



CBP Security Policy and Procedures Handbook

HB1400-02B
August 13, 2009



U.S. Customs and
Border Protection

Security Never Sleeps

BACK

VOLUME CONTENTS

1. FOREWORD.....V

2. REVISION HISTORY.....XVII

3. PHYSICAL SECURITY HANDBOOK.....VII

4. INFORMATION SECURITY: SAFEGUARDING CLASSIFIED
AND SENSITIVE BUT UNCLASSIFIED INFORMATION HANDBOOK ... 735

5. BADGES, CREDENTIALS AND OFFICIAL IDENTIFICATION 845



U.S. Customs and Border Protection

Commissioner

FOREWORD

AUG 13 2009

The Office of Internal Affairs (IA) Security Management Division (SMD) is responsible for establishing policies, standards, and procedures to ensure the safety and security of the U.S. Customs and Border Protection (CBP) personnel, facilities, information, and assets. IA/SMD has developed the CBP Security Policy and Procedures Handbook to provide CBP with uniform standards and procedures for the proper administration of Physical Security; Safeguarding Classified and Sensitive but Unclassified Information; and Badges, Credentials, and Official Identification. This handbook serves as mandatory minimum requirements for CBP managers to implement and improve the security posture for their designated CBP area of responsibilities.

This handbook implements security policies and standards published in a number of relevant source documents including numerous Public Laws, Presidential Directives, regulations, rules, Interagency Security Committee security design criteria, and U.S. Department of Homeland Security (DHS) Management Directives (MD) regarding integrating, managing, and governing various Security functions. It is issued under the authority of DHS MD 11080; *Security Line of Business Integration and Management*, January 3, 2006.

This handbook supersedes the CBP memorandum; *Interim Physical Security Guidance for Customs and Border Protection (CBP) Facilities*, October 25, 2006; Customs Handbook (HB) 1400-02A, *Physical Security Handbook*, April 2000; Customs Directive No. 5230-029A, *Employee Badges and Credentials*, April 20, 2002; Customs HB 1400-03, *Safeguarding Classified Information Handbook*, February 15, 1991; U.S. Immigration and Naturalization Service (INS), *Security Officer's Handbook (SOH)*, September 2001; legacy U.S. Department of the Treasury, U.S. Customs Service, INS, U.S. Border Patrol, and U.S. Department of Agriculture's Animal and Plant Health Inspection Service security policies and directives.

The CBP Security Policy and Procedures Handbook is effective immediately and applicable to ALL CBP-owned, -leased or -occupied offices, facilities, installations, ports of entry, and stations. Compliance with this handbook is mandatory and will ensure consistent standards and effectiveness in executing security initiatives for the preservation of CBP's mission to safeguard our Nation from terrorists and the instruments of terror.

This handbook may be accessed through the CBPnet, Office of Internal Affairs website quick links at <http://cbpnet.cbp.dhs.gov/xp/cbpnet/ia/> or CBP's Policy Online Document Search (PODS) website: <http://pods.cbp.dhs.gov/>. To request further assistance or offer feedback regarding this handbook, contact the Security Management Division at (202) 325-0110 or by submitting your comments through the [SMD Policy and Procedures Handbook Comment form](#).

A blue ink signature of Jayson P. Ahern, written in a cursive style, extending across the page.

Jayson P. Ahern
Acting Commissioner

FOR OFFICIAL USE ONLY
CONTENTS

BACK

1. CHAPTER 1: PURPOSE 1

1.1. PURPOSE..... 2

2. CHAPTER 2: POLICY 3

2.1. POLICY..... 4

2.2. POLICY EXCEPTION REQUIREMENTS 5

3. CHAPTER 3: BACKGROUND 7

3.1. BACKGROUND 8

4. CHAPTER 4: AUTHORITIES AND REFERENCES 9

5. CHAPTER 5: RESPONSIBILITIES 15

5.1. COMPONENT HEAD..... 16

5.2. CBP COMPONENT CHIEF SECURITY OFFICER 16

5.3. ASSOCIATE CHIEF SECURITY OFFICER 16

5.4. PHYSICAL SECURITY BRANCH (PSB) CHIEF 16

5.5. FIELD SECURITY OPERATIONS BRANCH (FSOB) CHIEF..... 16

5.6. REGIONAL SECURITY OFFICERS (RSOs)..... 16

5.7. DISTRICT SECURITY OFFICERS (DSOs) 16

5.8. DESIGNATION OF SECURITY OFFICERS AND OFFICIALS 17

5.9. PHYSICAL SECURITY SPECIALISTS (PSSs) 17

5.10. IA/PSD PERSONNEL SECURITY OFFICERS 17

5.11. IA/SMD INFORMATION SECURITY OFFICERS 18

5.12. CLASSIFIED DOCUMENT CUSTODIAN, CLASSIFIED CONTROL STATION 18

5.13. DERIVATIVE CLASSIFIERS 18

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

5.14. DESIGNATED OFFICIAL (DO) 18

5.15. ASSESSMENTS 18

6. CHAPTER 6: FACILITY PROTECTION 19

6.1. GENERAL 20

6.2. PLANNING FACILITY PROTECTION..... 20

6.3. DETERMINING BUILDING SECURITY LEVEL 22

6.4. BUILDING SECURITY LEVELS..... 22

6.5. FACILITY SECURITY LEVEL DETERMINATIONS FOR FEDERAL FACILITIES 23

6.6. SPECIAL REQUESTS 28

6.7. SECURITY CONTRACTOR SUITABILITY 28

6.8. GENERAL OFFICE REQUIREMENTS 29

6.9. FIRE DETECTION AND SUPPRESSION (SPRINKLER) SYSTEMS 31

6.10. SECURE BORDER INITIATIVE (SBI) 32

6.11. SECURITY SURVEY PROCESS 33

7. CHAPTER 7: EXTERIOR PROTECTION 35

7.1. GENERAL 36

7.2. PHYSICAL BARRIERS 36

7.3. FENCING..... 36

7.4. GATES 37

7.5. PROTECTIVE LIGHTING 38

7.6. DOORS 38

7.7. WINDOWS..... 38

7.8. MANHOLES, GRATES, AND STORM DRAINS..... 39

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

7.9. OPENINGS..... 39

7.10. SHAFTS, VENTS, AND DUCTS..... 40

7.11. FIRE ESCAPES AND BUILDING WALLS 40

7.12. FACILITIES IN REMOTE LOCATIONS 40

7.13. EXTERIOR SIGNAGE 40

7.14. OTHER SIGNS 41

7.15. LOADING DOCKS AND SERVICE ACCESS 42

8. CHAPTER 8: INTERIOR PROTECTION..... 43

8.1. INTERIOR CONTROLS 44

8.2. ACCESS CONTROL 44

8.3. VEHICLE 44

8.4. ROUTINE CONDITIONS 46

8.5. AREA DESIGNATIONS 46

8.6. SECURITY VAULTS (PERMANENT STORAGE OR MORE THAN 72 HOURS)..... 48

8.7. VAULT DOORS 49

8.8. STRONGROOMS 50

8.9. INTRUSION DETECTION SYSTEMS 50

8.10. HOLD ROOMS 50

8.11. PLANNING ALARM INSTALLATIONS 51

8.12. CLOSED CIRCUIT TELEVISION SYSTEMS 53

8.13. OPEN STORAGE CERTIFICATION PROCESS 54

9. CHAPTER 9: LOCKS AND KEYS..... 59

9.1. LOCKS 60

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

9.2. COMBINATION LOCKS..... 63

9.3. ELECTRONIC LOCKS 65

9.4. BIOMETRIC SYSTEMS 65

9.5. KEYS 65

10. CHAPTER 10: SAFES AND STORAGE EQUIPMENT 71

10.1. PHYSICAL PROTECTION AND STORAGE OF MATERIALS 72

10.2. REFERENCES 72

10.3. CLASSIFIED INFORMATION 72

10.4. SUPPLEMENTAL PROTECTION 74

10.5. GSA-APPROVED SECURITY CONTAINERS 75

10.6. WEAPONS STORAGE 75

10.7. RECORD SAFES DESIGNED FOR FIRE PROTECTION 77

10.8. COMBINATION LOCKS..... 77

10.9. REPLACEMENT OF UNAPPROVED STORAGE CONTAINERS 78

10.10. DEFECTIVE GSA-APPROVED SECURITY FILING CABINETS..... 78

10.11. MAINTAINING GSA-APPROVED SECURITY CONTAINERS..... 79

10.12. REPAIRING APPROVED SECURITY CONTAINERS..... 79

10.13. RECERTIFICATION OF GSA-APPROVED CONTAINERS 80

11. CHAPTER 11: ACCESS TO FACILITIES..... 83

11.1. GENERAL 84

11.2. DEFINITIONS 84

11.3. AUTHORITY 86

11.4. GENERAL 86

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

11.5. RESPONSIBILITIES 86

11.6. ACCESS CONTROL 88

11.7. GSA-OPERATED OR LEASED FACILITIES 90

11.8. NON-GSA OPERATED OR LEASED FACILITIES..... 91

11.9. PHOTO ACCESS CARDS (PAC) 91

11.10. VISITORS 92

11.11. ESCORTS 95

11.12. VISITOR PARKING..... 95

11.13. ELECTRONIC ACCESS CONTROLS 96

11.14. SCREENING PROCEDURES 97

11.15. PROHIBITED ENTRY NOTICE 99

11.16. PROHIBITED ITEMS 99

11.17. NATIONAL CAPITAL REGION DHS/CBP PHOTO ACCESS CARD (PAC) 100

11.18. SIGNAGE 101

11.19. PHOTOGRAPHY 101

11.20. SECURITY VIOLATIONS 102

11.21. OTHER 102

11.22. REFERENCE 102

12. CHAPTER 12: SERVICES 107

12.1. LAW ENFORCEMENT PROTECTION 108

12.2. CONTRACT GUARD SERVICES 108

12.3. COST FACTORS 110

BACK

12.4. GUARD DUTIES 111

12.5. PERSONNEL REQUIREMENTS 112

12.6. RESPONSIBILITIES BY FACILITY TYPE..... 114

12.7. FEDERAL PROTECTIVE SERVICES..... 116

12.8. OTHER LAW ENFORCEMENT..... 116

12.9. AUTHORITIES/REFERENCES..... 117

13. CHAPTER 13: PROGRAM DEVELOPMENT AND STRATEGIC PLANNING 119

13.1. GENERAL 120

13.2. STRATEGIC PLANNING..... 120

13.3. PROGRAM MANAGEMENT AND ADMINISTRATION..... 121

13.4. PERSONNEL DEVELOPMENT AND TRAINING 122

13.5. PHYSICAL SECURITY TRAINING 122

13.6. SECURITY AWARENESS, TRAINING AND EDUCATION (SATE) PLANS. 123

14. CHAPTER 14: INCIDENT RESPONSE AND THE HOMELAND SECURITY ADVISORY SYSTEM (HSAS) 125

14.1. GENEAL 126

14.2. INCIDENT RESPONSE..... 126

14.3. REPORTING PROCEDURE 127

14.4. INCIDENT REPORTING 128

14.5. EVENT REPORT COMPLETION 129

14.6. EMERGENCY PREPAREDNESS PROGRAM 129

14.7. EMERGENCY COMMUNICATIONS 131

BACK

14.8. WIRELESS PRIORITY SERVICE (WPS) 132

14.9. CBP EMPLOYEE EMERGENCY CHECK-IN PROCEDURES 133

14.10. EMERGENCY PLANNING AND RESPONSE 134

14.11. DEFINITIONS 135

14.12. PROCEDURES 136

14.13. RESPONSIBILITIES 138

14.14. BEST PRACTICES 139

14.15. PROTECTIVE MEASURES 140

14.16. AUTHORITIES/REFERENCES 147

15. CHAPTER 15: OCCUPANT EMERGENCY PLAN (OEP) 149

15.1. PURPOSE AND SCOPE 150

15.2. AUTHORITY/REFERENCES 151

15.3. RESPONSIBILITIES 151

16. CHAPTER 16: FIREARMS AND AMMUNITION 153

16.1. GENERAL 154

16.2. ASSIGNED FIREARMS 154

16.3. AUTHORITIES 154

17. CHAPTER 17: PROTECTION OF BUILDING DOCUMENTATION 155

17.1. GENERAL 156

17.2. DEFINITIONS 156

17.3. TYPES OF INFORMATION FOR DOCUMENT SECURITY 157

17.4. ELECTRONIC MEDIA 158

17.5. MARKING/LABELING OF INFORMATION 158

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

17.6. RESPONSIBLE CARE FOR DISSEMINATION OF SBU BUILDING INFORMATION 159

17.7. REPRODUCTION OF SBU INFORMATION..... 161

17.8. STORAGE..... 161

17.9. RECORD KEEPING 162

17.10. NOTICE OF DISPOSAL 163

17.11. ENFORCEMENT 163

17.12. TRAINING..... 163

18. CHAPTER 18: SECURE ITEMS 165

18.1. GENERAL 166

18.2. ACCESS 168

18.3. REQUISITION AND SHIPMENT 169

18.4. STORAGE..... 171

18.5. INVENTORY 173

18.6. DESTRUCTION..... 176

18.7. REPORTING REQUIREMENTS 177

19. CHAPTER 19: PROCEDURAL SECURITY 181

19.1. GENERAL 182

19.2. WORKPLACE SECURITY 182

19.3. RANDOM SECURITY AWARENESS MEASURES (RSAMs) 184

20. CHAPTER 20: WORKPLACE VIOLENCE 187

20.1. GENERAL 188

20.2. SECURITY PLANNING 189

BACK

20.3. SECURITY ASSISTANCE 190

20.4. PHYSICAL SECURITY MEASURES..... 191

20.5. SAMPLE PLAN..... 193

20.6. FEDERAL PROTECTIVE SERVICE INFORMATION..... 193

20.7. FPS CONTACT INFORMATION 194

21. CHAPTER 21: OFFICE AND LABORATORY EQUIPMENT 195

21.1. GENERAL 196

21.2. THREAT DETERMINATION 196

21.3. SPECIAL SECURITY CONSIDERATIONS 197

21.4. KENNEL (K-9) FACILITIES 197

21.5. CUSTOMS AND BORDER PROTECTION LABORATORY (CBPL) 197

22. CHAPTER 22: MAINTENANCE..... 199

22.1. GENERAL 200

22.2. SCOPE 200

22.3. CORRECTIVE MAINTENANCE 200

22.4. PREVENTIVE MAINTENANCE (PM)..... 200

22.5. MAINTENANCE PERSONNEL ACCESS AUTHORIZATION 201

22.6. RECORD KEEPING..... 201

23. APPENDIX 6.3: CBP MINIMUM STANDARDS 203

24. APPENDIX 6.10: SECURE BORDER INITIATIVE..... 233

25. APPENDIX 7.2: PERIMETER SECURITY BARRIERS 245

26. APPENDIX 7.3: FENCING 255

BACK

27. APPENDIX 7.5: PROTECTIVE LIGHTING 293

28. APPENDIX 7.6: DOORS AND DOOR HARDWARE 311

29. APPENDIX 7.7: WINDOWS..... 351

30. APPENDIX 7.8: OPENINGS 393

31. APPENDIX 7.15: LOADING DOCKS AND SERVICE ACCESS 417

32. APPENDIX 8.6: VAULTS 429

33. APPENDIX 8.8: STRONGROOMS 449

34. APPENDIX 8.9: INTRUSION DETECTION SYSTEMS 459

35. APPENDIX 8.10: HOLD ROOMS 491

36. APPENDIX 8.12: CLOSED CIRCUIT TELEVISION (CCTV) 509

37. APPENDIX 10: STORAGE OF WEAPONS AND
AMMUNITION (ARMORY) 545

38. APPENDIX 11.14: SCREENING PROCEDURES 565

39. APPENDIX 14: BUILDING-SPECIFIC SECURITY ALERT PLAN 587

40. OCCUPANT EMERGENCY PLANS: GUIDE 597

41. OCCUPANT EMERGENCY PLAN TEMPLATE 661

42. APPENDIX 20.5: WORKPLACE VIOLENT BEHAVIOR
PREVENTION PLAN (SAMPLE) 693

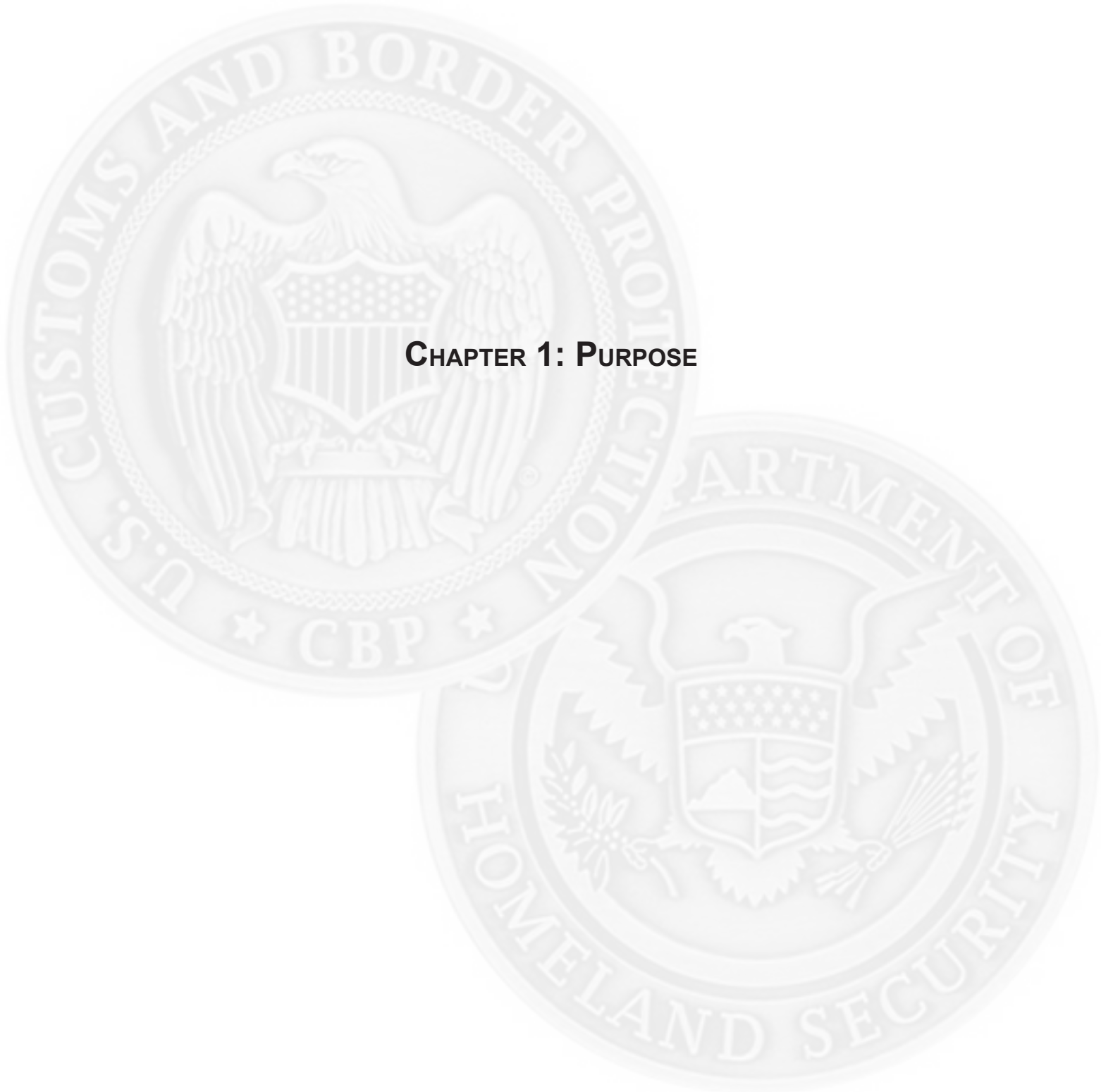
43. APPENDIX: SMD/FIELD SECURITY
OPERATIONS BRANCH (FUTURE) 705

44. APPENDIX: GLOSSARY..... 711

45. ADDITIONAL CBP SECURITY LINKS 729

REVISION HISTORY

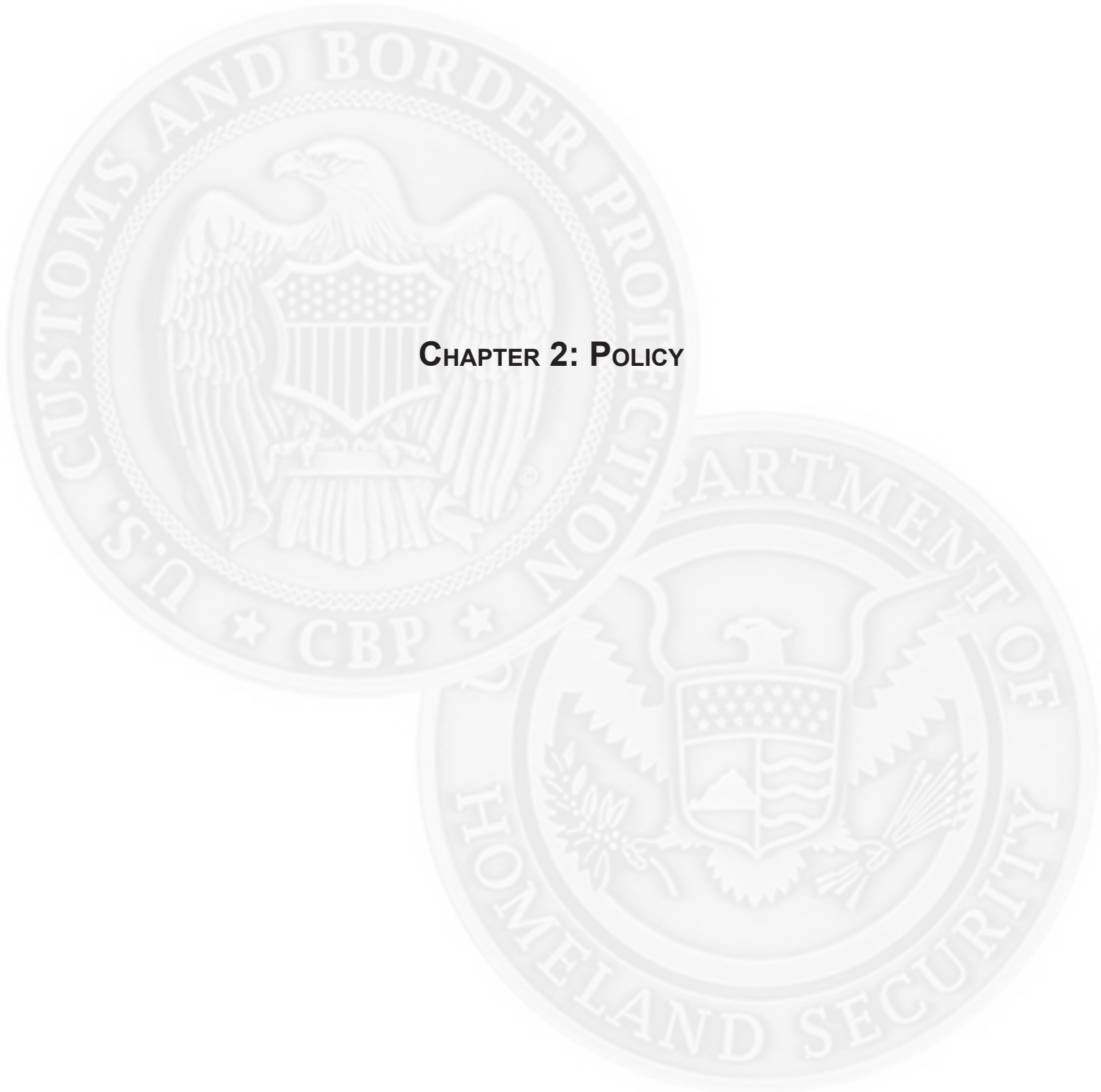
Version	Date	Description
1.0		Original release for review



CHAPTER 1: PURPOSE

1.1. PURPOSE

- 1.1.1. U.S. Customs and Border Protection (CBP) Internal Affairs, Security Management Division is responsible for providing operating policies, procedures, and practices for the physical protection of personnel, infrastructures, and assets from deliberate or unforeseen threats.
- 1.1.2. These standards shall be applied to all CBP facilities, owned, leased or occupied space. Compliance is mandatory for all new construction, renovation, and relocation projects. Existing CBP facilities are not required to be upgraded unless risk assessment determines otherwise.
- 1.1.3. These standards shall be used by the Office of Internal Affairs, Security Management Division (SMD) to serve as a guide for: Conducting security surveys for the development of threat assessments; evaluating security conditions during real estate market surveys and using the requirements guide for architectural and engineering (A&E) design efforts. Nothing in this policy handbook shall be construed as contrary to the provisions of any statute or other Federal regulation. In the event of conflict, specific statutory provisions shall apply.
- 1.1.4. Physical Security Programs shall be administered within each Region, District, and field activity based on the policy set forth in this handbook to ensure the protection of CBP assets. These programs shall be continually and effectively administered and monitored to ensure their integrity. At a minimum, a Physical Security Program shall include those items outlined in [Chapter 2.1: Policy](#).



