hosts.

[51] GM is posted on GitHub at: https://github.com/iadgov/GRASSMARLIN

A-10.4 Designers Resources

The security consultants must comply with VA's latest construction specifications for ESS, found on the VA CFM TIL, and augmented by VA Policies and Directives. Additional sections must be prepared by the designer as necessary to suit the project requirements.

The Whole Building Design Guide Cybersecurity Resource Page[52] provides current cybersecurity practices and references for all types of building control systems. An example sequence and duration of ESS activities during design and construction is outlined in Table A-10-1.

Table A-10-1 Typical Sequence of ESS Design and Construction Activities

Activity / Lead	New Project	Renovation Project	Typical Duration
Presolicitation RFP Considerations	Categorize system(s)	Categorize system(s)	NA
Design • Concept Design (10-15%) • 50% Progress • Pre-Final (90%) • Final (100%) Lead: A/E Documents/Models/Tools: • Construction Design Documents / Building Information Model (BIM) / CAD • CSET • GrassMarlin • Draft Baseline System Security Plan (SSP) • IT Contingency Plan and CONOPS	ESS front end or new susbsystem back end to connect to front end Confirm/revise system categorization, define network architecture, system components, concept of operations, drawings, and specifications. At 90% design create initial SSP and baseline risk assessment.	ESS front end upgrade or subsystem modernization Confirm/revise system categorization, define network architecture, system components, concept of operations, drawings, and specifications. At 90% design create initial SSP and baseline risk assessment.	3 – 6 Months

[52] https://www.wbdg.org/resources/cybersecurity.php

Activity / Lead	New Project	Renovation Project	Typical Duration
Construction Test and Development (T&D) and Patch Management Environments (Virtual or Physical) Lead: Construction/System Integrator Documents/Models/Tools: • VM • Kali Linux • Microsoft Enhanced Mitigation Experience Tool • Qualsys SSL Labs Server and Broswer Test • SamuraiSTFU • Security Techincal Implementation Guides (STIGS) • Software Content Automation Process (SCAP) Tool	Conduct ESS build and patch activities without impacting the organization's production systems (test and development environment typically provided by vendor).	Validate and verify the upgrade/modernization / patch is ready to support the additional systems without impacting the organization's production systems (test and development environment typically provided by vendor).	4 – 6 weeks
Construction Build/Configure Servers	Build and/or configure servers to properly operate the ESS solution.	Build and/or configure servers to properly operate the ESS solution.	1 – 2 weeks
Construction Install Supporting Software Lead: Construction/System Integrator	Install supporting software on ESS servers.	Install supporting software on ESS servers.	1 – 2 weeks

Activity / Lead	New Project	Renovation Project	Typical Duration
Construction Configure Supporting Software Lead: Construction/System Integrator Documents/Models/Tools: • Continuous Monitoring tool(s) • Interconnection Security Agreement (if required) • Kali Linux • Qualsys SSL Labs Server and Broswer Test • SamuraiSTFU • STIGS • SCAP • USACE PVT TSF	Configure ESS software to meet unique needs. After the operating system is loaded, apply hardening criteria (STIGs), run Security Content Automated Protocol (SCAP)-validated tool, perform factory acceptance testing (FAT) on major system components and devices, perform initial penetration testing.	Configure ESS software to meet unique needs. After the operating system is loaded, apply hardening criteria (STIGS), run Security Content Automated Protocol (SCAP)-validated tool, perform FAT on major system components and devices, perform initial penetration testing.	1 – 2 weeks
Construction Implement and assess security controls Lead: construction/system integrator Documents/Models/Tools: • CSET and SMART • System Security Plan (SSP) • Security Assessment Report (SAR) • Plan of Action & Milestones (POAM) • IT Contingency Plan and CONOPS (ITCP) • Incident Communication Procedures (ICP) • Secuirty Audit Plan (SAP)	Conduct RMF Steps 3 and 4 by applying controls identified during the requirements and design phase, by assessing the adequacy and effectiveness of security controls, and by documenting findings in the security assessment report. Create draft approval package.	Conduct RMF Steps 3 and 4 by applying controls identified during the requirements and design phase, by assessing the adequacy and effectiveness of security controls, and by documenting findings in the security assessment report. Create draft approval package.	12 – 20 weeks