CHAPTER 2: POLICY

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

2.1. POLICY

- 2.1.1. It is CBP policy that personnel, facilities, property, information and other agency assets shall be provided a consistent minimum level of protection. The minimum physical security standards provided in this Physical Security Handbook ensure a safe and secure work environment that contributes to the successful accomplishment of CBP's mission to secure the U.S. border against persons or agents of ill will and from dangerous or illegal goods. This policy includes, but is not limited to:
- Development of minimum physical security standards for CBP facilities, by identifying requirements for all physical security systems, devices, and building features. These requirements are to be applied to new construction, renovation, and relocation projects, as well as projects involving security enhancements;
 - Conduct of periodic surveys, inspections, and other formal on-site threat and vulnerability assessments; and
 - Participation in security projects managed by Headquarters and field offices. This includes evaluating CBP compliance with federal government regulations and standards for physical security requirements.
- 2.1.2. All new construction, relocation, and renovation projects must be coordinated through CBP Internal Affairs, Security Management Division, to ensure compliance with applicable regulations and policy.
- 2.1.3. Proposed Changes or Revisions. This handbook is intended to be a living document. As such, users of this policy handbook are encouraged to submit recommended changes and comments to SMD ([Policy and Procedures Handbook Comment form](#)). Comments shall reference the specific chapter and paragraph, and shall include a justification for the proposed change. Periodic revisions to this handbook will be published as necessary and to the extent practicable.
- 2.1.4. Protection Criteria. The Federal Protective Services (FPS) and CBP/IA/SMD determine the level of normal protective service on a case by-case basis. The facility's location, size, number of occupants and configuration; history of criminal or disruptive incidents in the surrounding area-not primarily directed toward the occupant agency's mission-the extent of exterior lighting, presence of physical barriers or other factors may be deemed pertinent and will be taken into consideration in the assessment.
- 2.1.5. Physical Protection. FPS provides normal and special protection through mobile patrol or fixed posts manned by contractually engaged uniformed personnel; security systems and devices; locking building entrances and gates during other than normal hours; cooperation of local law enforcement agencies; and a combination of these physical safeguards, depending upon the facility and the degree of risk defined. The degree of normal and special protection is determined by completion of a FPS physical security assessment or crime prevention assessment and implementation of CBP/IA/SMD minimum standards contained in this policy handbook.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- 2.1.6. Crime Prevention. The FPS collects and disseminates information about criminal activity on or against property under the charge and control of GSA, and provides crime prevention awareness training to occupant agencies upon request.
- 2.1.7. Facility Protection. In facilities where GSA has delegated protection authority to the agency or prime tenant, virtually all protection responsibilities are transferred to the agency, including acquisition, installation, and maintenance of physical security equipment and systems, and procurement and management of any guard contracts. In cases such as this, CBP/IA/SMD remains the approving authority for all security-related equipment and standards. CBP will not procure guard contracts on its own and will continue to procure guard services through FPS on a reimbursable basis. Normally, GSA/FPS will retain responsibility for mobile patrols, monitoring of alarms, response to incidents, request for criminal investigations, fire and facility safety and health inspections. GSA/FPS will provide such services at no charge to the agency beyond the Basic Security Charge, which is included in the rent.
- 2.1.8. Design Factors. It is imperative that security systems and procedures are considered from the start of the design phase so that conduit runs and alarm wiring, structural requirements, reinforcing devices and other necessary construction requirements are provided in the original plans.

2.2. POLICY EXCEPTION REQUIREMENTS

- 2.2.1. General. Only in rare situations where compelling operational requirements or conditions necessitate deviation from the specific minimum requirements in this handbook, the CBP Office shall:
- Request in writing any necessary exceptions from the requirements in this handbook prior to approval of the design concept;
 - Submit a waiver request which shall document all security vulnerabilities that could arise if the waiver is granted;
 - Submit a waiver request which shall provide, if possible, a mitigation plan that states what measures will be taken to minimize security vulnerabilities if a waiver is granted. Document how the proposed mitigation plan reduces risk to an acceptable level when compared to operational requirements; include persuasive evidence that the security of Federal employees and facilities will not be compromised by a less-than-standard facility;
 - Include justification, risk analysis, cost comparisons, criteria applied, and other pertinent data. Lack of funds or cost savings do not justify an exception. Exceptions are granted on a case-by-case basis and are not automatically extended to cases which appear to have similar circumstances; and
 - Submit exception requests directly to the Director for Security Management Division through CBPSPHCOMMENTS@cbp.dhs.gov.
- 2.2.2. Exceptions that are approved will be for fixed term, unless specifically noted all exceptions will be granted for one fiscal year. At the close of term of the exception the CBP office requesting the exception will be required to submit a new waiver request.

[RETURN TO TOP](#)





CHAPTER 3: BACKGROUND

3.1. BACKGROUND

- 3.1.1. Perimeter Security. Perimeter security standards pertain to the areas outside government control. Depending on the facility type, the perimeter may include sidewalks, parking lots, outside walls of the building, a hallway, or an office door. The elements of perimeter security are: parking, closed circuit television monitoring, lighting, and physical barriers.
- 3.1.2. Entry Security. Entry security standards refer to security issues related to the entry of persons and packages into a facility. The elements of entry security are: receiving/shipping, access control, and entrances/exits.
- 3.1.3. Interior Security. Interior security standards refer to security issues associated with prevention of criminal or terrorist activity within the facility. This area concerns secondary levels of control after people or things have entered the facility. The long-term elements of interior security are employee/visitor identification, utilities, occupant emergency plans, and day care centers.
- 3.1.4. Security Planning. Security planning is the development of long-term plans that incorporate requirements, standards, procedures, and processes to implement preventive and responsive countermeasures in the event of a breach of facility security.
- 3.1.5. Security planning also sets security standards addressing broader issues with implications beyond security at a particular facility. The elements of security planning are: intelligence sharing, security awareness training, tenant assignment, administrative procedures, and construction/renovation.
- 3.1.6. A comprehensive security system provides protection against a defined set of threats by informing the user of attempted intrusions and providing resistance to the would-be intruder's attack paths. This resistance must be consistent around the entire perimeter of the protected area.
- 3.1.7. There are four main security elements that must be properly integrated to achieve a proper balance of physical security. These are:
- Detection. This is the process of detecting and locating intruders as far from the protected areas as feasible. Early detection gives the user more time for effective alarm assessment and execution of pre-planned response;
 - Assessment. Assessment is determining the cause of the alarm or recognizing the activity. This must be done as soon as possible after detection to prevent the intruder's position from being lost;
 - Delay. Intruders must be delayed long enough to prevent them from achieving their objectives before the response force can interdict them; and
 - Response. A response force must be available, equipped, and trained to prevent the intruders from achieving their objective. The response time must be less than the delay time if the response force is to intercept the intruders before they achieve their objective.



CHAPTER 4: AUTHORITIES AND REFERENCES

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

4.1. EXECUTIVE ORDERS

- [EO 10450](#), Security Requirements for Government Employment, dated 23 Apr. 1953
- [EO 12196](#), Occupational safety and health programs for Federal employees, dated 26 Feb. 1980
- [EO 12333](#), United States Intelligence Activities, dated 4 Dec. 1981
- [EO 13355](#), Strengthened Management of the Intelligence Community, dated 27 Aug. 2004
- [EO 12656](#), Assignment of Emergency Preparedness Responsibilities, dated 18 Nov. 1988
- [EO 12829](#), National Industrial Security Program, dated 6 Jan. 1993
- [EO 12885](#), Amendment to EO 12829, dated 14 Dec. 1993
- [EO 12958](#), Classified National Security Information, dated 20 Apr. 1995
- [EO 12968](#), Access to Classified Information, dated 7 Aug. 1995
- [EO 12977](#), Interagency Security Committee, dated 19 Oct. 1995
- [EO 13228](#), Establishing the Office of Homeland Security and the Homeland Security Council, dated 8 Oct. 2001
- [EO 13284](#), Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security, dated 23 Jan. 2003
- [EO 13286](#), Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security, dated 5 Mar. 2003

4.2. CODE OF FEDERAL REGULATIONS/FEDERAL ACQUISITION REGULATION (FAR)

- [Homeland Security Acquisitions Manual, §3004.470-2, December 2006.](#)
- [41 CFR §102-74](#), Facility Management, dated 1 Jul. 2007
- [48 CFR §1](#), Federal Acquisition Management Systems, March 2005.

4.3. PUBLIC LAW

- [PL 91-596](#), Occupational Safety and Health Act of 1970
- [PL 107-296](#), Homeland Security Act of 2002

4.4. DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVES

- [DCID 6/1](#), Security Policy for Sensitive Compartmented Information, dated 1 Mar. 1995
- [DCID 6/3](#), Protecting Sensitive Compartmented Information within Information Systems, and Appendices, dated 24 May 2000
- [DCID 6/4](#), Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information, dated 2 Jul. 1998
- [DCID 6/7](#), Intelligence Disclosure Policy, dated 20 Apr. 2001
- [DCID 6/9](#), Physical Security Standards for Sensitive Compartmented Information Facilities, dated 18 Nov. 2002

4.5. DEPARTMENT OF HOMELAND SECURITY MANAGEMENT DIRECTIVES

- [DHS MD 0565](#), Personal Property, dated 10 Dec. 2004
- [DHS MD 11000](#), Office of Security, dated 8 Sep. 2006
- [DHS MD 11005](#), Suspend Access to DHS Facilities, Sensitive Information and IT Systems, dated 23 Mar. 2006

[DHS MD 11030.1](#), Physical Protection of Facilities and Real Property, dated 21 Apr. 2003

[DHS MD 11045](#), Protection of Classified National Security Information: Accountability, Control, And Storage, dated 4 Oct. 2004

[DHS MD 11046](#), Open Storage Area Standards for Collateral Classified Information, dated 22 Feb. 2005

[DHS MD 11047](#), Protection of Classified National Security Information Transmission & Transportation, dated 3 Jun. 2005

[DHS MD 11056.1](#), Sensitive Security Information (SSI), dated 3 Nov. 2006

[DHS MD 11080](#), Security Line of Business Integration and Management, dated 3 Jan. 2006

4.6. DEPARTMENT OF HOMELAND SECURITY DELEGATIONS

[DHS Delegation 7035.2](#), Delegation of the Chair of the Interagency Security Committee to the Assistant Secretary of Infrastructure Protection, dated 15 Aug. 2007

[DHS Delegation 8001](#), Delegation to the Chief, Office of Security, for Security Clearances of DHS Personnel, dated 28 Feb. 2003

[DHS Delegation 8100.3](#), Delegation of Original Classification Authority, dated 2 Jun. 2006

[DHS Delegation 8150](#), Delegation to Chief, Office of Security, of Determination Authority and Cognizant Security Authority, dated 17 Jun. 2003

[DHS Delegation 12000](#), Delegation to Designate Officers and Agents, dated 14 Dec. 2005

[DHS Delegation 12002](#), Delegation to Designate Officers and Agents on Behalf of Mount Weather Police Department, dated 26 Jun. 2006

4.7. CUSTOMS AND BORDER PROTECTION DIRECTIVES

[CBP Directive 3290-010B](#), Physical Security Standard for Customs and Border Protection Laboratories, dated Feb. 2008

[CBP Directive 5230-032](#), Personal Property Management, dated 1 Jun. 2005

4.8. CUSTOMS AND BORDER PROTECTION HANDBOOKS

[CBP HB 5200-13B](#), Personal Property Management Handbook, dated Nov. 2005

4.9. LEGACY

Immigration and Naturalization Service, Security Officer's Handbook, dated Mar. 1997

[Immigration and Naturalization Service](#), Personal Property Operations Handbook

[CIS HB 1400-02A](#), U.S. Customs Service, Physical Security Handbook, dated Apr. 2000

[CIS HB 4400-01A](#), U.S. Customs Service, Seized Asset Management and Enforcement Procedures Handbook, dated Jan. 2002

[CIS HB 3200-07A](#), U.S. Customs Service, Canine Enforcement Program Handbook, dated Aug. 2002

4.10. INTERAGENCY SECURITY COMMITTEE STANDARDS

ISC Standard, Facility Security Level Determinations for Federal Facilities

ISC Standard, Security Design Criteria for New Federal Office Buildings and Major

[RETURN TO TOP](#)

Modernization Projects

[ISC Standard](#), Security Standards for Leased Spaces

4.11. UNIFIED FACILITIES CRITERIA

[UFC 4-010-01](#), DoD Minimum Antiterrorism Standards for Buildings, dated 8 Oct. 2003

[UFC 4-010-02](#), DoD Minimum Antiterrorism Standoff Distances for Buildings, dated 8 Oct. 2003

[UFC 4-022-01](#), Security Engineering: Entry Control Facilities / Access Control Points, dated 25 May 2005

4.12. UNIFIED FACILITIES GUIDE SPECIFICATIONS

[UFGS-08 11 13](#), Steel Doors and Frames, dated Jul. 2006

[UFGS-08 14 00](#), Wood Doors, dated Jul. 2006

[UFGS-08 33 23](#), Overhead Coiling Doors, dated Jul. 2007

[UFGS-08 34 59](#), Security Vault Door, dated Apr. 2006

[UFGS-08 71 00](#), Door Hardware, dated Oct. 2007

[UFGS-28 16 00.00 20](#), Basic Intrusion Detection Systems (IDS), dated Apr. 2006

[UFGS-28 23 23.00 10](#), Closed Circuit Television Systems, dated Apr. 2006

[UFGS-32 31 13.53](#), High-Security Chain Link Fences and Gates, dated Apr. 2008

4.13. FEDERAL AND MILITARY SPECIFICATIONS AND STANDARDS

[AA-D-600D](#), Door, Vault, Security (with Amendment 1), dated 15 May 2000

[FF-L-2740A](#), Locks, Combination (with Amendment 1), dated 12 Jan. 1997

4.14. DEPARTMENT OF JUSTICE

[Vulnerability Assessment of Federal Facilities](#), dated 28 Jun. 1995

4.15. DEPARTMENT OF DEFENSE

[DoDI 2000.16](#), DoD Antiterrorism (AT) Standards, dated 2 Oct. 2006

[DoDI 5200.08](#), Security of DoD Installations and Resources, dated 10 Dec. 2005

[DoD 5200.08-R](#), Physical Security Program, dated 9 Apr. 2007

[DoD 5220.22-M](#), National Industry Security Program Operating Manual (NISPOM), dated 28 Feb. 2006

[DoD 5220.22-M-Sup 1](#), National Industry Security Program Operating Manual Supplement, dated Feb. 1995

[MIL-HDBK-1013/1A](#), Design Guidelines for Physical Security of Facilities, dated 15 Dec. 1993

[MIL-HDBK-1013/10](#), Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities, dated 14 May 1993

[MIL-HDBK-1013/14](#), Selection and Application of Vehicle Barriers, dated 1 Feb. 1999

4.16. GENERAL SERVICES ADMINISTRATION

[PBS-P100](#), Facilities Standards for the Public Buildings Service, dated Mar. 2005

4.17. OFFICE OF PERSONNEL MANAGEMENT

[Dealing With Workplace Violence, a Guide for Agency Planners Handbook](#), dated Feb. 1998

[Back](#)

[RETURN TO TABLE OF CONTENTS](#)

4.18. NATIONAL FIRE PROTECTION ASSOCIATION

[NFPA 101](#), Life Safety Code, dated 2006



[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.





CHAPTER 5: RESPONSIBILITIES

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

5.1. COMPONENT HEAD

5.1.1. The Component Head, defined as the highest-ranking individual within each Component, is the Commissioner of CBP. The Component Head, in addition to other duties, is responsible for ensuring that security management duties, as defined in [DHS MD 11080](#), are carried out effectively and efficiently.

5.2. CBP COMPONENT CHIEF SECURITY OFFICER

5.2.1. The Assistant Commissioner (AC) of the Office of Internal Affairs is the designated CBP Chief Security Officer. The AC oversees a wide range of investigative and security related functions including applicant and employee background investigations, clearances, employee misconduct investigations, INFOSEC, OPSEC, Physical Security, Industrial Security and management inspections.

5.3. ASSOCIATE CHIEF SECURITY OFFICER

5.3.1. The Director for CBP Office of Internal Affairs, Security Management Division (CBP/IA/SMD), exercises the general authority delegated by the Assistant Commissioner for the Office of Internal Affairs. Under the general supervision of the Assistant Commissioner for Internal Affairs, the Director of CBP/IA/SMD, as the Associate Chief Security Officer, has been appointed to discharge these responsibilities.

5.4. PHYSICAL SECURITY BRANCH (PSB) CHIEF

5.4.1. The Physical Security Branch (PSB) Chief provides complete, effective, security management oversight, policy formulation, and compliance and quality assurance for the physical security program to include the protection of facilities/sites, property assets to include mission-essential infrastructures, and personnel.

5.5. FIELD SECURITY OPERATIONS BRANCH (FSOB) CHIEF

5.5.1. The Field Security Operations Branch (FSOB) Chief is responsible for ensuring that national security programs are implemented, assigning adequate resources to implement and maintain security programs, designating Regional Security Officers (RSO) and other appropriately cleared security officials to discharge these responsibilities.

5.6. REGIONAL SECURITY OFFICERS (RSOs)

5.6.1. The Regional Security Officers (RSOs) are responsible for ensuring that security programs are carried out within their respective regions, assigning adequate resources to implement and maintain security programs, and designating a RSO alternate, and other appropriately cleared security officials to discharge these responsibilities.

5.7. DISTRICT SECURITY OFFICERS (DSOs)

5.7.1. The District Security Officers (DSOs) are responsible for coordinating compliance with CBP security programs through the RSO and serve as the primary point of contact for all security issues within their districts.

[RETURN TO TOP](#)

5.8. DESIGNATION OF SECURITY OFFICERS AND OFFICIALS

- 5.8.1. The responsible manager shall designate security officers and officials as required or deemed appropriate. Each designation shall be in writing and a copy of the designation provided to the RSO. The RSO shall include the names of individuals designated as Security Liaisons (SLs) in the report of key security personnel which is provided annually to the CBP Office of Internal Affairs, Security Management Division.

5.9. PHYSICAL SECURITY SPECIALISTS (PSSs)

- 5.9.1. Physical Security Specialists (PSSs). Personnel designated as PSSs are responsible for familiarizing themselves with the applicable portions of this policy handbook and the Federal, departmental, and CBP security directives referenced herein, and for knowledgeably administering the security programs relevant to their respective mission. Unless the specific organizational security officer designation is used, the term security officer as used in this policy handbook shall apply to all organizational security officers.
- 5.9.2. Personnel Security Officers (PSOs) are responsible for the suitability portion of the personnel security system that encompasses the risk designation program, the assignment of public trust position designations, initiating required entry background investigations, and adjudicating suitability as delegated by the Office of Personnel Management (OPM).
- 5.9.3. Security Liaisons (SLs) are responsible for coordinating compliance with the implementation of CBP security programs through the DSO/RSO and serve as the primary point of contact for all security issues within their facilities.
- 5.9.4. Qualifications. Only qualified individuals with sufficient grade and experience, capable of performing the applicable duties set forth in this policy handbook, shall be appointed as security Liaisons.
- 5.9.5. Security Clearance. Security Liaisons shall, at a minimum, possess a national security clearance commensurate with that required for the highest national security program relevant to their respective activity.
- 5.9.6. Training. For basic training, security Liaisons shall review and familiarize themselves with the contents of this policy handbook and the applicable Federal, departmental, and CBP security regulations referenced in this handbook. At the discretion of the responsible manager, security Liaisons may attend training courses on a variety of security subjects offered by a number of different agencies.

5.10. IA/PSD PERSONNEL SECURITY OFFICERS

- 5.10.1. [IA/PSD Personnel Security Officers](#), when designated, are responsible for coordinating compliance with the implementation of all position-risk and -sensitive position programs, which includes ensuring that the required background investigations for sensitive positions are conducted. See the [Personnel Security Handbook](#) for more detailed information.

5.11. IA/SMD INFORMATION SECURITY OFFICERS

- 5.11.1. IA/SMD Information Security Officers, when designated, are responsible for coordinating compliance with all regulations for safeguarding national security information, proprietary information, sensitive information, or Privacy Act records.
- 5.11.2. Top Secret Control Officer (TSCO). The TSCO receives, dispatches, and maintains an accountability register of Top Secret material in an approved Top Secret control center.

5.12. CLASSIFIED DOCUMENT CUSTODIAN, CLASSIFIED CONTROL STATION

- 5.12.1. The Classified Document Custodian of a Classified Control Station receives, dispatches, and maintains an accountability register of Secret and Confidential material in an approved classified control station.

5.13. DERIVATIVE CLASSIFIERS

- 5.13.1. The Agency Security Manager specifically designates employees who originate the production or generation of classified information as Derivative Classifiers.

5.14. DESIGNATED OFFICIAL (DO)

- 5.14.1. Designated Official (DO). The highest ranking official of the primary tenant agency of a Federal facility or, alternatively, a designee selected by mutual agreement of tenant agency officials. For facilities owned and leased by the U.S. General Services Administration (GSA), the definition that appears in [41 CFR § 102-71.20](#) of the Code of Federal Regulations protects personnel and property in the event of emergencies such as fire, bomb threats, civil disturbances and natural disasters. The DO (as defined in [41 CFR § 102-71.20](#)) is responsible for developing, implementing and maintaining an Occupant Emergency Plan (OEP). For further detail on the OEP, see [Chapter 15, Occupant Emergency Plan](#).

5.15. ASSESSMENTS

- 5.15.1. The assessment will be used by the DO of the facility, in conjunction with CBP/IA/SMD, to determine the type and extent of security countermeasures. (A link to the Physical Security Project Prioritization Tool will be established when that item is made available.)



CHAPTER 6: FACILITY PROTECTION

6.1. GENERAL

- 6.1.1. The degree of facility protection shall be determined by the Regional or District Security Officer based on the results of a comprehensive security assessment of the facility.
- 6.1.2. Perimeter protection is the first line of defense in providing physical security for personnel, property, and information at a facility.
- 6.1.3. The second line of defense, and perhaps the most important, is interior controls.
- 6.1.4. The cost of security controls above these minimum standards normally shall not exceed the monetary value of the item or areas to be protected, unless necessitated through an assessment.

6.2. PLANNING FACILITY PROTECTION

- 6.2.1. The objective of planning facility protection is to ensure the integrity of operations and the security of assets. Security planning must be an integral part of selecting, designing, constructing, reconfiguring, or moving into a CBP facility.
- 6.2.2. The modification of a facility or addition of security measures after occupying a facility can be costly and impractical. Therefore, the responsible Project Manager and Designated Official (DO), as defined in the Federal Property Management Regulation (FPMR), will coordinate from the outset, on any addition, alteration, or new construction with CBP/IA/SMD. The coordination shall begin with the funding and concept phase, including the designers and architects and continue through the contracting process, actual construction, installation, and acceptance.
- 6.2.3. When CBP occupies General Services Administration (GSA)-leased facilities, it is imperative that the CBP/IA/SMD Security Specialist and the Security Liaison (SL) establish a working relationship with the GSA and local law enforcement officials. The SL is required to participate and maintain an active role as a member of the Building Security Committee (BSC).
- 6.2.4. Facility Protection in CBP-owned or leased Facilities. For buildings and grounds owned or leased by the CBP, the DO having jurisdiction over the real property is responsible for implementing additional security measures above the minimum standards. The degree of protection to be provided for the space will be determined by the physical security assessment conducted by CBP/IA/SMD. The assessment will evaluate the security of that specific facility, taking into consideration the facility's location, size and configuration, history of criminal activity or disruptive incidents, extent of exterior lighting, presence of physical barriers, and other factors that may be deemed pertinent.
- 6.2.5. Facility Protection in GSA-Owned or Leased Facilities. For building and grounds for which GSA has space assignment responsibility, GSA is responsible for furnishing standard protection not less than the degree of protection provided by commercial building operators of similar space for normal risk occupants. The degree of protection is determined by a Federal Protective Service (FPS) physical security

assessment and the minimum security standards contained in this policy handbook. This protection may include guards, access control, intrusion detection (alarms), closed circuit television surveillance (CCTV), inspection of packages, etc., when the FPS assessment determines that the security countermeasures are warranted for general Government occupancy and not necessitated by special activities or specific agencies. Special protection required due to the nature of the business conducted within the space or unusual public reaction to an agency's program and missions (whether or not of a continuing nature) is determined jointly by the FPS, CBP/IA/SMD, and the occupant agency or agencies and is provided on a reimbursable basis.

- 6.2.6. Protection Criteria. The FPS and CBP/IA/SMD determine the level of normal protective service on a case by-case basis. The facility's location, size, number of occupants and configuration, history of criminal or disruptive incidents in the surrounding area, even those not primarily directed toward the occupant agency's mission; the extent of exterior lighting, presence of physical barriers or other factors may be deemed pertinent and will be taken into consideration.
- 6.2.7. Physical Protection. FPS provides normal and special protection through mobile patrol or fixed posts manned by contractually engaged uniformed personnel; security systems and devices; locking building entrances and gates during other than normal hours; cooperation of local law enforcement agencies; or a combination of these, depending upon the facility and the degree of risk involved. The degree of normal and special protection is determined by completion of a FPS physical security assessment, crime prevention assessment, and CBP/IA/SMD minimum standards outlined in this handbook.
- 6.2.8. Crime Prevention. The FPS collects and disseminates information about criminal activity on or against property under the charge and control of GSA, and provides crime prevention awareness training to occupant agencies upon request.
- 6.2.9. Facility Protection. In facilities where GSA has delegated protection authority to the agency or prime tenant, virtually all protection responsibilities are transferred to the agency, including acquisition, installation, and maintenance of physical security equipment and systems, and procurement and management of any guard contracts. In cases such as this, CBP/IA/SMD remains the approving authority for all security-related equipment and standards. CBP will not procure guard contracts on its own and will continue to procure guard services through FPS on a reimbursable basis. Normally, GSA/FPS will retain responsibility for mobile patrols, monitoring of alarms, response to incidents, request for criminal investigations, fire and facility safety and health inspections. GSA/FPS will provide such services at no charge to the agency beyond the Basic Security Charge, which is included in the rent.
- 6.2.10. Design Factors. It is imperative that security systems and procedures are considered from the start of the design phase so that conduit runs and alarm wiring, structural requirements, reinforcing devices, and other necessary construction requirements are provided in the original plans.

6.3. DETERMINING BUILDING SECURITY LEVEL

6.3.1. CBP/IA/SMD has determined that all CBP facilities shall meet the Level III security requirements listed in the table below. A higher level of security may be assigned to a facility based on the risk assessment conducted.

6.3.2. Determine the building security level in accordance with the criteria and process used in determining the Facility Security Level (FSL) of a Federal facility. This categorization serves as the basis for implementing protective measures under other Interagency Security Committee (ISC) standards. Consistent with the authority contained in [Executive Order 12977](#), "Interagency Security Committee," dated October 19, 1995, this Standard is applicable to all buildings and facilities in the United States occupied by Federal employees for non-military activities. These include existing buildings; new construction; major modernizations; facilities owned, to be purchased, or leased; stand-alone facilities, Federal campuses; and, where appropriate, special-use facilities.

- Use the "Facility Security Level Determinations for Federal Facilities—An [Interagency Security Committee Standard](#)," 2007;

Federal holdings are divided into four out of the five security levels for this Physical Security Handbook, based primarily on staffing size, number of employees, use, and the need for public access.

- See [Appendix 6.3, CBP Minimum Standards](#), for detailed information on facility security levels.

6.4. BUILDING SECURITY LEVELS

FACTOR	I	II	III	IV	SCORE
Mission Criticality	LOW	MEDIUM	HIGH	VERY HIGH	
Symbolism	LOW	MEDIUM	HIGH	VERY HIGH	
Facility Population	<100	101-250	251-750	>750	
Facility Size	<10,000 sq. ft.	10,000-100,000 sq. ft.	100,000-250,000 sq.ft.	>250,000 sq.ft	
Threat to Tenant Agencies	LOW	MEDIUM	HIGH	VERY HIGH	
					Sum of above
Facility Security Level	I 5-7 Points	II 8-12 Points	III 13-17 Points	IV 18-20 Points	Preliminary FSL
Intangible Adjustment	Justification				+/- 1 FSL
					Final FSL

- Facility Security Level Determinations for Federal Facilities—[An Interagency Security Committee Standard](#) defines the criteria and process to be used in determining the Facility Security Level (FSL) of a Federal facility:
 - This categorization serves as the basis for implementing protective measures under other ISC standards. Consistent with the authority contained in Executive Order 12977, “Interagency Security Committee,” dated October 19, 1995, this Standard is applicable to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities. These include:
 - Existing buildings;
 - New construction, or major modernizations;
 - Facilities owned, to be purchased, or leased;
 - Stand-alone facilities;
 - Federal campuses;
 - Individual facilities on Federal campuses (where appropriate); and
 - Special-use facilities.

6.5. FACILITY SECURITY LEVEL DETERMINATIONS FOR FEDERAL FACILITIES

6.5.1. New Leases in Existing Buildings

- The appropriate security level for each lease requirement should be determined by a CBP/SMD Security Specialist (except in the case of GSA leases, whereby FPS/DHS shall make this determination in consultation with CBP/SMD, based on a risk assessment as an application of the recommendations set forth in the Department of Justice “Vulnerability Assessment of Federal Facilities” (DOJ study), dated June 28, 1995, the ISC Security Leasing Criteria, September 2004 and the new “Facility Security Level Determinations for Federal Facilities (FSL) An Interagency Security Committee Standard,” 2007:
 - Where CBP anticipates making a new lease in an existing building (including succeeding lease actions), all of the ISC Lease Security Standards (operating standards) listed for that security level must be met, with the exception of those requirements specifically prescribed under “New Construction - Blast/ Setback Standards;
 - The standards shall be considered minimum requirements; and it is the intent that offerors unwilling or unable to meet the requirements should be considered non-responsive. A distinction should be drawn between operating standards and new construction standards;
 - Operating standards pertain to the operational and perhaps out-source able nature of security, i.e., access control via guard service, CCTV monitoring, magnetometers, x-ray machines and HVAC security, to name a few. While the minimum operating standards must be met, existing

[RETURN TO TOP](#)

buildings are not required to meet the blast/setback standards required for new construction. CBP, at their own expense, may increase (but not decrease) the level of security required in the Lease

- Security standards. As an example, a recommended security Level III for an agency could be raised to a Level IV, at the agency's request; or perhaps only a specific, isolated standard could be added to the Level III requirement.

6.5.2. Lease Construction Projects

- When lease construction shall be sought (the SFO specifies a build-to-suit) to satisfy a requirement, the Lease Security Standards (operating standards) identified for the required security level shall be incorporated into lease construction Solicitation For Offers (SFOs);
- These projects shall incorporate the new construction-blast/setback standards specified in Section III for the specified security level as well as new construction design criteria contained in the "ISC Security Design Criteria", dated May 28, 2004, or latest version. In some cases, lease construction may be offered (although not specifically requested) in direct response to a solicitation for space (i.e., the Government mayor may not be the anchor tenant). In this situation, the proposal for new construction would be held to the higher standards than that of potentially competing existing buildings under the same solicitation; and
- The existing buildings shall be required to meet only the minimum lease security standards (operating standards only) and shall not be subject to the new construction-blast/setback requirements or the ISC Design Criteria.

6.5.3. Perimeter Security

- Security control is required over public areas and building entry points. This includes adjacent surface parking lots and structures under the building owner's control. Private tenancies shall be expected to comply. Security control means (generally) the right to inspect at point of entry and at any time present in the public space, the right to deny access and the right to remove vehicles from the premises;
- Security control is obtainable by any of 3 methods: lessor-furnished (turnkey), operating agreement (shared-responsibility), or full leasehold control (government-furnished) depending on how the owners propose. The Government shall retain the right to provide control at anytime during the lease term;
- Garage control does not require Government parkers, but may require Government garage management. Implementation of a vehicle pass/ID system for contract/monthly parkers, acceptable to the Government, is required. Signage is required to alert parking patrons to inspection and towing policies and removal of unauthorized vehicles;
- Adequate lighting, with emergency power backup, for the exterior of the building is required. Parking areas shall also be adequately lighted. 24-hour Closed Circuit Television (CCTV) surveillance cameras with time lapse video recording

[RETURN TO TOP](#)

is required at lobbies and parking areas or as otherwise deemed necessary by a Government Security Specialist;

- Applications of shatter-resistant material, acceptable to the Government, shall be applied on exterior windows in Government-occupied space;

NOTE: SHATTER-RESISTANT WINDOW PROTECTION REQUIREMENTS (as of November 2005) (BUILDING SHELL)

- The Lessor shall provide and install wet-glazed or mechanically attached, shatter-resistant material not less than 0.18 millimeters (7-mil) thick on all exterior windows in Government-occupied space. The offeror shall provide a description of the shatter-resistant window system in the attached Lessor Building Security Plan; and
- Alternatively, the Lessor shall provide certification from a licensed professional engineer that the window system conforms to a minimum glazing performance condition of 3B for a high protection level and a low hazard level. Window systems shall be certified as prescribed by WINGARD 4.1 or later or WINLAC 4.3 software to have satisfied the specified performance condition using the test methods provided in the US General Services Administration Standard Test Method for Glazing and Window Systems Subject to Dynamic Overpressure Loadings or ASTM F1642-04 Standard Test Method for Glazing and Glazing Systems Subject to air blast loadings.

6.5.4. Entry Security

- Security Guards for public lobbies and public entrances shall be required for such purposes as ID/pass control and manning x-ray and magnetometer equipment. Guards can be lessor-furnished or via operating agreement or full leasehold control methods. If guards are lessor furnished, they shall be trained and licensed in accordance with Federal Government standards consistent with the Federal Protective Service. Guards manning magnetometers and x-ray equipment shall be armed. For more information, refer to [Chapter 11: Access To Facilities](#);
- Magnetometers, manned by armed Security Guards, are required at public entrances as determined by the CBP/SMD Security Specialist. Guards shall direct the building population and visitors through the magnetometers. All government mail and packages entering the building shall be subject to x-ray screening and visual inspection by armed Security Guards. This includes packages and personal belongings of the building occupants and visitors, as well as shipments brought into a loading dock;
- The Government may divert large truck shipments to a secondary location for screening purposes. The Government reserves the right to negotiate security enhancements necessary for securing any unsecured non-federal block of space with a separate entrance (e.g., ground floor retail) based on a Government Building Security Assessment; and
- Intrusion Detection System (IDS) with central monitoring capability is required for the building perimeter. Internal IDS may be required as determined by a

Government Security Specialist. Exterior entrances shall have high security locks. Leases shall state that the Government reserves the right to post applicable Government rules and regulations at each public entrance in a Federally occupied facility for such things as, but not limited to, barring the unauthorized possession of firearms and dangerous weapons. For more information on IDS, refer to [Appendix 8.9 IDS](#).

6.5.5. Interior Security

- Acceptable government-issued (e.g. driver's license) photo ID for all building occupants upon entry to the building is required. A visitor control/screening system, acceptable to the Government, is required. At a minimum, the system shall require Security Guards to screen visitors but could result in a level of control that may require escorting them;
- Utility areas shall be secured and only authorized personnel shall have access. Emergency power sources to critical systems (alarm systems, radio communications, computer facilities, CCTV monitoring, fire detection, entry control devices, etc) are required;
- Specific protection measures shall be required to protect the building environment from airborne chemical, biological, or radiological attacks. Accessible fresh air intakes shall be relocated, extended or secured to prevent easy ground or roof access. Access to mechanical areas and building roofs shall be strictly controlled. Dedicated Heating, Ventilation and Air Conditioning (HVAC) shall be required for lobbies, centrally-operated mail rooms (specifically required by the government) and loading docks, to prevent widespread dispersion of a contaminant released in those areas;
- Procedures (should airborne hazards be suspected or found) are required for the notification of the lessor's building manager, building security guard desk, local emergency personnel, or other Government emergency personnel, for the possible shutdown of air handling units serving any possibly affected areas;
- Securing accessible return-air grilles is required. Protection measures shall not adversely affect the performance of the building HVAC system. Access to building information, including mechanical, electrical, vertical transport, fire and life safety, security system plans and schematics, computer automation systems, and emergency operations procedures shall be required. Such information shall be released to authorized personnel only. Names and locations of Government tenants shall not be disclosed within any publicly accessed document or record; and
- A fire alarm system, with voice communication, is required for emergency notification and instructions to building tenants, in the event of possible contamination of the HVAC system or other emergency.

6.5.6. Administrative Procedures

- Building managers and owners are required to cooperate with and participate in the development and implementation of Government Occupant Emergency Plans

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

(OEP). Conduct background security checks and/or establish security control procedures for contract service personnel as deemed necessary;

- The Government reserves the right, at its own expense and manpower, to temporarily upgrade security during heightened security conditions due to emergency situations such as terrorist attacks, natural disaster and civil unrest. The measures shall be in accordance with the latest version of the Homeland Security Advisory System.

6.5.7. New Construction/New Construction -Lease

- For any lease resulting in new construction (not existing buildings), in addition to the above Minimum Lease Security Standards, the Interagency Security Committee (ISC) Design Criteria, dated May 28, 2001 or latest version, shall also apply as well as the following blast/setback standards shall be met;

6.5.8. Blast/Setback Standards

- For non-law enforcement agencies (excluding childcare, but including the U.S. Courts), a 50 foot setback guideline with appropriate window glazing, as prescribed by WINGGARD 3.15 or later or WINLAC 4.3 software, to achieve a glazing performance condition of 3b and a facade protection level of “medium” given a blast load standard of 4 psi/28 psi-msec is required.
- For some law enforcement agencies, a 100 foot setback guideline with appropriate window glazing, as prescribed by WINGARD 3.15 or later or WINLAC 4.3 software, to achieve a glazing performance condition of 2 and a facade protection level of “higher” given a blast load standard of 10 psi/89 psi-msec is required. For more information on windows, refer to [Appendix 7.7 Windows](#);
- Setback refers to the distance from the face of the building’s exterior to the protected/defended perimeter (i.e., any potential point of explosion). This would mean the distance from the building to the curb or other boundary protected by bollards, planters or other street furniture. Such potential points of explosion may be, but no limited to, such areas that could be accessible by any motorized vehicle (i.e. street, alley, sidewalk, driveway, parking lot);
- Glazing Performance Condition 3b provides for a high protection level and a low hazard level. For a blast of 4psi/28psi-msec, the glazing cracks and fragments enter the space and land on the floor not further than 10ft. from the window;
- “Medium Level Protection” to the facade shall result in moderate damage, but repairable. The facility or protected space shall sustain a significant degree of damage, but the structure should be reusable. Some casualties may occur and assets may be damaged. Building elements other than major structural members may require replacement;
- Glazing Performance Condition 2 provides for a very high protection level and a hazard level of “none”. For a blast of 4psi/28psi-msec or 1 Opsi/89 psi-msec, the glazing cracks but is retained by the frame. Dusting or very small fragments near the sill or on the floor are acceptable; and

[RETURN TO TOP](#)

- “Higher Level Protection” to the facade shall result in minor damage, but repairable. The facility or protected space may globally sustain minor damage with some local significant damage possible. Occupants may incur some injury, and assets may receive minor damage.

6.6. SPECIAL REQUESTS

6.6.1. Building Permit

- The lessor shall provide a copy of the building permit to the U.S. Customs and Border Protection Office of Internal Affairs (IA), Security Management Division (SMD).

6.6.2. Blueprints, AutoCAD, Floor Plans, Time Requirements

- No later than 30 days after completion of the job, the contractor/lessor shall provide IA/SMD with all blueprints of the space and all associated areas (i.e. roof, garage) on AutoCAD and a hard copy of the floor plan;
- The security system shall be included in the blueprints after the initial floor design. The security system shall be on a separate layer. It shall not be included on the same layer of the electrical system. The security system shall be treated as sensitive information and shall not be given to any contractor who does not have a need to know. A hardcopy of as -built of the Security System along with the AutoCAD copy shall be provided to SMD no later than 30 days after the completion of the job. (This shall include any changes made during the construction phase).

Note: Security Plan shall include furniture layout.

6.6.3. Pre-Construction Meeting

- A pre-construction meeting is required by the Security Management Division. This meeting shall include representatives from GSA, FPS, Lessor, General Contractor (GC), and the CBP/Security Management Division. At this meeting, the GC shall provide a proposed project schedule for review and discussion. Based on this discussion, the GC shall submit the final detail project schedule before construction starts.

6.6.4. Security Requirements

- The CBP/Security Management Division requires one business week after the space has been totally built out (including carpet, painting, electrical, plumbing, HVAC, communication cable, and video cable, except for the installation of the ceiling tile) to complete our security and communication requirements. Once these tasks are completed, an inspection may be needed before the ceiling tiles are installed. After that, a final walk through shall take place by the SMD and GSA to prepare a punch list to present to the contractor/lessor. No security project shall be considered substantially complete.

6.7. SECURITY CONTRACTOR SUITABILITY

- Any contractors working on this project shall be required to complete and

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

submit background information prior to starting any CBP/IA project. Refer to the [Homeland Security Acquisitions Manual, §3004.470-2](#), which states that a contractor must complete a background investigation before work may commence.

6.8. GENERAL OFFICE REQUIREMENTS

6.8.1. Planning Office Security

- These general guidelines should be used in conjunction with the CBP Minimum Standards in [Appendix 6.3, CBP Minimum Standards](#).