Activity / Lead	New Project	Renovation Project	Typical Duration
Conduct testing on initial build Lead: construction/system integrator Documents/Models/Tools: • Kali Linux • SamuraiSTFU • SAR • POAM	Test ESS solution in a test and development environment to ensure system errors are found, corrected before solution is deployed on network.	Test ESS solution in a test and development environment to ensure system errors are found, corrected before solution is deployed on network.	2 – 4 weeks
Construction — conduct pilot implementation deployment Lead: construction/system integrator Documents/Models/Tools: • Kali Linux • SamuraiSTFU • OIT IT Repository and Authority To Operate (ATO) GRC Tool • USACE PVT TSF • SSP • POAM • SAP	Pilot implementation of ESS solution on a small subset of user base to evaluate solution against real-world requirements. Conduct site acceptance testing, final penetration testing, and create final approval package.	Conduct site acceptance testing, final penetration testing, and create final approval package.	Varies with size of deployment (number of facilities and interconnections)
Receive Authorization (ATO) and move to production Lead: construction/system integrator Documents/Models/Tools: • Continuous Monitoring tools • OIT IT Repository and Authority To Operate (ATO) GRC Tool	Deploy the ESS to full production and implement continuous monitoring.	Deploy the ESS to full production and extend continuous monitoring to new systems.	NA

A-10.5 ESS Performance Work Statement Template

A typical Electronic Security System (ESS) Performance Work Statement template is provided in the Annex to Chapter 10. Cybersecurity of the ESS begins in the planning and design phases, it is imperative that the ESS design and construction teams understand the NIST and VA RMF processes and the various documents and artifacts associated with an Authorization package. In general, the following documents will be required:

- System Security Plan (SSP)
- Plan of Action & Milestones (POAM)
- Security Assessment Report (SAR)
- Information Technology and Contingency Plan (ITCP)
- Incident Communication Procedures (ICP)
- Security Audit Plan (SAP)

The GSA Fed RAMP website has many templates and guidance at:
https://www.fedramp.gov/resources/templates-3/

A-10.5.1 ESS Performance Work Statement Template

Performance Work Statement: Electronic Security Systems

A. General Information

Description of Services/Introduction: Provide all personnel, equipment, tools, materials, supervision, non-personal services, and other items necessary to procure, install, service, and maintain Electronic Security Systems (ESS). ESS can include the incorporation of physical security and force protection measures, and Automated Control Systems to include building automation systems, fire alarm systems (FAS), life-safety systems, mass notification systems (MNS), chemical/biological/radiological detection/response systems, and other related electronic systems. For specific security specification requirements, refer to VA CFM Master Specifications Divisions 27 27 05 11 Requirements for Communications Installations; 27 10 00 Control, Communications and Signal Wiring; 27 15 00 Communications Structured Cabling; 28 28 13 00 (PACS); and 28 13 16 (PACS and Database Management); see also CFM Telecommunications Design Manual (TDM) specifically Chapter 7 and the OIT Design Guide.

B. Attachment 1.0: Information Assurance (IA) Requirements

1.0 General: This exhibit provides detailed cybersecurity requirements for this PWS. Upon Contractor request the Government will provide a review of documents before official

submittals. Cybersecurity will be placed on the agenda of the post-award orientation meeting for further discussion upon contractor request.

2.0 Completion and Government Acceptance of the System(s) Security Plan: In accordance with VA Handbook 6500 and NIST SP 800-53 R4, all VA Information Systems (IS) are required to obtain an Authority to Operate (ATO) via the Risk Management Framework (RMF) process. The VA OIT Governance, Risk, and Compliance (GRC) tool, the Enterprise Mission Assurance Support Service (eMASS), is the tool used for producing and submitting a System Security Plan that meets the requirements of RMF, in order to obtain an ATO. Where cloud services are utilized, refer to VA Directive and Handbook 6517 for additional requirements.

3.0 Completion and Government Acceptance of Cybersecurity Artifacts and Other Required Cybersecurity Documents: The Contractor must register their system in the VA OIT GRC tool, then develop and upload all required artifacts and supporting documentation. This effort should result in the creation of a System Security Plan (SSP) packet. The required artifacts are determined by the system security classification, system categorization, and cybersecurity controls. This information includes but is not limited to the list below:

a. System Description Statement
b. Configuration Management Plan
c. Disaster Recovery Plan
d. Continuity of Operations
e. Contingency Plan
f. Incidence Response Plan
g. Risk Assessment Report
h. Plan of Action and Milestones (POAM)
i. System Architecture/Topology/Data Flow
j. Configuration Validation Checklist
k. Security Classification Guide
l. System Configuration Guide
m. Hardware Inventory List
n. Software Inventory List
o. Physical Security Plan
p. Personnel Security Plan

q. Information Assurance Vulnerability Management (IAVM) Process

r. Patch Management Process, Connection Approval / System Approval documentation

s. Ports, Protocols, and Services (PPS) List

t. Active Directory (AD) Documentation, (when applicable)

The data representing this information must be uploaded directly, or cut and pasted, into VA OIT GRC tool for each applicable control. In addition, VA OIT GRC tool will provide a rollup of inherited controls for each system once it has been properly identified and classified within the VA OIT GRC tool. The current version of the Department of Homeland Security (DHS) Cyber Security Evaluation Tool (CSET) must be used as a development tool for VA OIT GRC tool artifacts.

4.0 Completion of Scan/Fix/Scan Testing and Analysis: This work is performed before the Security Control Assessor (SCA) assesses the system(s) and provides a certification recommendation to the Authorizing Official (AO). The Contractor must assess (scan and perform manual checks) its own system using approved cybersecurity scanning tools. When issues are found (High, Medium, Low Impact Levels) the Contractor must fix those issues and rescan the system to ensure all issues have been fixed and/or properly and acceptably mitigated. High impact level findings that cannot be fixed are to be reported to the Government immediately through the VA OIT GRC tool along with a valid reason the vulnerability cannot be fixed and a mitigation plan to fix the vulnerability in the future. The goal is for the system to have a proper cybersecurity posture before the SCA comes in to assess the system. The scan/fix/scan process should find and fix all issues before the SCA's assessment.

5.0 Completion of Documentation to Connect to the Government VA Network: This must be based on the VA Network Enterprise Center's connection approval process (CAP). The Contractor must provide required assistance and documentation to the Government to satisfy the CAP. Normally this entails having an approved ATO, but it may vary depending on the site. When Penetration Vulnerability Testing (PVT) will be performed on the sites network then completion of the Network Enterprise Center CAP should be scheduled to occur before PVT. When PVT is not performed then the timeline for the CAP must be at least forty-five (45) days before connecting to the sites network.

11 GLOSSARY & ACRONYMS

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

A/E: Architect(s) and Engineer(s) consultants.

Access Control: The act of managing ingress or egress through a portal by validating a credential or individual (NFPA 730).

Alterations: See table 2-1 Project Scopes/Requirements Table.

Anti-Ram: 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 or "M" rating in tests for certification under ASTM F2656.

Authority Having Jurisdiction (AHJ): The final decision-maker, who is responsible for overseeing the implementation of physical security and resiliency requirements for facilities within his or her jurisdiction. See section 1.3 Administration and Enforcement.

Balanced Design: Controlled failure of a system with an established hierarchy of component failures, where connections are designed for the maximum strength of the connecting components and members supporting other members are designed for the maximum strength of the supported members. For window systems, the glazing must fail before all other components. (ASCE/SEI 59-11 Blast Protection of Buildings)

Baseline Requirements: Minimum requirements that must be implemented unless deviations are justified by a risk assessment and approved by the AHJ.