6.8.2. Location of Office and Building Structure

- The physical location of the Internal Affairs Offices must meet the criteria within the guidelines of NEAP, FEMA, and OSHA safety regulations. In addition, the Building shall meet all Interagency Security Committee, Security Design Criteria's for New Federal Office Buildings, and Major Modernization/and or ISC leasing criteria projects.(i.e. HazMat, proximity to Industrial Facilities, pollutions- noise, air, water, secured parking, floodplains, known disaster areas);
- Due to the critical nature of the protective and investigative responsibilities of the U.S. Customs and Border Protection Office of Internal Affairs, the following must be considered prior to determining fixed site locations:
 - o Investigative Responsibilities (Prisoner Processing and Security, Evidence Storage, Classified Storage, File Storage, Surveillance, Vehicle Storage, Weapons & Munitions Storage);
 - o (See [Section 6.11](#) for the GSA ISC Guidelines).
- To reduce the vulnerabilities of window exposure to public areas, streets, and parking facilities, the exact location of the office within a commercial or federal facility, shall be determined by the Security Management Division Physical Security Specialist with Federal Protective Service and General Services Administration during market survey. The Building/Office must meet or exceed local Fire & Safety codes. A complete re-inspection should be conducted prior to the building being selected.

6.8.3. Location Within the Building

- The Internal Affairs Offices shall not be located on the ground floor of any building. Top floor locations shall be considered as an alternative to lower exposed areas. Space should be located on the third to seventh floors:
 - o The offices shall be located in contiguous space on one or more floors.;
 - o The Internal Affairs Offices shall not be located in window space that is adjacent to outside fire escapes, ledges, balconies, public parking, mezzanines, or directly above the loading dock area.

6.8.4. Building Security

- The building shall have a 24-hour security system;

- The CBP Offices personnel must have 24-hour unrestricted access to the office space and parking.

6.8.5. Parking

- Parking within adjacent parking garage is the optimum situation. These buildings shall be considered before other buildings that do not offer that alternative. A building which sits above a parking garage shall also be considered, depending upon access control to the parking garage and available secured storage of CBP vehicles;
- Special security requirements for the parking area for official vehicles shall depend on local conditions, which shall be evaluated before the market survey. If on site, or adjacent parking is available, parking shall be within a reasonable walking distance of approximately one block of the office building; and
- Protective and Investigative vehicles shall require secured parking implementations. The parking area, or drop off point, must be within close proximity to an elevator (preferably a service elevator) in order to expedite prisoner/detainee handling and processing.

6.8.6. HVAC

- A building that has an HVAC system, zoned floor to floor, or within a floor, and is energy efficient, shall be given priority over other buildings that do not have these capabilities;
- Buildings with HVAC systems that are turned off over weekends **MUST** have the capability to provide 24 hour heating/cooling when CBP personnel are working after hours, or on the weekends. Certain areas such as labs, communications equipment, security equipment, and Office of Internal Affairs technical equipment, and duty desk, etc., shall require 24-hour cooling. If needed, an additional independent HVAC system could be installed to provide mandatory 24-hour cooling to these areas.

6.8.7. Elevators

- A freight or public elevator that can be keyed off for exclusive use by CBP is desirable when transporting prisoners/detainees. The elevator shall go from the drop off point in the parking area to the floor on which processing is located;
- Access to both the freight elevator and loading dock must be made available to U.S. Customs and Border Protection personnel;
- All other elevators that open into Office of Internal Affairs space shall grant access only to the Visitor Waiting Lobby during normal working hours; and
- All other elevators that open into Office of Internal Affairs space require access control systems and devices.

6.8.8. Egress

- Every effort shall be made to design IA space so that the IA office has two ways of egress, a front door and a back door. Preferably, the doors shall not be located

near each other and shall open out into different hallways.

6.8.9. Emergency Signaling Devices

- Audio speakers shall not be installed inside private offices. Required speakers shall be installed in the Office of Internal Affairs hallway immediately outside the private offices. Required speakers shall be installed in the Office of Internal Affairs hallway immediately outside the private offices with the volume adjusted so that people inside these offices can hear the alarm;
- All other audio signaling devices, such as fire alarms, are subject to testing by CBP before they can be installed in the Office of Internal Affairs offices. No equipment found capable of passing speech components shall be accepted. Fire Alarm Strobe Lights located in Office of Internal Affairs areas are acceptable. All fire alarm equipment shall meet all current local, fire, and life safety codes;
- Emergency lighting shall be provided throughout the space. This can be achieved either through stand alone emergency lighting fixtures, or by having the building standard ceiling lights on an emergency lighting circuit that is supported by a standby generator; and
- Exit doors within our space need to be identified with illuminated exit signs that are powered by the emergency lighting system. If required, additional signs shall be placed throughout to direct employees to the exits from all interior corridors within the Office of Internal Affairs space.

6.8.10. Perimeter Doors

6.8.11. Perimeter doors must be constructed of 12-gauge steel clad, hollow core metal, 1¾-inches thick. Solid core wood doors are not authorized for use on the perimeter of a facility. Door frames must be constructed of hollow metal that is equal in strength to that of the door. For more information on Doors, refer to [Appendix 7.6 Doors and Door Hardware](#).

- Perimeter doors must be equipped with door stoppers and door closers. Double doors, glass doors, and doors with louvers are unacceptable, unless these doors open into the Waiting Room/Lobby from a public hallway. If doors must be installed so that the hinge pins are exposed in the unsecured area, then non-removable pins shall be installed. On out swinging doors, a steel astragal, which precludes access to the latch bolt and deadbolt, must be installed on the door. In addition to the public entry door, there shall be at least one more perimeter door in all Office of Internal Affairs offices;
- All perimeter doors shall be fitted with a Mortise lockset with deadbolt, which is ANSI F20 compliant, unless otherwise noted. Doors utilizing electronic access control devices shall use an electric Mortise lockset with power transfer hinge or electric strike with a rating of 1200 foot pounds, or as specified by CBP/SMD on a case by case basis. All exit doors must comply with local fire codes.
- For more information, see [Appendix 7.6. Doors and Door Hardware](#).

6.9. FIRE DETECTION AND SUPPRESSION (SPRINKLER) SYSTEMS

- The U.S. Customs and Border Protection require a fire detection system that provides 100% coverage of the controlled office area;
- All detection systems used must meet or exceed local and NFP A national fire detection codes. It is incumbent upon the contractor to ensure all doors, security devices and access control systems meet or exceed local and national NFPA fire codes;
- In some offices, the installation of a suppression system may be required. The use of a suppression system shall require modifications to the electrical and air handling systems. If this installation is necessary, it shall be identified when floor plans are prepared;
- Installation, maintenance, and service of the fire detection and suppression systems shall be the responsibility of building management; and
- All problems with the systems protecting Office of Internal Affairs space shall be reported to the appropriate agency supervisor.

6.9.1. Radio Communication Antennae and Base Stations(s)

- It may be necessary to install radio communication antennae on the roof of the building and radio communication base stations associated equipment in the elevator equipment area or similar type area near the roof;
- Coaxial cable(s) have to connect the antenna(s) to the base station(s). At a minimum, a dedicated 20 amps, 120 VAC, duplex outlet shall be required for power to each base station installed and telephone keying lines for remotely controlling the base station(s). A building ground shall also be provided for the radio base station(s). Every effort should be made to restrict access and secure base stations.

6.9.2. Generator Service

- Emergency power sources to critical systems (communications system, intrusion detection system, Duty Agent room, Communication Equipment Room, and Office of Internal Affairs Technical Support Division Closet) are required.

6.9.3. Cleaning

- IA office cleaning must be performed during normal working hours. Maintenance should be aware that name checks shall be conducted on cleaning and maintenance personnel. If the facility is GSA-leased, GSA will provide the appropriate documents identifying cleaning crew personnel that have been properly adjudicated.

6.10. SECURE BORDER INITIATIVE (SBI)

- 6.10.1. The Department of Homeland Security's Secure Border Initiative (SBI) addresses the security challenges along the southern and northern land borders of the United States. SBI, in coordination with the other border security missions conducted by ICE, USCIS, USGC, Intelligence, and the Department of Justice works to address our Nation's immigration border security challenges. The scope of SBI provides

DHS and CBP with the optimum mix of personnel, technology, infrastructure, and response platforms to detect, identify, classify, and respond to illegal breaches of borders shared with Canada and Mexico and thereby bring the situations to the appropriate law enforcement resolution. SBI will employ next generation technology in the area of cameras, ground-based radar, communications, unmanned aerial vehicles, underground sensors, and sophisticated software packages for terrain environments. SBI will bring together multiple state of the art systems as well as traditional security infrastructure to create a comprehensive border security program.

6.10.2. For more information, see [Appendix 6.10. Secure Border Initiative](#).

6.11. SECURITY SURVEY PROCESS

6.11.1. This is in development. When complete, this will contain the steps in conducting the survey and a possible checklist which will include the Physical Security Project Prioritization Tool:

- Findings;
- Requirements;
- Source document(s); and
- Response.





CHAPTER 7: EXTERIOR PROTECTION

7.1. GENERAL

- 7.1.1. Perimeter protection is the first line of defense in providing physical security for a facility. This can be accomplished by installing fences or other physical barriers, outside lighting, lockable gates, intrusion detectors, or a guard force. Perimeter protection also includes, but is not limited to walls, lockable doors, windows, bars, and grills.
- 7.1.2. A perimeter barrier defines the physical limits of a facility, controls access, and creates a physical and psychological deterrent to unauthorized entry. It delays intrusion into an area, making the possibility of detection and apprehension more likely. It aids security forces in controlling access and assists in directing the flow of persons and vehicles through designated entrances.
- 7.1.3. Every vulnerable point shall be protected to deter or prevent unauthorized access to the facility. The roof, basement, and walls of a building may contain vulnerable points of potential entry. A security assessment of the perimeter shall address manholes and tunnels, gates leading to the basement, elevator shafts, ventilation openings, fire escapes, skylights, and any opening 96 square inches or larger, that are within 18 feet of the ground.
- 7.1.4. The extent of any perimeter control levels above those outlined in this policy handbook will be determined by the DO in conjunction with CBP/IA/SMD, based upon a comprehensive security assessment. The assessment report shall recommend perimeter countermeasures to the facility manager.

7.2. PHYSICAL BARRIERS

- 7.2.1. Physical barriers may be of two general types-natural and man-made. Natural barriers include mountains, cliffs, canyons, rivers, or other terrain difficult to traverse. Man-made barriers include items such as fences, walls, floors, roofs, grills, bars, or other structures which deter penetration. If a natural barrier forms one side or any part of the perimeter, it in itself shall not automatically be considered an adequate perimeter barrier, since it may be overcome by a determined intruder. Man-made barriers shall be provided for CBP perimeters.

7.3. FENCING

- 7.3.1. Fences are the most common perimeter barrier or control. A perimeter fence should be Uninterruptible, kept free of plant growth, and maintained in good condition. Fences are used to:
- Demarcate property lines;
 - Impede unauthorized vehicular and pedestrian access;
 - Control and direct authorized vehicular and pedestrian access;
 - Impede natural nuisance alarms (used as a baseline wherever a perimeter intrusion detection system is used); and
 - Segregate areas within a property such as parking lots and storage yards (not

[RETURN TO TOP](#)

considered perimeter fences), and to control and direct the flow of authorized visitors.

- For more information, see [Appendix 7.3, Fencing](#)

7.3.2. Chain Link

- The entire site must be contained by an 8' (2.43 m) high perimeter fence;
- Chain link fencing is low in maintenance cost, a minimal safety hazard, and has openings small enough to discourage the passage of pilfered articles;
- Chain link fencing shall be laid out in straight lines to permit unhampered observation. It shall be constructed of 9-gauge or heavier mesh material (type I, II, or IV as defined in [Appendix 7.3, Fencing](#) with mesh openings (two-inch-square) and shall be no less than seven feet high and have a top guard for a total of 8 feet;
- Chain link fencing shall extend to within two inches of firm ground. It shall be taut and securely fastened to rigid metal posts set in concrete;
- The fabric height will be 7' (2.13 m) and have twisted and barbed selvage at the top and bottom. There must be a minimum 1' (.305 m) top guard, for a total fence height of no less than 8 feet (2.43 m);
- Apply anti-erosion measures, such as surface priming, as necessary;
- Where the fence traverses culverts, troughs, or other openings larger than 96 square inches in area, the openings shall be protected by fencing, iron grills, or other barriers to prevent passage of intruders without impeding drainage; and
- Pipes/culverts or openings through fence larger than 96 square inches shall be secured.

7.3.3. Barbed Wire

- Standard barbed wire is twisted, double strand, number 12-gauge wire, with four-point barbs spaced four inches apart;
- Barbed wire fencing, including gates intended to prevent trespassing, shall be no less than seven feet in height plus a top guard, tightly stretched, and shall be firmly affixed to posts not more than six feet apart; and
- Distances between strands shall not exceed six inches.

7.4. GATES

7.4.1. For more information, see the section on [Gates](#) in [Appendix 7.3, Fencing](#).

7.4.2. Gates provide a break in a perimeter fence or wall to allow entry. Gates are protected by locks, intermittent guard patrols, fixed guard posts, contact alarms, CCTV or a combination of these. The number of gates and perimeter entrances shall be limited to those absolutely necessary, but shall be sufficient to accommodate the peak flow of pedestrian and vehicular traffic.

7.4.3. Gates shall be adequately lighted. They shall be locked when not manned and periodically inspected by a roving guard force. Utility openings in a fence that do not

[RETURN TO TOP](#)

serve as gates shall be locked, guarded, or otherwise protected.

- 7.4.4. Intrusion detection devices may be desirable when the gate is used intermittently or when a higher level of protection is desired. Alternatives to detection devices include coded card keys, push button combination locks, and CCTV.

7.5. PROTECTIVE LIGHTING

- 7.5.1. For more information, see [Appendix 7.5, Protective Lighting](#).

- 7.5.2. Protective lighting is a valuable and inexpensive deterrent to crime. It improves visibility for checking badges and people at entrances, inspecting vehicles, preventing illegal entry, and detecting intruders both outside and inside buildings and grounds. Locate protective lighting where it will illuminate shadowed areas and be directed at probable routes of intrusion. Overlap lighting to prevent dark areas. If justified, include emergency power for lighting.

7.6. DOORS

- 7.6.1. Doors are vulnerable points in the security of any building. All doors shall be installed so the hinges are on the inside, to preclude removal of the screws or the use of chisels or cutting devices. Pins in exterior hinges shall be welded, flanged, or otherwise secured, or hinge dowels shall be used to preclude the door's removal. Doors shall be 12-gauge hollow metal or 1 3/4" solid wood. Remember that locks, doors, door frames, and accessory builders' hardware are inseparable when evaluating barrier value. Do not put a sturdy lock on a weak door. The best door is of little value if there are exposed removable hinge pins, breakable vision panels, or other weaknesses that would allow entry. Transoms and other windows near doors shall be sealed permanently or locked from the inside with a sturdy sliding bolt lock or other similar device, or equipped with bars or grills.
- 7.6.2. Overhead roll doors not controlled or locked by electric power shall be protected by slide bolts on the bottom bar. Chain link crank-operated doors shall be provided with an iron keeper and pin for securing the hand chain, and the shaft shall be secured. A solid overhead, swinging, sliding, or accordion type garage door shall be secured with a cylinder lock or padlock, with, a metal slide bar, bolt, or crossbar shall be provided on the inside. Metal accordion grate or grill-type doors shall have a secured metal guide tracks at the top and bottom and be secured with a cylinder lock or padlock.

- 7.6.3. For more detailed information, see [Appendix 7.6, Doors and Door Hardware](#).

7.7. WINDOWS

- 7.7.1. Windows are another vulnerable point for gaining illegal access to a building. Windows shall be secured on the inside using a lock, locking bolt, slide bar, or crossbar with a padlock. The window frame must be securely fastened to the building so that it cannot be pried loose.

- 7.7.2. Bars and steel grills can be used to protect a window. These shall be at least one

[RETURN TO TOP](#)

half-inch in diameter, round, and spaced apart six inches on center. If a grill is used, the material shall be number nine gauge two-inch square mesh. Outside hinges on windows shall have non-removable pins. The hinge pins shall be welded, peened, flanged, or otherwise secured so they cannot be removed. Bars and grills must be securely fastened to the window frame so they cannot be pried loose.

7.7.3. For more detailed information, see [Appendix 7.7, Windows](#).

7.8. MANHOLES, GRATES, AND STORM DRAINS

7.8.1. Many facilities have manholes and tunnels providing personnel service entrance into buildings and other manholes may provide entrance to tunnels containing pipes for heat, gas, water, and telephone. If a tunnel penetrates the interior of a building, the manhole cover shall be secured. A chain or padlock can be used to secure a manhole. Steel grates and doors flush with the ground level may provide convenient access. These openings may be designed into the facility as they may provide light and ventilation to the basement levels. If the frame is properly secured, the grates or doors can be welded into place or they can be secured with a chain and padlock. Sewers or storm drains which might provide an entrance shall be secured.

7.8.2. For more detailed information, see [Appendix 7.8, Openings](#).

7.9. OPENINGS

7.9.1. Operable Openings are doors, windows, transoms, skylights and all similar devices that can be opened or closed to allow or prevent passage of people, air, or light. Openings can also include, but are not limited to, elevators, penthouses, hatchways, or doors to the roof. Roof doors are often overlooked because of infrequent use. These openings are the usual points of entry for intruders especially at ground level and in their concealed and semi-concealed locations. Operable openings are also the hardest points to protect simply because they are designed for passage.

7.9.2. Protecting operable openings shall be based on the following criteria:

- Is the opening really required?
- Is the opening 96-square inches or larger?
- Validate existing openings that may no longer be required. If not required:
 - Is the opening less than 18 feet from the ground or less than 14 feet from another structure? If yes, than it shall be covered with bars or grilles and equipped with intrusion detection device;
 - Permanently seal the wall in a manner that maintains the penetration resistance of the wall containing the opening; and
 - The door is eliminated from the brick wall, the door assembly will be removed and the opening bricked up; properly anchoring new construction.
 - For further information see [Appendix 7.8, Openings](#).

7.10. SHAFTS, VENTS, AND DUCTS

7.10.1. Ventilation shafts, vents, or ducts, and openings in the building to accommodate fans or the air conditioning system, can be used to enter a facility.

- A ventilation fan can be removed or the blade bent to make a sufficiently large opening for entry;
- Bars are recommended to deter such access.

7.10.2. For more detailed information, see [Appendix 7.8. Openings](#).

7.11. FIRE ESCAPES AND BUILDING WALLS

7.11.1. Normally, outside fire escapes do not provide an entrance directly into the building. However, they can provide easy access to the roof or openings high above the ground level. Windows or other openings off the fire escape shall be capable of being opened only from the inside. The exterior fire escape shall not extend all the way to the ground.

7.11.2. Walls are not normally considered possible points of entry because of their usual solid construction. However, they cannot be disregarded because intruders may be able to break through them to gain entrance. Reinforcement at critical points may be necessary to deter forced entry.

7.12. FACILITIES IN REMOTE LOCATIONS

7.12.1. Large facilities located in sparsely inhabited areas have an inherent form of protection by virtue of their isolation. Constructing a fence around the perimeter usually will provide an adequate deterrent to entry. Occasional observation by a roving guard force may be necessary depending on the sensitivity of the facility. Warning signs or notices shall be posted to deter trespassing on government property. CCTV systems can be especially helpful if guard force personnel are available to monitor them.

7.13. EXTERIOR SIGNAGE

7.13.1. Warning Signs. Warning signs or notices shall be posted to deter trespassing on government property. Signs shall be plainly displayed and be legible from any approach to the perimeter from a reasonable distance. The size and coloring of such signs, lettering, and interval of posting must be appropriate to each situation.

7.13.2. Under [41 CFR §102-74.365, Conduct on Federal Property](#), the building rules and regulations applicable to property under the authority of the U.S. General Services Administration and to all persons entering in or on such property must be posted at entrances. Signage such as Inspections, Admission to Property, and Conformity with signs and directions, weapons and explosives and other regulations are covered under subparts of 41 CFR §102-74.365.

7.13.3. Control Signs. Signs shall be erected where necessary to assist in control of authorized entry, to deter unauthorized entry, and to preclude inadvertent entry. Persons in or on CBP property shall at all times comply with signs of a prohibitory,

[RETURN TO TOP](#)

regulatory, or directory nature and with the lawful direction of security guards or other authorized individuals.

7.14. OTHER SIGNS

7.14.1. Condition of Entry. Signs setting forth the conditions of entry to a CBP facility or area shall be plainly posted at all principal entrances and shall be legible under normal conditions at a distance not less than 50 feet from the point of entry. The signs shall state that packages, briefcases, and other containers in the immediate possession of visitors, employees, or other persons arriving on, working at, visiting, or departing from CBP property, are subject to inspection. Any person and vehicle is subject to a full search at any time and, if found to be in violation of federal, state or local laws, is subject to arrest.

7.14.2. For more information, see [Chapter 11, Access to Facilities](#).

7.14.3. Restricted Areas. Signs or notices legibly setting forth the designation of restricted areas and conditions of entry shall be plainly posted at all entrances and at other points along the perimeter as necessary.

7.14.4. Explosives. Signs or notices must clearly indicate that no person entering or on Customs and Border Protection property shall carry or possess explosives, or items intended to be used to fabricate explosives or incendiary devices, either openly or concealed, except for official purposes. See [41 CFR §102-74.435](#)

7.14.5. Weapons Prohibited. [18 USC §930](#) prohibits possession of a firearm or other dangerous weapon in Federal facilities, unless authorized by law, and defines “dangerous weapons” as a weapon, device, instrument, material, or substance, animate or inanimate, that is used for, or is readily capable of, causing serious bodily injury or death, except that such term does not include a pocket knife with a blade of less than 2-1/2 inches in length.