Cache: A storage facility requiring a high level of security, often referring to facilities storing pharmaceuticals or other supplies for use in emergencies.

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

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. Historically, the term for a security video system was closed circuit television (CCTV), a closed analog video system. Very few video systems today are either closed or completely analog, making CCTV an antiquated term and leading the security industry to use various terms to describe a video system. Because security video serves two distinct purposes, assessment and surveillance, the term used here is video assessment and surveillance system or VASS. This provides a common term based on the functions the system serves, independent of technology.

Command Centers: Note the **National Incident Management System (NIMS)** is a standardized approach to incident management developed by the Department of Homeland Security, using

the term **Incident Command Post**, rather than **Incident Command Center**. The Incident Command Post is wherever the Incident Commander needs to be to control the ongoing response. It may be near the Fire Command Center or if the incident is on the far side of the building the Incident Command Post may be away from the Fire Command Center. See also **Fire Command Center (FCC)** and **Emergency Operations Center (EOC).**

Computer Room: Formerly Main Computer Room. Revised in anticipation of future changes to TIL ICT standards to reflect federal government data center consolidation and resulting deprecation and removal of Backup Computer Rooms, thus eliminating the need for the qualifier "Main" on the remaining computer room.

Comprehensive Emergency Management Plan (CEMP)

Consequences: Consequences assessment looks at the value of a building's critical assets, those that need to be protected, and the importance of the building's operations, within a wider network of public or private activities. (FEMA 452)

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.

Crime Prevention Through Environmental Design (CPTED): A multi-disciplinary approach to deterring criminal behavior through environmental design. CPTED strategies rely upon the ability to influence offender decisions that precede criminal acts by affecting the built, social and administrative environment. (International CPTED Association)

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

Critical Equipment: Equipment that supports critical systems for the Continuity of Operations in VHA mission critical facilities (see Annex to Chapter 1).

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

Department of Agriculture (USDA)

Department of Defense (DoD)

Department of Health and Human Services (HHS)

Department of Homeland Security (DHS)

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 as "sniffers" and "itemizers").

Deterrence: Any physical or psychological device or method that discourages action. (NFPA 730)

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.

Earthquake Zones: See seismic zones.

Electronic Security System (ESS): A sub-element of the physical security system, an electronic security system is comprised of Physical Access Control System (PACS); Intrusion Detection System (IDS); Video Assessment and Surveillance System (VASS); Duress, Security Phones, Intercom (DSPI) System; and Detection and Screening System (DSS). The ESS is commonly integrated to support correlation of security activity between subsystems.

Emergency Operations Center (EOC): A room in the building with communication feeds to monitor the incident, plan future activities and coordinate resources for the Incident Commander during the response phase of an event. Prior to the event, such as during preparation for a hurricane, and after an event, during recovery, the EOC plays a more controlling role.

Entrance Room: The separation point between utility-owned and VA-owned information technology service and equipment. Previously designated as a Demarcation Room, or Demarc.

Essential Electrical System (EES): A system comprised of alternate sources of power and all connected distribution systems, fuel systems, and ancillary equipment designed to ensure continuity of electrical power to designated areas and functions of a health care facility during disruption of normal power sources, and also to minimize disruption within the internal wiring system. See also Command Center.

Extraordinary Event or Incident: Events or conditions that are unusual or unpredictable in their severity and that may impose forces or loads on structures that exceed those for which the structure was designed.

Federal Emergency Management Agency (FEMA)

Fire Command Center (FCC): A room near an entrance that has the Fire Alarm Zone display, elevator display and controls, PA system, building plans, communications devices allowing personnel in the FCC to communicate with emergency responders elsewhere in the building, and other resources to aid response. See also Command Centers.

General Services Administration (GSA)

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

Hazard Vulnerability Assessment (Analysis) (HVA)

High Risk Area: A location where a threat/hazard may occur or be introduced.

Hurricane Areas: Hurricane preparedness requirements apply to VA facilities located within 16 kilometers (10 miles) of the Atlantic Ocean or 16 kilometers (10 miles) of the Gulf of Mexico. These requirements also apply to all inland VA facilities in Florida, Hawaii, and Puerto Rico. Similar requirements, for preparedness against tropical cyclones in the Pacific Ocean, apply to VA facilities located in Guam, American Samoa, and the Philippines. See also ASCE 7-10, section 26.2 Definitions, for Hurricane Prone Regions and Wind-Borne Debris Regions.

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

Illumination Engineering Society of North America (IESNA)

Incident Command Center (ICC): See Command Center.

Information and Communications Technology (ICT): A collective term for both information technology systems and telecommunications systems. The typical use in this standard is to refer to OIT and telecommunications standards on the TIL collectively, i.e. ICT standards, in anticipation of changes to the titles, scope, and content of the individual documents currently on the TIL.

Interagency Security Committee (ISC)

Intrusion Detection System (IDS): A system combining mechanical or electronic 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; also referred to as a sniffer.

Life-Safety Protected (LSP) Facilities: VA facilities that are intended to protect the life safety of the patients, staff, and visitors in case of an emergency. Although indispensable to the mission of VA, they are not required to remain operational during and following a natural or manmade extreme event or a national emergency.

Life-Safety Protected (LSP) Facilities w/ Mission Critical (MC) Utilities/Systems Redundancies: VA facilities that are intended to remain functional with minor repairs during and following a natural or manmade extreme event or a national emergency, in addition to protecting the life safety of occupants.

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 or Sally-port: A booth or chamber with two sets of remotely operated doors (or gates) that allows a person to enter at one end, undergo an access identification routine inside the booth, and when the routine is satisfied, the lock on the booth door at the other end is released. A mantrap is used in high security environments where absolute access control is required.

Mission Critical (MC) Facilities: VA facilities that are intended to remain fully functional during and following a natural or manmade extreme event or a national emergency.

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

National Archives and Records Administration (NARA)

National Disaster Medical System (NDMS)

National Environmental Policy Act (NEPA)

National Historic Preservation Act (NHPA)

National Incident Management System (NIMS): See also Command Centers.

National Terrorism Advisory System (NTAS): Formerly the Homeland Security Alert System (HSAS).

Nationally Recognized Testing Laboratory (NRTL): An organization which is recognized by OSHA in accordance with Appendix A of 29 CFR 1910.7 and which tests for safety, and lists or labels or accepts, equipment or materials and which meets all of the criteria in 29 CFR 1910.7(b).

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.

Personal Identification Number (PIN)

Personal Identity Verification (PIV)

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

Physical Access Control System (PACS): A system combining mechanical or electrical components, such as card readers, keypads, biometrics, and electromagnetic locks and strikes, for 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.

Resiliency: the power or ability to return to the original form, position, or shape after being bent, compressed, or stretched; elasticity (www.dictionary.com). For the resiliency of facilities, site energy availability, reliability, and redundancy are critically important to continuity of operations and to minimizing the duration of lost operations. For guidance on the resiliency of infrastructure see High Performance Based Design for the Building Enclosure: A Resilience Application Project Report, BIPS 10 / November 2011 at http://wbdg.org/ccb/DHS/bips_10.pdf.

Restricted Area: A 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.

Screened Vehicle: Motor vehicle that has been examined systematically to determine whether a security threat that needs to be mitigated is present.

Screening Vestibule: Designated space or area located for access control between the public building entrance and the lobby which must 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 resistance rating, or similar feature.

Security Control Center (SCC): A location for security personnel to monitor VASS, 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.