- Access control
 - Complete a risk assessment of the facility. If it is determined that positive accounting of personnel or assets is required, controlled egress will be part of the access control system.
 - The means of egress control will be at least equal to the access control for that portal.
 - Door control applications must meet local fire codes.
 - Uncontrolled egress will likely be adequate for most area control points at the majority of CBP/IA/SMD activities.
- Screening
 - All persons who are not CBP direct hire or full time contract employees, or do not possess a valid building pass for a particular Service facility (if applicable) will be considered as visitors;
 - All visitors requesting access to locations where a threat assessment has identified the need to screen for weapons, explosives, and incendiary devices

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

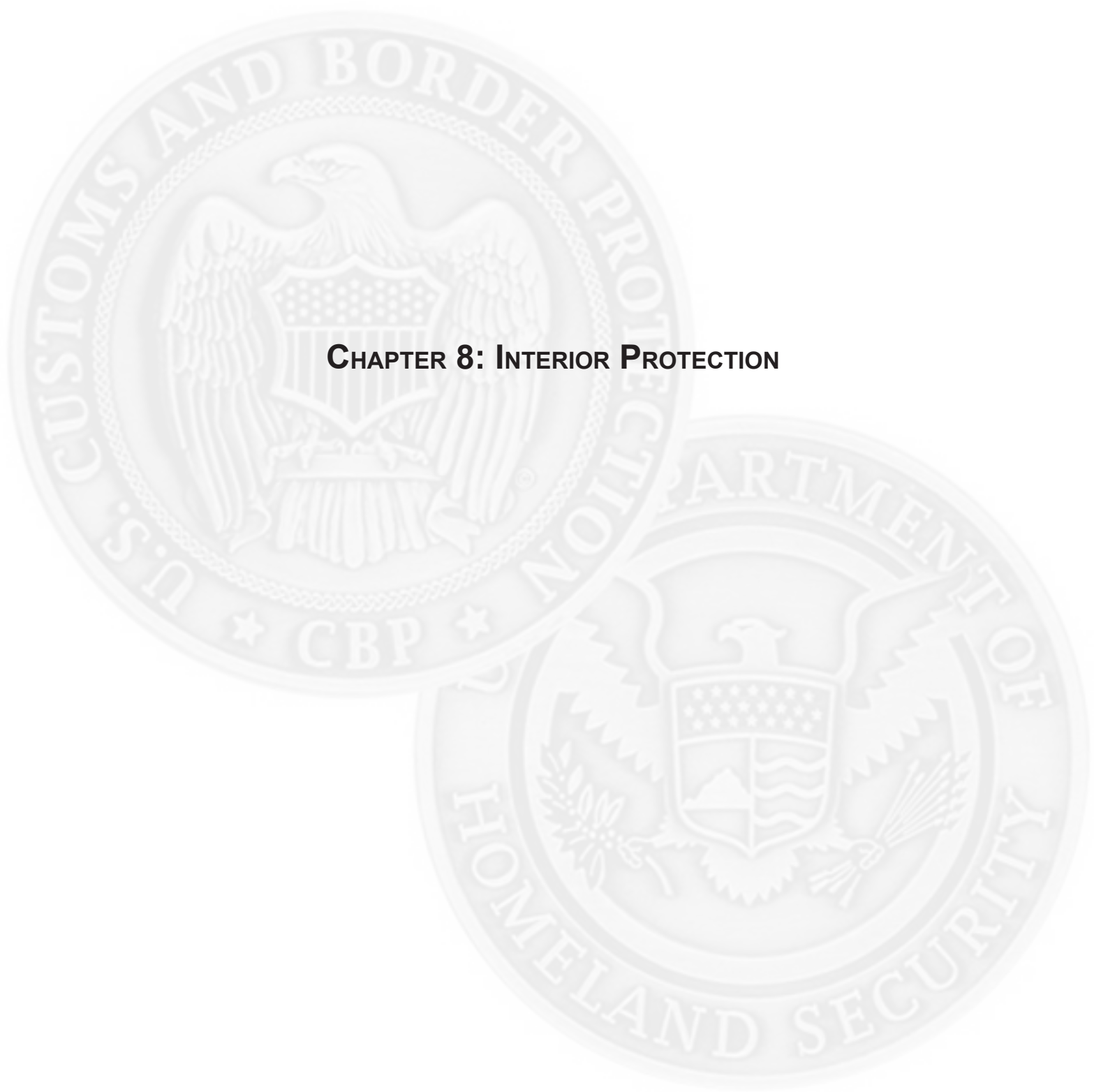
will be screened;

- o Threat assessment may indicate a need to screen packages for weapons, explosives, and incendiary devices. Such packages may be transported by:
 - A visitor requesting access,
 - A freight carrier,
 - An express package delivery firm,
 - The U.S. Postal Service, and
 - U.S. Government courier.

7.15. LOADING DOCKS AND SERVICE ACCESS

7.15.1. Loading docks and service access areas are commonly required for a building and are typically desired to be kept as invisible as possible. For this reason, special attention should be devoted to these service areas in order to avoid undesirable intruders.

- Information on Loading Docks and Service Access may be found in [Appendix 7.15, Loading Docks and Service Access](#).



CHAPTER 8: INTERIOR PROTECTION

8.1. INTERIOR CONTROLS

8.1.1. After exterior perimeter controls and access to the facility, the next line of defense is interior controls. When an intruder is able to penetrate the perimeter controls and the building exterior, the effectiveness of interior controls is tested. There are few facilities where every employee has access to every area in the facility. Accordingly, access to some areas is necessarily controlled. For example, interior controls are necessary to protect classified information from unauthorized disclosure, to prevent damage to the area or equipment, to prevent interference with operations, for safety purposes, or for a combination of these and other reasons. Usually, interior controls are applied to specific rooms or physical spaces within a building. The Designated Official is responsible for determining whether interior controls are necessary. Office area controls include key accountability systems, locking devices and access control systems such as sign-in registers and identifying credentials. Determine the extent of interior controls by considering the monetary value and mission criticality of the items or areas to be protected, the vulnerability of the facility, and the cost of the controls. Normally, the cost of security controls shall not exceed the value of the item or areas to be protected.

8.2. ACCESS CONTROL

8.2.1. Vehicles and Traffic Control. If public vehicle entrances have gates, these will be manually opened and closed. Vehicle entrances with restricted access at facilities associated with a high threat level will be equipped with electrical or hydraulic vehicle gates or movable barriers. Vehicle barriers may be controlled by:

- Card readers;
- Biometric devices;
- Proximity tags;
- Electronic keypads;
- Line-of-site or using CCTV; and
- One-way entry and exit lanes, created for high-traffic areas.

8.3. VEHICLE

- Vehicle loop detectors or other sensor systems may be used as request-to-exit devices, but must be located so as to prevent unauthorized activation.
- Vehicle screening may need to be conducted at locations associated with a high threat level. Screening is most associated with delivery vehicles entering a loading zone or dock area. If possible, the screening area shall:
 - Be at least 100 feet from the building;
 - Have a one-way restricted traffic lane;
 - Have signs and barriers to control traffic; and
 - Allow vehicles to exit the inspection area safely if denied access.

8.3.1. Pedestrians

- Access control systems must be provided at public waiting and information areas, visitor areas, sally ports, secure vestibule, loading docks, and entrances to restricted areas.
 - The access control system may be a personnel, hardware, or computer-based system;
 - A personnel-based access control system relies on a person to positively identify individuals requesting access, determine if the access is authorized, and secure the access point, ensuring that only authorized individual(s) have gained access.
- A hardware-based access control system uses mechanical push button or key locks to control access. This type of system is most suitable for interior areas with fewer than 25 users. Characteristics of this type of system are:
 - One combination or the same key is used for all authorized individuals;
 - No audit trail is available;
 - No power is required; and
 - A mechanical spring latch shall not be used as a lock-and-leave security measure.
- Automated access control systems are appropriate for large applications and may be required for programs associated with a high threat level. Systems may be in the form of stand-alone, one- or two-door units, small networks for 8 - 16 doors, or larger multi-door, multi-tasking systems. These types of systems are ideal for areas with 25 or more users and large systems controlling interior and exterior access control readers. Characteristics of this type of system are:
 - All authorized users are provided with unique pass cards, tags or personal identification numbers (pins);
 - Audit trails are available;
 - Electrical power is required at each control point; and
 - Individual users can be deleted from the system without the need to recover cards, tags, pins or keys.
- Egress Control
 - The decision to provide for controlled or uncontrolled egress will be based on a risk assessment of the facility. If it is determined that positive accounting of personnel or assets is required, controlled egress will be part of the access control system;
 - The means of egress control will be at least equal to the access control for that portal;
 - Door control applications must meet local fire codes; and
 - Uncontrolled egress will likely be adequate for most area control points at the majority of CBP/IA/SMD activities.

- Screening
 - All persons who are not CBP direct hire or full time contract employees, or do not possess a valid building pass for a particular Service facility (if applicable) will be considered as visitors;
 - All visitors requesting access to locations where a threat assessment has identified the need to screen for weapons, explosives, and incendiary devices will be screened; and
 - Threat assessment may indicate a need to screen packages for weapons, explosives, and incendiary devices. Such packages may be transported by:
 - A visitor requesting access;
 - A freight carrier;
 - An express package delivery firm
 - The U.S. Postal Service;
 - U.S. Government courier.

8.4. ROUTINE CONDITIONS

- 8.4.1. Basic requirements for admission to Federal property are contained in FPMR 101-20.302. Accordingly, during business hours, CBP facilities are normally open to the public and restricted to authorized individuals after business hours.
- 8.4.2. During business hours, property or portions thereof can be closed to the public only when situations require this action to ensure the orderly conduct of Government business. The decision to close the property or portions thereof to the public shall be made by the designated official under the occupant emergency program after consultation with the building manager and the responsible Security Officer. When property or a portion thereof is closed to the public, admission shall be restricted to authorized persons who will register upon entry to the property and, when requested, display CBP or other identifying credentials when entering, leaving, or while on the property. Property or portions thereof that are closed to the public shall be designated as a restricted or closed area.
- 8.4.3. Emergency Conditions. During certain DHS-declared building security alert conditions, the display of government identification and additional screening may be required to enter the facility during all hours.
- 8.4.4. Public Use of Buildings. The occasional use of public areas within public buildings for cultural, educational and recreational activities, is permitted by [41 CFR §102-74-460](#) and [FPMR 102-74](#). Any use of public facilities should go through the permitting process described in those sections as coordinated with CBP/IA and the appropriate GSA contact.

8.5. AREA DESIGNATIONS

- 8.5.1. The decision to designate an area as either a “Controlled Area” or a “Restricted Area” shall be made in conjunction with a decision to close the property or a portion

thereof to the public.

8.5.2. **Controlled Area.** A controlled area is defined as a room, office, building or other form of facility to which access is monitored, limited, or controlled. Admittance to a controlled area is limited to persons who have official business within the area. Responsible managers are authorized to designate an area as a controlled area after adequate security measures are in place. The following areas shall be designated as controlled areas:

- Any area where classified information or highly sensitive information is handled, processed, or stored;
- Any area that houses equipment that is significantly valuable or critical to the continued operations or provision of services;
- Any area where uncontrolled access would interfere with or disrupt personnel assigned to the area in carrying out their official duties;
- Any area where equipment or operations constitute a potential safety hazard; and
- Any area that is particularly sensitive, as determined by the responsible manager.

8.5.3. **Restricted Area.** A restricted area is a room, office, building, or other form of facility to which access is strictly controlled. Admittance to a restricted area is limited to personnel assigned to the area and persons who have been specifically authorized access to the area. Visitors to a restricted area and uncleared personnel must be escorted by personnel assigned to the area and all classified information must be protected from observation, disclosure, or removal. The responsible manager is authorized to designate an area as a restricted area after adequate security measures are in place. The following areas shall be designated as restricted areas:

- Any area approved by the CBP/IA/SMD for the storage of Top Secret Information;
- Any area approved by the CBP/IA/SMD for the open storage of Secret or Confidential classified information. This includes areas where classified information is normally or frequently displayed, such as charts, maps, drawings, photographs, equipment, or conference rooms where classified information is being discussed. This does not include an office in which classified information is discussed or displayed and action can be taken by occupants to prevent disclosure;
- Any area housing a Secure Telephone(s) [formerly known as Secure Telephone Unit (STU-III), now referred to as Secure Terminal Equipment (STE)];
- Any area where classified information is visually displayed on an approved standalone office information system;
- Any area that houses mainframe computers or designated Automated Information System (AIS) sensitive systems; and
- Any area that is highly critical or sensitive, as determined by the responsible manager.

8.5.4. **Special Access Program Area(s) (SAP).** A program established for a specific class

of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

- The Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office;
- An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only;
- Special Access Programs are required to be reviewed annually; and
- The processes and standards are based upon criteria established by [Executive Order \(EO\) 12968, "Access to Classified Information,"](#) Department of Defense (DOD) Directive 0-5205.7, "Special Access Program (SAP) Policy" and [Director of Central Intelligence \(DCID\) Directive 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information \(SCI\)."](#)

8.5.5. Other Special Access Program Areas. Government agencies outside the intelligence community may have special access programs which require stringent physical security standards for working and storage areas. CBP/IA/SMD areas where special access program information is stored, used, discussed, or processed will be constructed in accordance with standards issued by the sponsoring agency.

8.6. SECURITY VAULTS (PERMANENT STORAGE OR MORE THAN 72 HOURS)

8.6.1. A security vault is a completely enclosed space with a high degree of protection against forced entry. Vaults are commonly used for storing Top Secret information, special access program information, extremely valuable materials and seized property.

8.6.2. General Requirements for Vaults. There are three classes of vaults for the storage of classified material and equipment A, B and C. Class A vaults offer the maximum protection against tool and torch attack. Class B vaults offer less than maximum protection. A lightweight, portable "modular vault" meeting Federal Specification AA-V-2737 may also be used to store classified material and equipment. The modular vault is equivalent to a Class B vault. Class C vaults offer less than maximum protection and may be used where unique structural circumstances do not permit concrete vault construction. Utilization of any vault class, or the modular vault, is dependent upon the physical location environment where the vault is to be erected. The minimum construction requirements for each class of vault are described as follows. Reference: FED-STD 832 (This document establishes minimum construction requirements for high security vaults for storage of classified information and weapons).

8.6.3. For more detailed information, see [Appendix 8.6, Vaults.](#)

[RETURN TO TOP](#)

8.7. VAULT DOORS

8.7.1. Vault door and frame shall conform to [Federal Specification AA-D-600D, Class 5 Vault Door](#).

- Armory vault doors and security vault doors are both manufactured according to [Federal Specification AA-D-600D, Door, Vault, Security](#). The difference between the two doors is that armory vault doors, used to protect AA&E, are fitted with UL Standard 768, Group 1, mechanical combination locks. Security vault doors, used to protect classified information, are fitted with locks meeting [Federal Specification FF-L-2740, Locks, Combination](#). The armory vault door label (silver with red letters) states that it is a “GSA Approved Armory Vault Door”. The security vault door label reads “GSA Approved Security Vault Door” (label also silver with red letters);
- There are numerous GSA-approved Class 5 security vault doors being used for the protection of weapons, which is authorized under (link), however It is strongly recommend that locks be changed out to the UL Standard 768, Group 1, mechanical combination lock, when and if a failure occurs with an X-07, X-08 or X-09 lock. When that change is made it must be noted on the [Optional Form 89](#) (Maintenance Record for Security Containers/Vault Doors). It shall also be noted on the front of the armory door that is not authorized for the protection of classified information.

Federal Specification: AA-D-600D (see links below for documents)

Title: Federal Specification Door, Vault, Security

Scope: This specification covers vault doors that are designed to conform to the minimum standards for physical security equipment as required by the Information Security Oversight Office Directive governing the safeguarding of national security information. The doors provide protection against unauthorized entry for the periods of time specified.

Classes: Class 5-V:
Security vault door shall be resistant to 20 man-hours surreptitious entry, 30 man-minutes covert entry and 10 man-minutes forced entry.
Class 5-A:
Armory vault door shall be resistant to 30 man-minutes covert entry and 10 man-minutes forced entry.
Class 5-B:
Ballistic vault door shall be resistant to 20 man-hours surreptitious entry, 30 man-minutes covert entry, 10 man-minutes forced entry, ballistic resistant.

Document Date: 15 May 2000

Document Status: Active

Status:

[AA-600D Amendment 1, 25 May 2001](#)

[AA-600D base document, 15 May 2000](#)

[QPL-AA-D-600-7 14 May 2000](#)

GSA-Approved Armory Vault Doors

All armory vault doors listed below are Class 5 and are fitted with a UL Standard 768al combination lock. GSA approved armory vault doors can be purchased direct from the manufacturers using the National Stock Numbers listed below. See the Order tab for manufacturer information.

NSN	Description
7110-01-475-9598	Left hand swing, without optical device.
7110-01-475-9596	Right hand swing, with optical device.
7110-01-475-9595	Right hand swing, without optical device.
7110-01-475-9593	Left hand swing, with optical device.
7110-01-475-9590	Double leaf, right opening swing active leaf, with optical device.

8.8. STRONGROOMS

8.8.1. A strongroom is an enclosed space constructed of solid building materials. Strongrooms are normally used for the storage of classified material or sensitive materials, such as firearms or evidence. Protection is normally supplemented by guards or alarm systems. Rooms that have false ceilings and walls constructed of fibrous materials, and other modular or lightweight materials cannot qualify as strongroom.

8.8.2. For more information, see [Appendix 8.8, Strongrooms](#).

8.9. INTRUSION DETECTION SYSTEMS

8.9.1. Intrusion Detection Systems (IDS) are alarm systems designed to alert security personnel of an actual or attempted intrusion into an area while providing deterrence to intrusion. These warning systems detect intrusion or attempts, not prevent them. Any alarm system requires an assessment and a response capability to provide real protection for an area. All systems have weak points by which their functioning can be minimized or even completely interrupted or circumvented. The advantage and limitations of a variety of detection systems are described below.

8.9.2. **For more information, see [Appendix 8.9, Intrusion Detection Systems](#)**

8.10. HOLD ROOMS

8.10.1. A hold room is a secure facility for the detention of aliens encountered and processed by operational components of CBP.

8.10.2. For more information, see [Appendix 8.10, Hold Rooms](#)

8.11. PLANNING ALARM INSTALLATIONS

8.11.1. Alarms are used to detect approach or intrusion. Some alarms are intended for exterior protection, and some are suitable only for indoor installations. The following shall be addressed in determining the need for an alarm system:

- Sensitivity or criticality of the operation;
- Facility vulnerability to damage, interruption, alteration or other harm;
- Sensitivity or value of the information or property stored at the facility;
- Location of facility and accessibility to intruders;
- Other forms of protection in place or available; and
- Guard or law enforcement response capability.

8.11.2. Components of an Alarm System.

- An alarm system is composed of three main parts:
 - One or more sensors to detect the presence or actions of an intruder,
 - A control unit that constantly monitors the sensors and transmits an alarm signal when a sensor detects an intruder, and
 - The alarm annunciator.
- Perimeter protection alarm systems utilize point protection sensors almost exclusively, while area protection (volumetric) sensors are used primarily in interior alarm circuits to detect an individual within a building;
- Object protection provides direct security for individual items and is often the final stage of an in-depth protection system with perimeter and area-protection; and
- Alarm systems can be designed so that various parts of a building have separate sensor circuits, or zones, and it is not uncommon to have a separate duress or holdup alarm circuit to enable employees to summon security personnel.

8.11.3. The installation of alarm system components is very important.

- Individual sensors are designed to respond to specific stimuli that indicate the presence of an intruder or an attempt to gain entry into a protected area;
- Switch sensors must be mounted so that they detect the actual opening of a door or window, but at the same time, the manner of installation shall not make them so sensitive to movement that they actuate an alarm from vibrations caused by a truck passing on the street or the wind rattling doors and windows; and
- Care must be exercised in adjusting the sensitivity of the more complex sensors in order to avoid false alarms. Some units can be actuated by a flickering fluorescent light or a telephone bell. Electromagnetic interference from a mobile radio or a thunderstorm can trigger some detectors.

8.11.4. Sensors.

- The three basic types of sensors are:
 - Perimeter;

- o Volumetric; and
- o Proximity.
- Perimeter protection is the first line of defense. The most common points for sensing devices are doors, windows, vents and skylights. These may be protected, with detectors sensing their opening or breaking. The major advantage of perimeter-protection sensing devices is their simple design. The major disadvantage is that they protect only openings such as doors or windows. If intrusion occurs through a wall or ceiling, these devices are ineffective:
 - o Switches. These devices are usually magnetic operated switches affixed to a door or window in such a way that opening the door or window removes the magnetic field causing an alarm. High security switches are normally balanced or biased magnetic switches;
 - o Screens. Openings such as vents, ducts, skylights, and similar openings can be alarmed by thin wire filaments that signal an alarm if the screen is cut or broken. Often the wire filaments are placed in a frame of wooden rods and require little maintenance; and
 - o Glass Breakage. Electronic sensing devices used to detect a high-frequency sound pattern within the glass when it is broken, or the shock wave a substantial impact makes against the surface.
- Volumetric protection sensors are designed to detect the presence or actions of an intruder almost anywhere within an entire room, from floor to ceiling. A variety of volumetric devices are available. Each kind of detector has some advantages and limitations. Therefore, a device must be selected for a specific environment. A major advantage of volumetric devices is that they provide a highly sensitive and invisible means of detection in high-risk areas. The major disadvantage is that an improper application can result in frequent false alarms.
 - o Infrared. Passive infrared sensors are part of the motion-detection group. They sense the body heat of an intruder as he/she passes through the protected area. Infrared detectors are relatively free of false alarms; however items moved by air currents within the protected area can activate the alarm;
 - o Ultrasonic. Ultrasonic motion detectors generate a high frequency of sound that is out of the normal range of human hearing. An intruder disrupting the ultrasonic wave pattern initiates the alarm. Ultrasonic devices are prone to false alarms, due to excessive air currents or ultrasonic noise from mechanical equipment;
 - o Microwave. This kind of motion detector uses high-frequency radio waves, or microwaves, to detect movement. Because microwaves penetrate materials such as glass, and metal objects reflect them, they can detect motion outside the protection area and cause false alarm problems if not properly installed; and
 - o Photoelectric. Photoelectric devices transmit a beam across a protected area. When an intruder interrupts this beam, the circuit is disrupted causing an

alarm. Today's photoelectric devices use diodes that emit an invisible infrared light and usually pulses rapidly to prevent compromise by substitution. A disadvantage is that they can be defeated relatively easily; the beams are narrow and may be discovered or avoided.