Security Surveillance Television (SSTV): One of the Electronic Security Systems (ESS) which includes cameras, monitors, controlling and recording equipment, and centralized management and operations of the system, used for both event assessment and general surveillance; also referred to as Closed Circuit Television (CCTV) and Video Assessment and Surveillance System (VASS).

Seismic Zones: See VA H-18-8: VA Earthquake Design Requirements.

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

Sniffer: A trace particle detection device capable of identifying both explosives and narcotic; also referred to as an itemizer.

Standby Electrical System: Generators, switchgear, fuel storage, and distribution equipment necessary to provide standby electrical power to the mission critical facility.

Standoff: Horizontal distance from event to target.

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: The National Infrastructure Protection Plan (NIPP) defines threat as any “natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.”
http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Underwriters Laboratory (UL)

Uninterruptible Power Supply (UPS): A device to provide battery power via an inverter to critical equipment during loss of utility power, or until the essential electrical system (EES) or standby generators are online. A UPS is used when even a momentary interruption of electrical power cannot be tolerated by the equipment it supports.

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 defensive zone (perimeter).

Vehicle Barrier: A passive or active physical barrier consisting of natural or manmade features designed to keep unscreened vehicles from parking or traveling within the required standoff 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.

VHA Sites of Care: Veterans Health Administration (VHA) points of service are all rated through the VHA site classification process. Each unique point of service is rated in all four major medical care categories: outpatient, inpatient, residential, and extended care. These ratings are broken down into sub-ratings for each category and are based on actual workload completed at each point of service in the prior fiscal year. See VHA Handbook 1006.02 Appendix A, December 30, 2013, Site Classification Process.

Vulnerability: Susceptibility to physical injury to persons or damage to systems or functions. Vulnerability refers to the expected outcome in terms of damage, casualties, and business disruption if a threat is carried out or a hazard occurs. Vulnerability is measured by assessing features that would enhance or diminish building performance during a crime, terrorist attack, or a hazard event. (FEMA 452)

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

12 REFERENCES

This section lists applicable codes and regulations, standards, design guidelines, and resources. Use the latest edition of Codes, Standards and Executive Orders as a basis of design. Refer to PG-18-3, Topic 1, Codes, Standards and Executive Orders.

American National Standards Institute (ANSI)

- ANSI/SIA/CSAA SIA AC-01-1996.10, Access Control Standard Protocol for the 26-bit Wiegand TM Reader Interface
- ANSI/SIA/CSAA SIA AC-03-2000.06, Access Control Guidelines
- ANSI/SIA/CSAA SIA AV-01-1997.11, Two-Way Voice – Monitoring Service Command Set
- ANSI/SIA/CSAA STA1 Guide
- ANSI/SIA PIR-01-2000, Passive Infrared Motion Detector Standard - Features for Enhancing False Alarm Immunity

American Society for Testing and Materials (ASTM)

- ASTM F476 Standard Test Methods for Security of Swinging Door Assemblies
- ASTM F588 Standard Test Methods for Measuring the Forced Entry Resistance of Window Assemblies, Excluding Glazing Impact
- ASTM F842 Standard Test Methods for Measuring the Forced Entry Resistance of Sliding Door Assemblies, Excluding Glazing Impact
- ASTM F2200 Standard Specification for Automated Vehicular Gate Construction
- ASTM F2656/F2656M Standard Test Method for Vehicle Crash Testing of Perimeter Barriers
- ASTM F1233 Standard Test Method for Security Glazing Materials and Systems
- ASTM F1642 Standard Test Method for Glazing and Glazing Systems Subject to Airblast Loadings

American Society of Civil Engineers (ASCE)

- ASCE/SEI 7, Minimum Design Loads for Buildings and Other Structures (Third Printing)

Architectural and Transportation Barriers Compliance Board (Access Board)

- ABA Accessibility Standards

Building Industry Consulting Service International (BICSI)

- Building Industry Consulting Service International (BICSI) Telecommunications Distribution Methods Manual (TDMM)

Centers for Disease Control and Prevention (CDC)

- Biosafety in Microbiological and Biomedical Laboratories (BMBL)

Code of Federal Regulations (CFR)

- 41 CFR 101 Federal Property Management Regulations
- 42 CFR Part 73 Select Agents and Toxins
- 44 CFR 60.3 Flood plain management criteria for flood-prone areas

Facility Guidelines Institute

- Guidelines for Design and Construction of Hospitals and Outpatient Facilities
- Guidelines for Design and Construction of Residential Health, Care, and Support Facilities

Florida Department of Community Affairs

- Florida Building Code

General Services Administration (GSA)

- The Site Security Design Guide
- GSA Security Containers

IDManagement.gov (GSA National Customer Service Center)

- FIPS 201 (HSPD-12) Evaluation Program
- GSA HSPD-12 Approved Products List

Interagency Security Criteria (ISC)

- Alternate Path Analysis & Design Guidelines for Progressive Collapse Resistance
- ISC New Federal Office Buildings and Major Modernization Projects (For Official Use Only)
- ISC Security Standards for Leased Space (For Official Use Only)

International Association for Healthcare Security and Safety (IAHSS)

- Healthcare Security Industry Guidelines

International Code Council (ICC)

- International Building Code (IBC)

International CPTED Association

- Crime Prevention through Environmental Design (CPTED)

International Organization for Standardization (ISO)

- ISO 7816-1: Identification Cards – Integrated Circuit Cards – Part 1: Cards with Contacts Physical Characteristics
- ISO 7816-2: Identification Cards – Integrated Circuit Cards – Part 2: Cards with Contacts - Dimensions and Location of the Contacts
- ISO 7816-3: Identification Cards – Integrated Circuit Cards – Part 3: Cards with Contacts - Electrical Interface and Transmission Protocols
- ISO 7816-4: Identification Cards – Integrated Circuit Cards – Part 4: Organization, Security and Command for Interchange
- ISO 14443: Identification Cards – Contactless Integrated Circuit Cards - Proximity Cards - Part 1: Physical Characteristics
- ISO 15693: Identification Cards Contactless Integrated Circuit Cards - Vicinity Cards – Part 3: Anti-collision and Transmission Protocol
- International Organization for Standardization (ISO) 8528-5, Reciprocating Internal Combustion Engine Driven Alternating Current Generating Sets, Part 5: Generating Sets

The Joint Commission (TJC)

- TJC Environment of Care

National Electrical Contractors Association (NECA)

- National Electrical Contractors Association Standard, NECA 303, Installing Closed-Circuit Television (CCTV) Systems

National Electrical Manufactures Association (NEMA)

- NEMA 250, Enclosures for Electrical Equipment

National Fire Protection Association (NFPA)

- NFPA 1: Fire Code
- NFPA 13: Standard for the Installation of Sprinkler Systems
- NFPA 22: Standard for Water Tanks for Private Fire Protection
- NFPA 70: National Electrical Code
- NFPA 72: National Fire Alarm and Signaling Code
- NPFA 75: Standard for the Fire Protection of Information Technology Equipment
- NFPA 99: Health Care Facilities Code,
- NFPA 101: Life Safety Code
- NFPA 110: Standard for Emergency and Standby Power Systems
- NFPA 730: Guide for Premises Security
- NFPA 731: Standard for the Installation of Electronic Premises Security Systems
- Thompson, A. C. T., Kammerer, A. M., Katzman, G. M., and Whittaker, A. S. "Natural Hazards," Chapter 7 in Meacham, B.J. and Johann, M.J., eds. Extreme Event Mitigation in Buildings: Analysis and Design. Quincy, MA: National Fire Protection Association, 2006.