- Proximity protection provides direct security for individual items.
 - Vibration. These seismic sensing devices use a piezoelectric crystal or microphone to detect the sound pattern that a hammer-like impact on a rigid surface would generate. These devices are attached directly to safes and filing cabinets, or to the walls, ceiling, and floor of vaults. False alarms may occur with these devices by passing vehicles or falling objects;
 - Capacitance. A capacitance device is used to protect specific objects such as security containers and safes. The capacitance alarm uses the metal construction of the container and causes it to act as a capacitor or condenser. When a change occurs in the electromagnetic field surrounding the metal object, the balance is disturbed and the alarm is activated. The system can only be applied to ungrounded equipment and accidental alarms can occur if the container is carelessly touched when the alarm is activated.

8.12. CLOSED CIRCUIT TELEVISION SYSTEMS

8.12.1. The Closed Circuit Television (CCTV) system is another core subsystem of an overall Electronic Security System (ESS). It is a collection of cameras, recorders, switches, keyboards, and monitors that allow viewing and recording of security events. The CCTV system is normally integrated into the overall ESS and centrally monitored from the Dispatch Center. Uses of CCTV systems for security services include several different functions as described below.

- Surveillance. CCTV cameras can be used to give a viewer the capability to be made aware of, or view, visual events at multiple locations from a centralized remote viewing area. CCTV camera technology makes visual information available that would normally only be available through multiple (possibly roving) human resources;
- Detection. CCTV cameras when employed with video content analysis or motion-path analysis, software and equipment, can be used as a means for intrusion detection. Additional information on CCTV can be found in [Chapter 11, Access to Facilities](#);
- Assessment. When alerted by an alarm notification, CCTV cameras allow Dispatch Center operators or other viewers to assess the situation and make a determination as to what type of response may or may not be required. An example is an intrusion alarm at a remote facility. Visual assessment and other confirmation may indicate an unannounced maintenance crew at work. If it is determined that intrusion has occurred appropriate response would follow;
- Deterrence. While more effective against unsophisticated burglars as opposed to trained covert insurgents, CCTV cameras may deter burglary, vandalism, or intrusion due to fear of discovery and prosecution;

[RETURN TO TOP](#)

- Evidentiary Archives. Retrieval of archived images may be helpful in identification or prosecution of trespassers, vandals, or other intruders;
- Facial Recognition. Cameras can be used for biometric facial recognition as discussed in [Chapter 11, Access to Facilities](#); and
- Intrusion Detection. CCTV cameras, when employed with video content analysis or motion path analysis software and equipment, are increasingly being used as a means for intrusion detection as discussed in [Appendix 8.9, Intrusion Detection Systems](#).
- For more detailed information, see [Appendix 8.12, CCTV](#).

8.13. OPEN STORAGE CERTIFICATION PROCESS

- 8.13.1. See [MD 11046 Open Storage Area Standards](#)
- 8.13.2. All CBP Open Storage Areas shall be certified as complying with DHS Management Directive 11046 (Open Storage Area Standards for Collateral Classified Information).
- 8.13.3. CBP/IA/SMD is the security approval authority for CBP open storage areas.
- 8.13.4. Open Storage Area is defined as: A room or area constructed and operated pursuant to DHS Management Directive 11046, for the purpose of safeguarding national security information that, because of its size or nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.
- 8.13.5. Examples of CBP Open Storage Areas include:
 - Homeland Secure Data Network (HSDN) rooms: is the secret collateral network for DHS and its components. See [Figure 1](#);
 - Vaults: A security vault is a completely enclosed space with a high degree of protection against forced entry. Vaults are commonly used for storing Top Secret information, special access program information, and extremely valuable materials.
- 8.13.6. General Requirements for Open Storage Area Certification. HSDN and Vault Certification
 - Policy
 - Construction and accreditation of a collateral-level, open-storage facility shall be considered only when the volume or bulk of classified material, or the functions associated with processing the classified material, make the use of GSA-approved security containers impractical;
 - DHS Management Directive (MD) 11046 prescribes the standards for openly storing classified national security information. CBP Operational Division may exceed the standards cited in MD 11046, but may not lessen them. If a CBP office chooses to exceed the standards cited, sufficient justification must exist to warrant any increased expenditures;
 - Requests to waive requirements cited in MD 11046 shall be submitted, in

writing, through the Security Officer/Security Liaison of the requesting office to the Internal Affairs (IA), Security Management Division (SMD), Physical Security Branch (PSB), via CBP.Security@dhs.gov. Waiver requests shall include sufficient justification to support the request and identification of compensatory measures that will be implemented to mitigate deficiencies; and

- o CBP offices that have open storage areas that were approved prior to the publication of MD 11046, will not need to have their areas re-certified unless a change has been made that affects the structure and measures in place at the time of the original certification, or the standards used for approval of the area are less than those required by this directive. In the latter instance, offices shall bring the area(s) up to the standards cited herein within one year of publication of this directive, and the area shall be recertified in accordance with this directive.

8.13.7. CBP Office Procedures for Requesting for Open Storage Area(s) Certification

- HSDN Certification: If a CBP office determines that an open storage area for classified information is necessary for their facility, the office will submit a request to CBP's Office of Intelligence & Operations Coordination (OIOC) outlining the justification to begin the process for Open Storage Area Certification. The OIOC will verify whether funding is available for equipment and construction of the Open Storage Area and initiate a HSDN account;
- If funding is available, OIOC will send a request to the Internal Affairs (IA), Security Management Division (SMD), Physical Security Branch (PSB), via CBP.Security@dhs.gov to initiate the certification process for Open Storage Area; and
- Vault Certification: If a CBP office determines that an open storage area for classified information is necessary for their facility, the office will submit a request to CBP's Office of Field Operations, Logistic Mission Support, Seizures and Penalties Division outlining the justification to begin the process for Open Storage Area Certification. The Seizures and Penalties Division will then notify request a Vault Certification whether funding is available for equipment and construction of the Open Storage Area.
- For more information, see [Appendix 8.6. Vaults](#).

8.13.8. Once SMD/IA/PSB receives the request, an Open Storage Certification Survey, MD 11046 with attachments A and B will be sent to the requesting office via email.

- The requesting CBP office will complete the entire survey ensuring that they meet the requirements outlined in Attachments A & B.
 - o Attachment A. Compliance with construction standards cited in MD 11046 shall be used to verify that the open storage area meets the minimum required construction standards;
 - o Attachment B. The sample Standard Operating Procedures (SOP) shall be modified and tailored to suit the specific open storage area to be certified.

[RETURN TO TOP](#)

- Upon completion of the survey package, the requesting CBP office will send survey to IA/SMD/PSB via CBP.Security@dhs.gov;
- For Vaults, inform Seizures and Penalties Division of intent to conduct Physical Security Open Storage Survey.
 - PASS -If the office meets the requirements outlined in the survey package, IA/SMD/PSB will schedule a physical security assessment of the facility to verify compliance with Attachment A and implementation of SOP in place.
 - If the customer passes, a memorandum signed by the SMD Director will be sent to CBP Office Director (Open Storage/Vault/HSDN room).
 - The memorandum will authorize a specific area being approved and will specify the maximum level of material authorized for open storage.
 - A copy of the approval memorandum, Open Storage Survey Checklist, and SOP shall be maintained by the CBP office.
 - FAIL. If the customer fails the initial certification survey, SMD/PSB will send a memorandum signed by the SMD Director outlining recommended corrective actions that must be addressed prior to approval of certification.

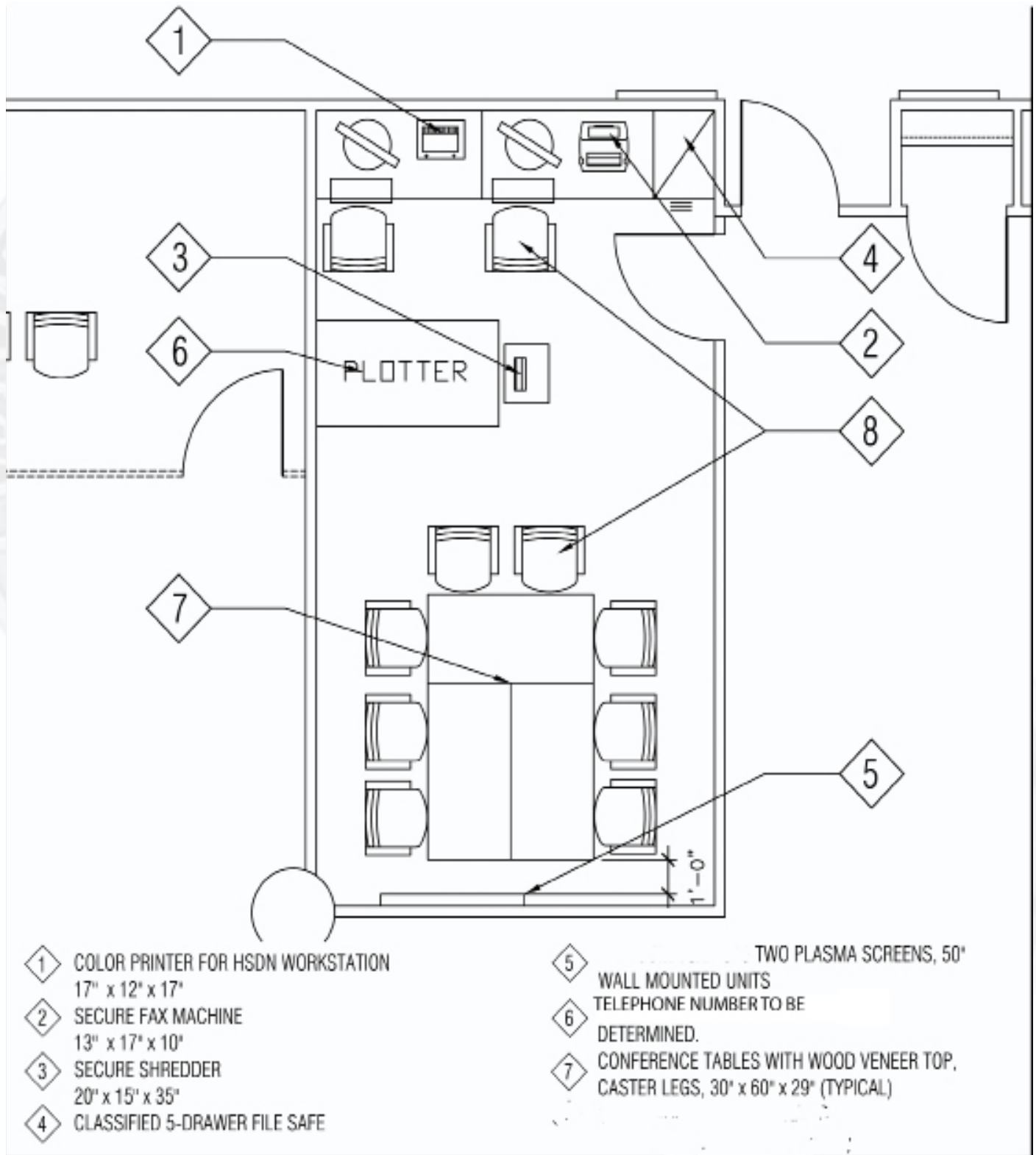
8.13.9. Open storage area is not authorized until all corrective actions have been implemented.

8.13.10. Upon verification of corrective actions, the Director of SMD will send a memorandum to CBP Office Director (Open Storage/Vault/HSDN room) indicating approval.

8.13.11. A copy of the approval memorandum, Open Storage Survey Checklist, and SOP shall be maintained by the CBP office.

8.13.12. The approval memorandum, Open Storage Survey Checklist, and SOP, shall be maintained by SMD/PSB and within the approved open storage area.

Figure 1: HSDN Room - Example







CHAPTER 9: LOCKS AND KEYS

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

9.1. Locks

9.1.1. General

- All exterior doors must have a lock with dead bolt or approved equal locking capability. All locks with a latch bolt must be equipped with a deadlocking latch feature. When specifying locks, use [American National Standards Institute](#) (ANSI) series lock numbers to obtain the proper type of lock for the function desired. The locks must meet all Federal handicap accessibility standards. All mortise locksets, whether or not required for security, must be grade one, commercial standard locks per ANSI/BHMA (Builders Hardware Manufacturers Association) A156.13. Unless specified, all interior non-security locksets may be cylindrical locks (bore lockset) as specified in ANSI/BHMA A156.2. The criteria in [ASM 273.44, Postal Service Locks](#), also apply. [Appendix 7.6, Doors and Door Hardware](#) contains an approved list of panic-style entry and exit devices and high security devices;
- Technology advances in the 1980s made locks vulnerable to newly developed opening techniques. In response, the Government prepared [Federal Specification FF-L-2740](#). FF-L-2740 addresses advances in combination lock neutralization technology. Three locks, the X-07, X-08 and X-09, all electro-mechanical locks, have met FF-L-2740;
- Some locks have interchangeable cores, which allow the same key system to include a variety of locks. Padlocks, door locks, cabinet locks, and electrical key switches can all be operated by the same key system. Because these cores are removable by a special key, this system allows for rapid re-keying of locks in the event that the key is compromised; and
- Locks are keyed in several different ways. When several locks are keyed differently, each is operated by its own key. When they are keyed alike, one key will open them all. Locks that are master-keyed are keyed differently, yet have one key that will open them all. Master-keying is done for convenience and represents the controlled loss of security. Master-keying is not used unless permitted by regulation.

9.1.2. Locking Hardware

- Locks are the most acceptable and widely-used security devices for protecting facilities, classified materials, and property. All containers, rooms, and facilities must be locked when not in actual use. Locking devices vary greatly in appearance as well as function and application. Locks merely deter or delay entry and shall be supplemented with other protection devices when a proper balance of physical security is needed. Some locks require considerable time and expert manipulation to open, but all locks can be defeated by force and with the proper tools. Locks must never be considered as a stand-alone method of security.
- For further information on locks and locking hardware, see [Appendix 7.6, Doors and Door Hardware](#).

9.1.3. Types of Locks

- Key locks consist of but are not limited to the following:
 - Dead bolt locks, sometimes called tubular dead bolts. These are mounted on the door in a manner similar to cylindrical locksets. The primary difference is in the bolt. When the bolt is extended (locked), the dead bolt projects into the door frame at least one inch, and it cannot be forced back (unlocked) by applying pressure to the end of the bolt. The dead-bolt lock has the potential for providing acceptable levels of protection for storerooms and other areas where more security is desired. In situations where there is a window in or adjacent to the door, a double cylinder dead-bolt lock (one that requires a key to open from either side) shall be used;
 - Mortise locks, so named because the lock case is mortised or recessed into the edge of the door. The most common variety of mortise locks has a doorknob on each side of the door. Entrance doors often have an exterior thumb latch rather than a doorknob. Mortise locks are desired due to flexibility and can incorporate dead bolt without compromising fire or life safety compliance. Mortise locks for security must adhere to ANSI/BHMA A156.13 standards and must have a dead bolt with a minimum throw of 1 inch;
 - Stand-alone access-control electro-mechanical locksets are primarily used to control entry into an area. Rather than using a key, these open by pushing a series of numbered buttons. The locks can be either electrically or mechanically activated. Some of the advantages of using these locks are low cost, easy installation, easy combination changing, and simple operation. These devices are used for access control and do not provide a high degree of security when used alone. Some models have “time penalty” and error alarm features and can be tied to an existing alarm system. The combination or code used to activate an electro-mechanical door lock shall be changed at least every two years and when any person having knowledge of the combination no longer requires access to the area;
 - Padlocks are detachable locks that are typically used with a hasp. Low security padlocks, sometimes called secondary padlocks, are used to deter unauthorized access, and they provide only minimal resistance to force. Low-security locks are made with hardened steel shackles. Precautions must be taken to avoid confusing these locks with similar brass or bronze locks. The brass or bronze locks are commonly used but do not meet the security requirements of the hardened shackled locks. High-security padlocks that meet FF-P-2827A provide the maximum resistance to unauthorized entry when used with a high security hasp;
 - Cylindrical locksets, often called key-in-knob or key-in-lever locks. These are normally used to secure offices and storerooms. The locking cylinder located in the center of the doorknob distinguishes these locks. Some cylindrical locksets have keyways in each of the opposing knobs that require a key on either side to lock and unlock them. Others unlock with a key, but may be

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

locked by pushing or rotating a button on the inside knob. These locks are suitable only for very low-security applications.

- All CBP lock cylinders must be of a high security, pick resistant design with angled key cuts, rotating tumblers, keyway side biting, and a slider mechanism. The cylinders must be Underwriters Laboratories (UL) listed under UL437 and certified under American National Standards Institute (ANSI)/Builder's Hardware Manufacturer's Association (BHMA) certification A156.30, Levels MIAM and ANSI/BHMA A156.5, Grade 1.
- All cylinders must incorporate three locking elements: a slider mechanism, a sidebar mechanism with tumbler rotation, and a pin tumbler elevation. All cylinders must be constructed of solid brass with hardened steel inserts. The lock tumblers must combine a dual-axis action with one axis utilized for pin tumbler rotation and the other axis utilized for positioning key cuts. Randomly selected tumbler pins must incorporate a hardened steel insert. The cylinders must be capable of being immediately re-keyed to a new combination or a new system.
- Interchangeable cores should be used to facilitate this process. A suitable number of spare cores should be maintained to facilitate lock changes in the event of a lost or stolen master key.
- The manufacturer must have the capability of establishing a key system with a minimum of six angle cuts in six possible pin positions with the capability of two distinct positions of cut per pin chamber, if required by the parameters of the system. The manufacturer must have the capability of producing a keying system in either of two distinct and different keying specifications and pinning specifications. The system must be capable of incorporating a key, with each being capable of more than one biting per position to expand master keying and key changes. The key must also incorporate the capacity to include twelve possible side bittings along the key blade located on two different planes or surfaces of the key. The system must also have the capability to provide a single master key with over 1 million (1,000,000) usable, non-interchangeable change keys in a single keyway. The key thickness must be no less than one hundred, twenty-five thousandths (.125") and must be made from a nickel silver alloy. Each key must be custom coined for tracking and identification purposes.
- The locking system must be deemed proprietary information shared only among authorized U.S. Customs and Border Protection (CBP) entities and the manufacturer. Security Specialists assigned to the Office of Internal Affairs, Security Management Division (IA/SMD) and employees serving as Collateral Security Liaison's for IA/SMD, will have the authority to request additional pinning materials and duplicate keys.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

9.2. COMBINATION LOCKS

- Combination locks are classified as Group 1, Group 1 R, or Group 2
 - GROUP 1 - Those locks that have a high degree of resistance to expert or professional manipulation. The protection against expert manipulation includes advanced design features not found in conventional designs;
 - GROUP 1 R - Those locks that have a high degree of resistance to expert manipulation, including use of radiological means; and
 - GROUP 2 - Those locks that have a moderate degree of resistance to unauthorized opening.
- DHS/CBP uses two types of mounted combination locks, one for the protection of classified material and one for the protection of weapons and ammunition. Combination locks that protect classified material must meet the requirements of Federal specification [FF-L-2740, Locks, Combination](#). Combination locks that protect weapons and ammunition must meet the requirements of Underwriters Laboratories Inc. Standard For Combination Locks UL 768, Group 1;
- These locks have been approved under FF-L-2740 for the protection of classified material. The model X-07 lock was approved in November 1991, the X-08 in March 1999, and the X-09 in June 2002. GSA-approved security containers and vault doors for the protection of classified material have had FF-L-2740 compliant locks installed at the time of manufacture since March 10, 1992;
- GSA-approved weapons containers and armory vault doors are available for the protection of arms, ammunition, and explosives. Mechanical combination locks that resist manipulation attempts for 20 man-hours are UL-listed as Group 1.
 - For further details, see [Appendix 10, Storage of Weapons and Ammunition \(Armory\)](#).
- Pedestrian door dead bolts covered by Federal specification [FF-L-2890, Lock Extension \(Pedestrian Door, Dead bolt\)](#) are intended for use on interior pedestrian doors used for normal entrance and egress during day-to-day operations. These locks have been approved under FF-L-2890: the model CDX-07 door lock was approved in November 1991, the CDX-08 in March 1999, and the CDX-09 in June 2002. While the CDX-07 and CDX-08 are still approved for securing classified material, they are no longer being manufactured. The Lockmaster LKM-7000 series also meets FF-L-2890; and
- Combination padlocks under the [FF-P-110, Padlock, Changeable Combination](#) Federal specification are intended for use as determined for low level resistance to forced entry and high level tell-tale manipulation or surreptitious action. The padlocks are intended for use ashore and aboard ocean going vessels, indoors, or outdoors, semi-protected by a structural overhang similar to eaves or a lean-to.

9.2.1. Combinations to locks will not be the same throughout a CBP facility, e.g. doors, vaults, etc.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

9.2.2. Changing Combinations

- Combinations to locks installed on security containers/safes, perimeter doors, windows and any other openings should be changed by the responsible individual, the Security Officer, or by a bonded contractor immediately when:
 - The container is placed in use;
 - An individual knowing the combination no longer requires access to the container, unless other means of preventing access exist;
 - The combination has been lost or is suspected to have been lost;
 - At least 12 months have passed;
 - As directed by the manufacturer; or
 - The container is taken out of service.
- Combinations to containers taken out of service must be reset to the standard factory combination of 50-25-50 prior to removal from the office space
 - Methods. Combination locks have either hand-change or key-change capability. A number of combination locks produced by a variety of manufacturers have been approved by GSA. These GSA-approved locks along with the non-approved locks use slightly different operating instructions and unique keys or particular hand change techniques for changing combinations. Often the experience necessary, as well as change keys, operating instructions, and changing procedures, are lost with the passing of time;
 - See the [Department of Defense Lock Program](#) for information on security hardware selection, requirements, specifications, national stock numbers, purchasing, training, and troubleshooting of equipment failures.
 - For assistance, contact SMD (CBP.Security@dhs.gov).

9.2.3. Selecting Combinations

- When selecting combination numbers avoid multiples of 5, ascending or descending numbers, simple arithmetical series, and personal data such as birth dates and Social Security Numbers. Use numbers that are widely separated. This can be achieved by dividing the dial into three parts and using a number from each third as one of the high-low-high or low-high-low sequences. Use a unique combination for each container. Do not re-use this combination anywhere else in the same office. Carefully follow any manufacturers' instructions in installing combination numbers.

9.2.4. Protecting Combinations

- Combinations should be known only by those persons whose official duties require access. The written combination should be protected at the highest classification level of material in the container or be protected in a manner commensurate with the value of the protected material;
 - Combinations should be memorized. They must not be carried in wallets or

concealed on persons or written on calendars, desk pads, etc.; and

- o When opening any kind of combination lock, be sure that no unauthorized person can learn the combination by observing the sequence of numbers being entered or dialed. It may be necessary to position your body so as to block the dial from the view of anyone standing nearby.

9.2.5. Recording Combinations

- Each Security Officer should assure that a record of the combination to each vault, secure room, combination padlock, and security container is recorded showing the location of the container or room, the name, home address, and home telephone number of a person responsible for the container. Standard Form (SF) 700, Security Container Information, has been designed for this purpose;
- A central repository, usually the most secure container, should be designated to hold the sealed SF 700 for use during emergencies. Only appropriately authorized employees should be given access to a combination. Combinations shall be controlled in the same manner as keys.

9.3. ELECTRONIC LOCKS

9.3.1. Electronic lock access control systems use a card key programmed with a particular code which is read by a card reader that communicates with an automated central or local processor for access control. The card reader obtains data from the card by reading punched holes, magnetic strips or spots, imbedded wires, or any of several other methods. To open a door or activate a turnstile or lock, the card is typically inserted into a slot or groove and the coded area is read by the reader. If the code is an authorized one, the processor will direct the lock to open. Key cards shall be voided in the system when lost, stolen, or when access is no longer required and the card recovered.

9.4. BIOMETRIC SYSTEMS

9.4.1. Biometric locking systems are available that use neither keys nor combinations. These include locks which open by using one of eight primary categories of biometrics technology: fingerprints, hand geometry, retinal scan, signature dynamics, voice verification, heat detection, facial recognition, or key stroke dynamics. These biometrics systems are primarily designed to control access to extremely sensitive, special-use areas where positive personal identification is an operational necessity.

9.5. KEYS

9.5.1. General

- This establishes the CBP policy and procedures for a standardized approach to the key management program, including administrative oversight, accountability, issue, receipt, duplication, replacement and documentation. This policy applies to all keys, all spaces, office equipment, vehicles, padlocks, lockers or other assets owned and operated by DHS/CBP;

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- Directives and guidance for the key management program include the following:
 - The Homeland Security Act of 2002, PL 107-296, enacted 11/25/02;
 - Department of Justice Vulnerability Assessment of Federal Facilities, June 1995;
 - Department of Defense Lock Program, UG-2040-SHR, July 2000;
 - MD 11000 Office of Security;
 - MD 11030.1 Physical Security of Facilities and Real Property; and
 - MD 11049 Security Violations and Infractions.

9.5.2. Key management and oversight helps protect life, property and provides a level of security to facilities and all occupants. Keys are the property of DHS and a part of physical security, which require strict control, management and accountability through keying systems integrity. Locks are the most common mechanism for access control on doors and security containers and often provide the primary protection against intrusion and theft. When a key is affected and/or compromised, the system is affected and compromised. Lack of an operational key control program can result in the compromise of personnel, property, and information. A functional key control program will ensure accountability; provide administrative oversight, and continuity of security through key issuance, duplication and replacement. Although a determined individual can open most key locks in a few minutes, they are used primarily to delay, discourage, or deter theft or unauthorized access. Exterior door locks shall at a minimum meet UL 437 standards.

9.5.3. The integrity of a key system is important to safeguarding property and controlling access. The security officer shall ensure that responsible individuals maintain control of the facility's key system by storing, issuing, and accounting for all keys. Issuance of keys must be kept to a minimum and only issued to persons who have an official need. Master keys must be carefully controlled; successful compromise of a master keyed installation can be very difficult and costly to remedy (assuming it is even discovered). Master keying systems can also incorporate a lock with a removable interchangeable lock core. Accurate accountability records must be kept and all key records and documentation will be maintained for no less than one year. When keys are no longer needed they will be destroyed and documentation verifying destruction will be maintained.

9.5.4. A facility master key inventory and log will be maintained for the purpose of chain of accountability and access control and will include as a minimum:

- The number assigned to each key and lock;
- How many keys per lock;
- Location of each lock, to include but not limited to room, container, or cage no.; and
- Access list of persons authorized to use master keys.

9.5.5. Computerized systems may be used

9.5.6. The Security Officer or Key Control Person will approve and monitor all requests for issuance of new, duplicate, or replacement keys and ensure appropriate documentation is completed.

9.5.7. Physical Protection of keys will include, but is not limited to:

- Keys can only be stamped with blind control codes.
- Blind codes must not be reflective of buildings, door numbers or offices.
- Duplicate keys must be kept to a minimum, and when made the Master Key Inventory will be updated with required information;
- Non-issued keys must be safeguarded and controlled within a locked cabinet or container accessed only by the Key Control Person; and
- The key storage cabinet or container will be locked when not in use.

9.5.8. Employee Protection of Keys

- DHS employees issued keys are to protect and secure them at all times, ensuring keys are not left on desks, in unlocked drawers, or where they can be easily taken and copied.
- Employees shall only use their keys to access their assigned work areas and shall lock doors when leaving any secured area;
- DHS employees assigned keys are not authorized to lend keys to individuals not specifically authorized;
- No person shall knowingly alter duplicate, copy or make a facsimile of any key to a lock of any building or property;
- The unauthorized possession, use or reproduction of any DHS key is a security violation; and
- A penalty shall be incurred for multiple losses.

9.5.9. Protection of Cores

- Excess cores will be secured in a locked cabinet or container and secured from unauthorized access;
- Excess cores will be inventoried; and
- Cores must not be removed by construction or other maintenance personnel.

9.5.10. Key Issuance

- A key issue form will be documented in every instance of a CBP key issue and contain as a minimum:
 - Building number, floor number, and room, container or cage number;
 - Key serial number;
 - Key identification code;
 - Quantity of keys issued;
 - Brief statement of key control responsibilities;

- o Printed full name of person issued key(s);
- o Organizational identifier of person issued key(s);
- o Signature of person issued key(s) acknowledging their key control responsibilities;
- o Printed name of person issuing key(s);
- o Signature of person issuing key(s); and
- o Date key(s) issued.
- No person shall be issued multiple keys for the same area;
- In no case shall the issuance of keys be authorized by the same person to whom the key is to be issued;
- Requirement for access does not constitute being issued a key, if other means are available for access. I.e., intercoms, request for entry, guards etc.;
- Keys shall be issued only to those individuals who have a legitimate and official requirement for the key;
- Keys are only issued to the occupant of the area, space or office or to a person they designate in writing; and
- Only the authorized recipient of an issued key may sign for that key and no other person.
- When assuming key control duties and responsibilities, the following minimum actions will be taken:
 - o All keys will be jointly inventoried every time a new key control person is assigned by both in-coming and out-going key control person and documented ensuring accountability;
 - o Inventory will be documented and both persons will sign accountability document; and
 - o Inventory will include both individual's name and signature, date of inventory, any discrepancies found and actions taken.

9.5.11. Key Return

- Keys will be returned to the Key Control Person upon the departure or reassignment of any person who was issued a key(s), and will not be given to any other individual for use or turn-in;
- Any person returning a key will complete their original key issued form which will contain as a minimum:
 - o The printed name and signature of person returning the key(s) and date;
 - o The printed name and signature of key control person receiving key(s) and date;
 - o Identification code of key(s) returned; and
 - o Identification of serial number(s) of key(s).

- Any employee issued official keys on a temporary basis shall promptly return them as ensured by the Key Control Person.

9.5.12. Loss/Damage/Destruction of Keys (Key Replacement)

- When a key to a designated controlled or restricted area is lost, the locks to that area must be changed, depending on risk, as soon as possible as old locks remain exposed until replaced;
- Lost or stolen keys must be reported immediately to the Key Control Person;
- Anyone reporting a lost or stolen key must provide written documentation to the Key Control person. This will include; date, time, circumstances of the loss, any key identification and any action taken to retrieve the key;
- Locks shall be re-keyed in a timely manner and new keys issued when keys are lost or stolen; and
- If a master key is lost, every master lock must be replaced and, depending how the keying is done, new keys distributed to the key holders.

9.5.13. Documentation

- Key and excess core inventory logs will be developed and maintained for a period of no less than one year after the life of the key system being used;
- Key access logs will be developed and maintained for a period of one year;
- A key issued form will be developed and utilized for key(s) issue and turn in. The form will be maintained until the key(s) are returned and for a period of no less than one year after the key(s) are returned; and
- All keys and excess cores will be secured and annually inventoried and documented.
- The DoD Lock Program can be referenced for documentation guidance. See [Section 9.1. LOCKS](#), above.





CHAPTER 10: SAFES AND STORAGE EQUIPMENT

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

10.1. PHYSICAL PROTECTION AND STORAGE OF MATERIALS

10.1.1. GSA-approved security containers may be utilized for the physical protection of Customs and Border Protection (CBP) information and property to include classified documents, components, materials, equipment, funds, valuables, weapons, jewelry, precious metals, etc. When such containers do not meet appropriate requirements for protecting specific types of information and property, appropriate written guidance shall be developed and approved by CBP Headquarters (HQ), Internal Affairs, Security Management Division (CBP/IA/SMD). Nothing in this policy handbook shall be construed to contradict or inhibit compliance with the law or building codes.

10.2. REFERENCES

- o [Executive Order 12829](#), National Industrial Security Program;
- o [Executive Order 12958](#), as amended, Classified National Security Information;
- o FF-L-2740 Locks, Combination;
- o FF-L-2937 Combination Lock, Mechanical;
- o General Services Administration (GSA) Website (<http://www.gsa.gov>);
- o AA-C-2737 Modular Vault Systems;
- o [Department of Defense Lock Program Website](#);
- o AA-F-358 Filing Cabinets, Legal and Letter Size, Uninsulated, Security;
- o AA-F363 Filing Cabinet, Security, Maps and Plans, General Filing, and Storage

10.3. CLASSIFIED INFORMATION

10.3.1. Classified information shall be secured under conditions adequate to prevent access by unauthorized persons. Requirements specified in this section represent acceptable security standards. Policy concerning the use of force for the protection of classified information is specified in [Chapter 12, Services](#), of this policy handbook. Weapons or sensitive items such as funds, jewels, precious metals or drugs, etc., shall not be stored in the same container used to safeguard classified information and property. Security requirements for Sensitive Compartmented Information (SCI) are established by the Director of Central Intelligence Directives. Contact CBP/IA/SMD for guidance on the storage of SCI and Special Access Program (SAP) material. Current holdings of classified material shall be reduced to the minimum required for mission accomplishment. Classified information that is not under the personal control and observation of an authorized person is to be guarded or stored ONLY in approved locked security containers, vaults, rooms or areas, as follows:

- TOP SECRET Information
 - o TOP SECRET information shall be stored by one of the following methods:
 - In a GSA-approved security container with one of the following supplementary controls:

- The location housing the security container shall be subject to continuous protection by cleared guard or duty personnel; or
- Cleared guard or duty personnel shall inspect the security container once every two hours.
- o The location housing the container must be protected using one of the following two methods:
- o An Intrusion Detection System (IDS) meeting CBP/IA/SMD standards outlined in [Chapter 8, Interior Protection](#), with a personnel response time to alarm within 15 minutes of the alarm annunciation or
- o A Security-In-Depth Determination (a determination by CBP/IA/SMD, that layered complementary controls are sufficient to deter and detect unauthorized entry), when the GSA approved container is equipped with a lock meeting [Federal Specification FF-L-2740](#).
- o With written approval from CBP/IA/SMD, Top Secret material may be stored in a modular vault, vault, or a secure room (Open Storage) constructed in accordance with Chapter 8, Vaults, and equipped with an IDS with the personnel responding to the alarm within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth, or a 5 minute alarm response time if it is not.

10.3.2. SECRET Storage.

- SECRET material shall be stored by one of the following methods:
 - o In the same manner as prescribed for Top Secret information;
 - o In a GSA-approved security container or vault without supplemental controls; or
 - o Until October 1, 2012, in a safe, steel file cabinet or safe-type steel file container that has an automatic unit locking mechanism.
- All such receptacles will be accorded supplemental protection during non-working hours.
 - o Until October 1, 2012, in any steel file cabinet that has four sides and a top and bottom (all permanently attached by welding, rivets or peened bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key operated or combination padlock. The keepers of the rigid metal lock bar shall be secured to the cabinet by welding, rivets, or bolts, so they cannot be removed and replaced without leaving evidence of the entry. The drawers of the container shall be held securely, so their contents cannot be removed with forcing open the drawer. This type of cabinet will be accorded supplemental protection during non-working hours.

10.3.3. CONFIDENTIAL Storage.

- CONFIDENTIAL material shall be stored in a manner prescribed for the storage of Top Secret or Secret, without supplementary controls.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

10.3.4. BULK Storage

- Bulk Storage of classified material requires prior approval of the CBP/IA/SMD.

10.3.5. Storage of Sensitive-but-Unclassified Information

- Sensitive and/or Limited Official Use (LOU) information must be stored in a room or area affording sufficient physical and personnel access control and preventing unauthorized access, such as a locked room. If a locked room does not afford sufficient protection against unauthorized access, then at a minimum, materials will be further secured in:
 - o Key-lock metal cabinets;
 - o Locked desk drawer

10.3.6. All unclassified information not otherwise designated as LOU shall be stored in accordance with office policy and procedures, where applicable.

10.3.7. Storage of secure forms, stamps, ink and other related materials should refer to [Chapter 18, Secure Items](#).

10.3.8. Specialized Security Equipment

10.3.9. Specialized security equipment shall address unique requirements and may be approved by CBP/IA/SMD in certain situations. When approved by CBP/IA/SMD the following apply:

- o One and two-drawer Service Approved Security Containers which are securely fastened or guarded to prevent theft of the container, may only be used in mobile facilities or in areas where small amounts of classified information are stored;
- o GSA-approved “Map and Plan” Service file container may be used for storage of odd-sized items such as computer diskettes or tapes, maps, charts, plans, and other media containing classified information; and
- o GSA-approved modular vaults meeting Federal Specification AA-V-2737 may be used to store classified information. See the [Appendix 8.6, Vaults](#) for more detailed information.

10.4. SUPPLEMENTAL PROTECTION

10.4.1. Intrusion Detection Systems (IDS), as described in [Chapter 8, Interior Protection](#), shall be used as supplemental protection.

10.4.2. Approved security guards may be utilized. When guards are authorized, the patrol schedule is 2 hours for TOP SECRET material and, 4 hours for SECRET material.

10.4.3. GSA-approved security containers and approved vaults secured with a locking mechanism meeting Federal specification FF-L-2740, located in an area of the facility with in-depth security as determined by CBP/IA/SMD, do not require supplemental protection.

10.4.4. All GSA containers used to secure classified materials, information, equipment,

weapons, and other valuables, must be housed in areas that will provide security from removal of containers and disclosure of information/material.

10.5. GSA-APPROVED SECURITY CONTAINERS

- 10.5.1. GSA establishes and publishes minimum standards, specifications, and supply schedules for all containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information, material, and property.
- 10.5.2. GSA-approved security containers are primarily used to store classified documents, components, materials, and equipment. They are also used to secure funds, valuables, and weapons.
- 10.5.3. There are two classes of GSA-approved containers currently being manufactured: Class 5, and Class 6.
- 10.5.4. Classified and non-classified materials shall never be stored together.
- 10.5.5. GSA-approved containers must have a GSA label affixed to the front of the door, the front of the top drawer, or the front of the control drawer. If the container no longer has the GSA label attached to it, it is no longer an approved container. If your container is no longer approved, see "Container Recertification" [section 10.13](#). GSA-approved containers manufactured before October 1990 are identified by their GSA label that has either black lettering on a silver background (or silver lettering on a black background). Since October 1990, only Class 5, 6, and 7 containers have been manufactured. GSA-approved Class 5 and 6 containers manufactured after October 1990 have a silver label with red lettering (or red with silver lettering). GSA-approved Class 7 containers have a silver label with green lettering. Class 7 containers were available in filing cabinet style only and are no longer manufactured. Information Processing System (IPS) containers are GSA approved containers for protection of computers. Their GSA approval labels have blue lettering.
- 10.5.6. Class 5 and 6 Approved GSA Containers
- Class 5 Containers are typically used for the storage of weapons and sensitive items such as funds, jewels, precious metals, etc. However, funds, jewels, precious metals, etc. shall not be store in the same container as weapons. Class 5 containers may also be used for the storage of classified documents, components, materials, and equipment. They provide the same protection as Class 6, plus ten minutes against forced entry attack. Class 5 containers come in several types: file cabinet, map and plan, weapon storage, COMSEC, and (IPS);
 - Class 6 Containers are typically used for storage of classified information such as documents, maps, drawings, and plans. They come in file cabinet and map and plan styles.

10.6. WEAPONS STORAGE

- 10.6.1. Weapons shall be stored in Class 5 or 6 GSA-approved containers instead of vaults or armories when authorized for storage.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- Class 5 is preferred for weapons storage because of the different styles of containers;
- There are several styles of Class 5 containers that can be used for weapons storage; and
- The Class 5 GSA-approved container is available with various drawers, adjustable shelves, and in weapons configurations for either rifles or handguns. When selecting a container, the appropriate style shall be procured for adequate safety and protection. A complete listing of types and styles of Class 5 and 6 GSA-approved containers can be found on the Federal Specifications and Qualified Products Lists (QPLs) provided on the [DoD's Lock Program Web site](#).

10.6.2. Class 5 security containers authorized for weapons storage must be adequately protected. The following factors must be considered for each container:

- Vulnerability when left unattended for extended periods of time;
- Vulnerability of the location where the container is placed;
- Accessibility and ease of removal of the container;
- Position where the container will be least vulnerable to unauthorized access by heavy lifting equipment (e.g., forklifts or dollies);
- Position from which unauthorized persons would find it extremely difficult to remove the container;
- The positive overall security of the arms stored in the container must be achieved. Regional Security Officers will ensure that structure protection provided by the storage container is adequately increased by the physical security measures specified in this policy handbook.
- Class 5 – Approved Weapons Container
 - Class 5: - 53 1/4" H x 22 1/2" W x 39 1/4" D;
 - Standard colors are gray, black, and parchment;
 - Group 1 lock or X-09 lock;
 - Casterbase does not come standard;
 - Interiors:
 - Weapon drawer
 - Correspondence drawer
 - 9MM Beretta Pistol rack
 - 45 & .38 Caliber Pistol rack
 - Adjustable shelf
 - Security lock
 - Universal and State Department rifle cart
 - Standard color is parchment
 - Drawer Dividers

- Drawer Liner

- For more information on storage of weapons and ammunitions, see [Chapter 16. Weapons and Ammunition](#).

10.7. RECORD SAFES DESIGNED FOR FIRE PROTECTION

10.7.1. A labeling system has been established by the Underwriters Laboratory (UL) to define the level of fire protection each safe can be expected to provide. Prior to 1972, the UL designations used an alpha designation that was the same as Safe Manufacturers National Association (SMNA). Both the former UL and SMNA designations are provided, along with the current equivalent UL designation. Fire protection container manufacturers and prices of equipment approved by the GSA are listed in FSS Group 71 Part III.

10.7.2. Burglary-Resistant Safes

- Containers designed for burglary protection are classified in accordance with test data and specifications that conform to requirements of the UL. burglary-resistant equipment will resist an attack by tools, torch, or explosives in proportion to their construction specifications. Burglary-resistant container manufacturers and prices of equipment approved by the GSA are listed in the FSS Group 71 Part III.

10.8. COMBINATION LOCKS

10.8.1. DHS/CBP uses two types of mounted combination locks, one for the protection of classified materials and one for the protection of weapons and ammunition. Combination locks that protect classified material must meet the requirements of Federal specification [FF-L-2740, Locks, Combination](#). Combination locks protecting weapons and ammunition must meet the requirements of Underwriters Laboratories Inc. Standard For Combination Locks UL 768, Group 1.

10.8.2. See [Chapter 9.2](#) for CBP policy on when to reset combinations.

10.8.3. Three locks have been approved under FF-L-2740 for the protection of classified materials.

- The model X-07 lock was approved in November 1991;
- The X-08 in March 1999; and
- The X-09 in June 2002.

10.8.4. GSA-approved security containers and vault doors for the protection of classified material have had FF-L-2740-compliant locks installed at the time of manufacture since March 10, 1992.

10.8.5. GSA-approved weapons containers and armory vault doors are available for the protection of arms, ammunition, and explosives. Mechanical combination locks that resist manipulation attempts for 20 man-hours are UL-listed as Group 1.

10.8.6. Pedestrian door dead bolts covered by Federal specification [FF-L-2890, Lock Extension \(Pedestrian Door, Dead bolt\)](#) are intended for use on interior pedestrian doors used for normal entrance and egress during day-to-day operations. Three

[RETURN TO TOP](#)

locks have been approved under FF-L-2890: the model CDX-07 door lock was approved in November 1991, the CDX-08 in March 1999, and the CDX-09 in June 2002. While the CDX-07 and CDX-08 are still approved for securing classified material, they are no longer being manufactured.

- 10.8.7. Combination padlocks under the [FF-P-110](#), Padlock, Changeable Combination Federal specification are intended for low level resistance to forced entry and high level tell-tale manipulation or surreptitious action. The padlocks are intended for use ashore and aboard ocean going vessels, indoors, or outdoors, semi-protected by a structural overhang similar to eaves or a lean-to.