UL (formerly Underwriters Laboratories)

- UL 639: Standard for Intrusion-Detection Units
- UL 681: Standard for Installation and Classification of Burglar and Holdup Alarm Systems
- UL 752: Standard for Bullet-Resisting Equipment

U.S. Army Corps of Engineers

- USACE Protective Design Center (PDC) Technical Report, PDC-TR-06-08, Single Degree of Freedom Structural Response Limits for Antiterrorism Design (Unrestricted)

U.S. Department of Commerce, National Institute of Standards and Technology (NIST)

- NIST Special Publication 800-53 R4 Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-82 R2 Guide to Industrial Control Systems (ICS) Security

- NIST Special Publication 800-116 A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)
- NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems

Federal Information Processing Standards (FIPS)

- FIPS Pub 200 Minimum Security Requirements for Federal Information and Information Systems
- FIPS Pub 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors

U.S. Department of Defense (DoD), Unified Facilities Criteria (UFC)

- UFC 3-340-01 Design and Analysis of Hardened Structures to Conventional Weapons Effects
- UFC 4-010-01 DoD Minimum Antiterrorism Standards for Buildings (Unrestricted)
- UFC 4-021-01 Design and O&M: Mass Notification Systems
- UFC 4-022-01 Security Engineering: Entry Control Facilities/Access Control Points, May
- UFC 4-022-02 Selection and Application of Vehicle Barriers
- UFC 4-023-03 Design of Buildings to Resist Progressive Collapse
- UFC Design 4-510-01 Design: Military Medical Facilities

U.S. Department of Homeland Security (DHS)

- Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors

Interagency Security Committee (ISC)

- Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper
- Securing Government Assets through Combined Traditional Security and Information Technology: An Interagency Security Committee White Paper
- The Risk Management Process: An Interagency Security Committee Standard

Federal Emergency Management Agency (FEMA)

- BIPS 06/FEMA 426: Reference Manual to Mitigate Potential Terrorist Attacks against Buildings

U.S. Department of State (DOS)

- SD-STD-01.01, Revision G, Certification Standard Forced Entry and Ballistic Resistance of Structural Systems
- SD-STD-02.01, Revision A, Test Method for Vehicle Crash Testing of Perimeter Vehicle Barriers and Gates

U.S. Department of Veterans Affairs (VA) (VA Pubs, CFM Tech Info Lib)

- VA Barrier Free Design Guide (PG-18-13)
- VA Directive 0730 Security and Law Enforcement, 2012, and VA Handbook 0730/4
- VA Directive 6500 Information Security Program (Note: User can request a copy of this directive from VA OIT Enterprise Records Management Service)
- VA Directive 6517 (2016) Risk Management Framework for Cloud Computing Services, and VA Handbook 6517 (2016)
- VA Electrical Design Manual
- VA Fire Protection Design Manual
- VA Handbook 0320, Comprehensive Emergency Management Program
- VA Handbook 0730/4, Security and Law Enforcement, Appendix B
- VA Handbook 1200. 6, Control of Hazardous Agents in VA Research Laboratories
- VA Handbook 1200.8, Safety of Personnel Engaged in Research
- VA Lighting Design Manual
- VA Office of Information and Technology FY 2013-2015 Information Resources Management Strategic Plan
- VA Program Guide PG-18-3, Design and Construction Procedures
- VA Program Guide PG-18-9, Space Planning Criteria
- VA Program Guide PG-18-14, Room Finishes, Door and Hardware Schedule
- VA Signage Design Guide
- VHA Directive 0320, Comprehensive Emergency Management Program (CEMP)
- VHA Directive 1047, All-hazards Emergency Caches
- VHA Directive 2008-062, Boiler Plant Operations

- VHA Directive 2010-016, Inspection of All-Hazard Emergency Caches by the Emergency Management Strategic Health Care Group
- VHA Handbooks 1200.8, 1200.6; Memo– BSL Research Lab Physical Security Inspections
- VHA Sites of Care at VHA Handbook 1006.02 Appendix A, Site Classification Process
- NCA Design and Construction Criteria

U.S. Postal Service (USPS)

- Publication 166, Guide to Mail Center Security

The White House

- Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors and Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors
- Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience
- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance

This page is intentionally blank.