10.9. REPLACEMENT OF UNAPPROVED STORAGE CONTAINERS

- 10.9.1. No non-security filing cabinets or containers in use or presently on the market have been approved for the storage of classified information. As cited in [Executive Order 12958](#), Classified National Security Information, Directive on Safeguarding Classified National Security Information, dated August 4, 1999, only GSA-approved Class 5 or Class 6 security filing containers are authorized for the storage of classified National Security Information.
- 10.9.2. In the past, a number of filing cabinets, equipped with locking bars and secured with combination padlocks, and security storage containers equipped with built-in combination locks, manufactured prior to the GSA-approval process, were conditionally authorized for storing classified information. Executive Order 12958, Classified National Security Information, Directive on Safeguarding Classified National Security Information, dated August 4, 1999, rescinds all previous conditional authorizations for containers storing classified information.
- 10.9.3. Security Officers and custodians must immediately replace these previously approved containers with GSA-approved Class 5 or Class 6 security containers. The expense of purchasing new security containers can be substantially lessened by taking practical steps to reduce the need for classified storage containers, as suggested below.
- 10.9.4. Conduct clean-out campaigns to remove unnecessary classified and other unclassified documents from containers. Excess material shall be archived or destroyed, as appropriate, and retained classified shall be moved into approved containers.
- In most offices, classified documents usually constitute a very small percentage of the documents in a given container. Remove classified files from existing non-approved containers and consolidate them in approved security cabinets. The non-approved cabinets can still be used for storing unclassified files;
 - Explore the requisitioning of approved containers through surplus channels before purchasing new equipment.

10.10. DEFECTIVE GSA-APPROVED SECURITY FILING CABINETS

- 10.10.1. After initially receiving GSA approval, a number of security containers have been

[RETURN TO TOP](#)

identified that require either the removal of the GSA approval label or must be repaired to eliminate a security hazard. The following Art Metal and Hamilton products shall be handled as indicated below:

- *Art Metal Products Inc.* The GSA-approval label must be removed from all two- and four-drawer, Class 5 security filing cabinets made by the Art Metal Products Inc. These containers shall not be used for storage of classified materials;
- *Hamilton Products Group, Inc.* Four- and five-drawer, Class 6 security filing cabinets made by this manufacturer prior to July 1988, are subject to defects. The defects allow the control drawer to be locked while another drawer is open. These cabinets must be checked without exerting excessive force on the control drawer handle to ensure that it cannot be locked with other drawers open. If it is possible to lock the cabinet with less than 10 foot-pounds of torque, a modification to the cabinet is required. Security officers who determine it necessary to retrofit a container must contact a local locksmith for repairs. Cabinets that are found to allow the locking, but are not repaired shall have the GSA-Approved label removed.

10.11. MAINTAINING GSA-APPROVED SECURITY CONTAINERS

10.11.1. General maintenance on GSA-approved security containers is recommended every 5 years. A trained and certified locksmith should be retained to examine and service security containers with built-in combination locks. Containers used for the storage of classified materials will be examined and repaired only by a cleared locksmith or under the constant supervision of a cleared person.

10.12. REPAIRING APPROVED SECURITY CONTAINERS

10.12.1. This section establishes procedures for the neutralization and repair of GSA-approved containers and vault doors; the information provided herein is derived from FED-STD 809A, and details unclassified procedures to neutralize and repair lockouts on GSA-approved security containers and vault doors in a manner allowing retention of the GSA approval. The terms used in this section are commonly understood by the technical community to which they apply, and are not used here in such a way as to introduce new or limited meanings.

- Individuals who repair or drill security containers, vault doors, and padlocks shall be cleared for access to the highest level of classified information stored within the container, or must be escorted and continuously watched while working on the container. Individuals must also be properly trained and certified in repairing GSA-approved containers.

10.12.2. General Requirements

- Determine if products are under warranty before attempting neutralization procedures on containers or vault doors. Only products with red or blue labels may be under warranty; red or blue label products more than a year old are not under warranty. Contact the manufacturer concerning warranty provisions; provide the serial number and description of container. GSA contracts require

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

manufacturers to provide warranties generally one year from the date of manufacture. During that time, if a lockout occurs due to failure of the locking system, the Government has the right to require the container manufacturer to provide access to the container contents within 24 hours. This provision applies in the continental US (CONUS) only. Contact GSA for further information regarding warranty provisions at www.gsa.gov. Neutralization of lockouts or repairs of any damage affecting the integrity of a security container approved for storage of classified material shall be done only by authorized or continuously escorted personnel specifically trained in the approved methods.

10.13. RECERTIFICATION OF GSA-APPROVED CONTAINERS

- 10.13.1. GSA-Approved Security Equipment Inspection/Recertification Training is now available through the [DoD's Lock Program](#).
- 10.13.2. GSA-approved containers and vault doors are products that have been designed, built, tested, and verified as meeting the requirements of Federal specifications. GSA researches and develops those specifications for the Federal government. Only products that have passed all GSA testing to the requirements of a designated Federal specification may bear the label "General Services Administration Approved." The manufacturer attaches the label to the container.
- 10.13.3. Since the early 1960s, security equipment approved by GSA has had an external label indicating approval. That label has been the designation of security equipment authorized for storage of classified material and, more recently, of equipment for storage of arms, ammunition, and explosives.
- 10.13.4. It is standard practice to remove the label if an approved container is opened, repaired, or otherwise modified in an unauthorized manner. A missing label indicates that a container may not have its original security integrity. However, the label may be missing for another reason. The label may have fallen off or may have been removed for a reason unrelated to the container's security integrity.
- 10.13.5. All maintenance and service activity of a container, including the reason the approval label is missing, shall be designated on the Security Container Records Form. If this has not been done, the container's security integrity may be vulnerable.
- 10.13.6. Containers modified from the original manufacturer's product, or damaged or improperly opened, may not be recertified unless returned to their original condition. This may require replacement of parts with new or salvaged OEM parts, or repair in accordance with Federal Standard 809.
- 10.13.7. This policy has been sent to all Federal agencies for incorporation into their relevant security regulations.
- 10.13.8. The figure below is an example of recertification labels from MBA USA (top) and Lockmasters (bottom). The container manufacturer's name will appear on a sticker in the center of the label. The color of the label will be indicated by a punch in the circle above the appropriate word.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Figure 1: Recertified Container Labels



- 10.13.9. More information on the GSA Security Equipment Inspection Program can be found at the [Department of Defense Lock Program](#) site.
- 10.13.10. Contact the Lock Program Technical Support Hotline, (800) 290-7607, if you have any questions about the inspection and recertification process.





CHAPTER 11: ACCESS TO FACILITIES

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

11.1. GENERAL

- 11.1.1. This chapter establishes the policy for access to CBP facilities, and limits the establishment of facility entry controls to those necessary for the safety of CBP employees and the protection of Government property and information.
- 11.1.2. This standardized approach will address accessing CBP facilities utilizing identification, cards, Photo Access Cards (PAC), other agency passes and credentials, X-Ray, magnetometer, irradiation screening devices and admittance to CBP facilities.

11.2. DEFINITIONS

- 11.2.1. **Badge:** An emblem (a small piece of plastic, cloth or metal) that signifies the bearer's status, rank or membership or affiliation. A device, patch, or accoutrement which is presented or displayed to indicate some feat of service, a special accomplishment, a symbol of authority (e.g., police), a simple means of identification. Also referred to in FLETC policy as a badge.
- 11.2.2. **CFR:** Code of Federal Regulation
- 11.2.3. **Credentials:** Documentation usually consists of an identity card, badge or a shield, etc., issued by a trusted third party after some form of identity verification. Credentials are utilized as identification showing that an individual is entitled to represent, or exercise official power as, part of a United States Government Agency.
- 11.2.4. **Designated Official:** The highest ranking official of the primary tenant agency of a Federal facility or, alternatively, a designee selected by mutual agreement of tenant agency officials. For facilities owned and leased by the U.S. General Services Administration (GSA), the definition appears in [41 CFR §102-71.20](#), of the Code of Federal Regulations.
- 11.2.5. **FIPS 201:** Federal Information Processing Standard (FIPS) 201, entitled Personal Identity Verification of Federal Employees and Contractors, was developed to satisfy the requirements of HSPD 12, which is comprised of two (2) specific components PIV-I and PIV-II. FIPS 201 requires that the PIV card be a smart card and the card body is similar to a bank credit card conforming to the [ISO/IEC 7810](#) specification.
- 11.2.6. The card must contain both contact and contactless interfaces, which may be provided by two separate integrated circuit chips (ICC) or by one dual-interface ICC. The contact interface must conform to the [ISO/IEC 7816-4:2005](#) specification
- 11.2.7. The contactless interface must conform to the [ISO/IEC 14443](#) specification.
- 11.2.8. In most cases, physical access applications will use the contactless interface, although there are special cases in which the contact interface will be used for physical access. This is according to the [NIST FIPS 201 PDF](#), the Standard Publication for Personal Identity Verification (PIV) of Federal Employees and Contractors.
- 11.2.9. [HSPD-7:](#) Homeland Security Presidential Directive 7 instructs Federal departments

and agencies to prepare plans for protecting physical and cyber critical infrastructure and key resources (CI/KR), owned or operated, including leased facilities by July 31, 2004.

- 11.2.10. [HSPD-12](#): Homeland Security Presidential Directive 12 establishes a policy for a common identification standard for Federal employees and contractors and mandates the establishment of a “mandatory Government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors”.
- 11.2.11. **IDMS**: Personal Identity Verification Identity Management System. A system comprised of one or more systems or applications used to manage the identity verification, validation, and issuance processes. A DHS/HQ central data base used to house personal identifiable information for all DHS employees and contractors.
- 11.2.12. **Internal Affairs Background Investigation Database (IABI)**: A CBP database utilized by CBP/PSD to input CBP personnel’s employment, suitability and clearance status for verification purposes by CBP Security personnel.
- 11.2.13. **Magnetometer**: An electronic device used specifically to search personnel for hidden metallic weapons (knives and guns) at entrances to airports, public schools, courthouses, and other guarded spaces. When used with access control equipment, they can perform two functions:
- (1) Detect the presence of concealed metal objects;
 - (2) Determine the size of those objects.
- Metal is detected by measuring the change in an established magnetic field when dense metal or ferrous materials are moved through the field. The antenna of a detector sets up a magnetic field around itself. As the antenna of the detector is brought near metal or metal is moved past the antenna, the pitch from a tone generator increases, thereby alerting the operator to the presence of metal. Measurement capabilities are adjustable allowing for varying the amount of metal desired to be detected.
- 11.2.14. **Photo Access Card (PAC)**: A PAC is a physical artifact, a plastic card issued by CBP to employees, contractors and detailees, which allow the bearers, authorized access to CBP Facilities.
- 11.2.15. [PIV-I](#): Specifies the minimum requirements for a Federal Personal Identification Verification (PIV) system that meets control and security objectives of [PIV-I](#), including the personal identity proofing process. PIV was defined by [NIST](#), the National Institute of Standards and Technology, an agency of the U.S. Commerce Department’s Technology Administration dealing with the performance of background checks for employees and contractors.
- 11.2.16. [PIV-II](#): Provides detailed technical specifications of components and processes required for interoperability of PIV cards with personal authentication, access control, and PIV card management systems across the Federal government and the issuance of smartcards.

- 11.2.17. Radiation Detector:** An electronic device used specifically to search for radioactive materials hidden in cargo or vehicles. Radiation detectors fall into two categories: gross counters and energy sensitive. Gross counters count each event (gamma or neutron) emission the same regardless of energy. Energy sensitive detectors -- used in radio-isotope identification devices (RIIDs) -- analyze a radioactive isotope's distinct gamma energy emissions and attempt to identify the source of the radiation. There are several manufacturers of radiation detectors and they use various technologies to measure radiation from containers, objects or people. Some radiation detectors are small hand-held electronic devices and others are large portal monitors that scans vehicles and cargo as they pass through.
- 11.2.18. Security Liaison (SL):** The individual responsible for coordinating compliance with the implementation of CBP security programs through the District Security Officer/ Regional Security Officer and serve as the primary point of contact for all security issues in the their facilities.
- 11.2.19. Visitor:** Any person who is not a DHS or CBP Federal employee or DHS or CBP contractor with current DHS or CBP suitability and issued a DHS or CBP Photo Access Card (PAC).
- 11.2.20. X-ray system:** A device or system that inspects the contents of a package or container for concealed explosives or contraband. Some systems can only detect objects made of materials possessing high atomic numbers, such as steel, tin, aluminum, and iron. Other systems can detect materials with both high and low atomic numbers. Some systems have two monitors, one for objects with high atomic numbers and one for objects with low atomic numbers. Color systems presently available use only one monitor to view both types of materials. Specific colors are assigned to high and low atomic number materials.

11.3. AUTHORITY

- [Privacy Act of 1974](#)
- [E-Government Act of 2002](#)
- [Homeland Security Presidential Directive 12 \(HSPD-12\)](#), August 2004.
- [Federal Information Processing Standard 201: Policy for a Common Identification Standard for Federal Employees and Contractors](#), February 2005.

11.4. GENERAL

- 11.4.1. Entry control facilities provide the first public impression of CBP. They will present the proper appearance for visitors, employees, and DHS personnel. The layout, landscaping, and architecture of the facilities are factors in this image. The architectural design of the facilities will comply with CBP's architectural design standards.

11.5. RESPONSIBILITIES

- 11.5.1. The Security Officer will ensure that all persons entering and exiting any CBP facility will adhere to access and egress procedures established in this handbook.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- Employees
 - All CBP Federal employees and contractors (including guards, maintenance, and cleaners) will complete a favorable suitability-to-be-authorized and issued a CBP identification prior to entering and/or performing any authorized work in a CBP owned or leased facility:
 - The CBP office of security will conduct federal, state and local criminal and warrant checks on cleaning force personnel and answering service employees;
 - New cleaning personnel and answering service employees must be checked prior to their utilization;
 - All names should be rechecked annually;
 - Cleaning personnel or answering service employees are to provide photo identification each time they enter the premises to perform their duties; and
 - The CBP office of security will issue standardized contractor PACs.
 - Photo access card (PAC) identification carriers are responsible to:
 - Maintain control of the issued photo access card (PAC) identification.
 - Safeguarding the photo access card (PAC) identification badge from loss or misuse,
 - Immediately report any lost or stolen photo access card identification badge; and
 - Notify his/her supervisor in writing of the circumstances surrounding the lost/stolen badge or credential. Follow OIA/CBP guidelines to report a lost/stolen badge of credential; the guidelines can be found at [the CBP web page](#).
 - Employees who have lost or forgotten their photo access card (PAC) identification or other issued CBP facilities issued access badge will be issued visitors identification after that employee has been verified in the CBP personnel security database;
 - Photo access card (PAC) identification will be relinquished by all employees, who shall, prior to resignation, termination; retirement, transfer etc., Complete [Form CBP-242.PDF](#) the issuing official will annotate the appropriate control log or automated system indicating return of the CBP national region photo access card (PAC) identification badge or other issued CBP facilities issued access badge.

11.5.2. The Designated Official will:

- Ensure compliance with minimum CBP security requirements as determined by IA/SMD;
- Establish additional protection requirements for facilities and space under their control as long as these procedures conform to the policy established by this

chapter;

- Develop and implement adequate procedures to protect CBP employees and property;
- Determine normal working hours and non-working hours for the facility;
- Determine if special access controls to the facility are necessary during normal working and non-working hours, and if they are necessary, establish only the minimum controls required;
- Coordinate and establish these special access controls and other protection requirements with GSA if the building is operated or leased by GSA; and
- The Designated Official or Security Liaison will determine if it is necessary to establish additional access controls to the facility during normal working hours:
 - o Access controls may be enhanced if the Designated Official or Security Liaison determines that there is a threat to harm employees, to steal Government property, or to gain unlawful access to information which is protected against unauthorized access by Government rules or regulations.

11.5.3. Designated Officials and Security Liaisons are responsible to ensure that the physical security policies and procedures applicable to individual program activities are adhered to by all employees.

11.5.4. Designated Officials or Security Liaison of a CBP owned facility establish and maintain physical security, predicated on programmatic requirements, if any, to protect:

- Government property;
- Records; and
- The well-being of service employees.

11.5.5. Designated officials or security officer of both CBP-owned and GSA-leased space ensure staff compliance with all applicable policies and procedures in safeguarding and protecting:

- Government personal property;
- Seized property (if applicable);
- Government records (personnel, classified documents, etc.); and
- ADP security requirements.

11.6. ACCESS CONTROL

11.6.1. At a minimum, access control systems will comply with [HSPD-12](#), [FIPS 201](#) policies, Government Smart Card Interoperability Specification ([GSC-IS V2.1](#)) and [Schedule 70 for Products and Service Components](#).

11.6.2. CBP/IA/SMD determines the necessary access control and systems for all CBP facilities based on the requirements of [HSPD 12](#) and [FIPS 201](#). Planning is required to include:

[RETURN TO TOP](#)

- Establishment of a system for positive identification of personnel and equipment authorized to enter and exit the facilities; and
 - Maintenance of adequate physical barriers that will be deployed to control the facilities.
- 11.6.3. The number of entrances will be kept to a minimum and each entrance must be controlled.
- CCTV will provide surveillance of all access control operations to include the access control area, vehicle search areas, final denial barriers, and pedestrian access points.
 - For further information, see [Chapter 8, Interior Protection](#).
- 11.6.4. The senior CBP official where a badge system is implemented is responsible for oversight and administration of the badge program. Personnel and equipment must be provided to properly administer a badge system.
- Planning will also include increasing vigilance and access restrictions during higher threat levels.
- 11.6.5. Basic requirements for admission to Federal property are contained in [41 CFR §102-74 et. seq.](#) Accordingly, during business hours, areas of CBP facilities are normally open to the public and only restricted to authorized individuals after business hours.
- During business hours, property or portions thereof can be closed to the public only when situations require this action to ensure the orderly conduct of CBP business. The decision to close the property or portions thereof to the public will be made by the designated official under the Occupant Emergency Program after consultation with the building manager and the responsible Security Liaison.
 - When property or a portion thereof is closed to the public:
 - Admission will be restricted to authorized persons who will register upon entry to the property;
 - Authorized persons will display a CBP photo access card (PAC) identification badge or issued visitor's identification while in the facility;
 - It will be designated as a restricted or closed area:
 - The decision to designate areas as either a “controlled area” or a “restricted area” will be made in conjunction with a decision to close the property or a portion thereof to the public.
 - Admittance to a controlled or restricted area will be limited to persons who have official business within that specific area.
- 11.6.6. Public access control (PAC) points and entry control facilities (ECF) act as a monitoring and clearance areas ensuring the proper level of access control for all personnel, visitors, and commercial traffic. The objective of a PAC and ECF is to ensure:
- Only authorized personnel and/or vehicles have access to specific facilities and/or areas;

- A level of protection from unauthorized access is provided; and
- Interception of contraband, such as weapons, explosives, drugs, classified material, etc.

11.6.7. Public access areas are areas within the building where services are provided to the general public:

- Uncleared persons may enter these areas without escort but will be properly screened prior to admittance;
- The public access control area (normally in the main entrance lobby of the building) will provide for screening of visitors and employees before admittance into CBP controlled areas/space; and
- The public access control operations can consist of a screening area, a [walk-through metal detector \(WTMD\)](#) or [hand-held metal detector \(HHMD\)](#), a guard, controlled doors, a controller, and a security receptionist.

11.6.8. All forms of issued DHS and CBP identification are the property of the U.S. Government and may be retrieved at any time by the issuing official or security authority for just cause including, but not limited to:

- Any unauthorized use, including use for other than official or authorized purposes;
- Altering the badge/card or pass in any manner from original issued condition;
- Repeated loss; and
- Failure to display while in facility.

11.7. GSA-OPERATED OR LEASED FACILITIES

11.7.1. IA/SMD in conjunction with the Federal Protective Service (FPS) will determine the normal level of protection necessary to control entry to GSA-operated facilities. If access controls during normal working hours are necessary according to the policy of this order; the access procedures will be developed in conjunction with GSA.

- GSA will determine the security hours access control procedures in conjunction with the Designated Official.

11.7.2. The FPS is responsible for providing facility perimeter physical security predicated on programmatic needs at all facilities leased to Federal agencies.

11.7.3. Specific information and details pertaining to the administration of security in each of these discrete security areas should be included in the Site Security Plan/Program.

- General Services Administration's (GSA) responsibilities for the protection of life and property in federally owned and leased buildings and the responsibilities of those occupying these facilities;
- Except as otherwise ordered, property shall be closed to the public after normal working hours. During normal working hours, property shall be closed to the public only in emergency situations when reasonably necessary to ensure the orderly conduct of government business. The decision to close a property shall

[RETURN TO TOP](#)

be made by the designated official under the facility site security plan/program;

- For buildings and grounds for which the GSA has space assignment responsibility, GSA will furnish as normal protection not less than the degree of protection provided by commercial building operators of similar space for normal risk occupants, as determined by GSA; and
- Occupants of GSA assigned space shall cooperate to the fullest extent possible with all pertinent facility regulations and procedures, and shall make recommendations for improving protection.

11.8. NON-GSA OPERATED OR LEASED FACILITIES

11.8.1. When CBP elements occupy facilities not under GSA control, the IA/SMD will determine if access control procedures are in accordance with the policy of this chapter.

11.8.2. Dissemination of Access Control Information: When access controls are implemented, the Designated Official will:

- Publicize access control procedures to all facility occupants;
- Make procedures available at each access control point for review by those wishing access to the facility;
- Provide written access control procedures to each guard post or receptionist, defining responsibilities and procedures; and
- Install signs at all facility entrances announcing that access to the facility is controlled.

11.8.3. CBP Offices

11.8.4. All CBP offices located outside the National Capital Region will utilize their own distinct CBP access card or badge for their facilities. CBP employees and CBP contractors and will:

- Request approval from CBP/IA/SMD in writing to issue their facility access cards/badges. At a minimum the request will:
 - o Provide detailed access card/badge description;
 - o Submit a copy of facilities access badge/pass procedures.
- Receive authorization in writing to issue facility Access Card/badge from CBP/IA/SMD.

11.8.5. CBP offices receiving authorization to issue access cards/badges will have written procedures in place for the administration, issuance, reporting of lost, stolen or destroyed of their facility access cards/badges.

11.9. PHOTO ACCESS CARDS (PAC)

11.9.1. The PAC should be kept in a safe place which is convenient enough to ensure that it will be brought to work. A good rule of thumb is to afford the PAC the same protection given to credit cards. DO NOT write Personal Identification Numbers on

the PAC.

- 11.9.2. The CBP Photo Access Card (PAC), identification badge, or other CBP facilities issued access card is not for official identification and will never be used outside of a CBP or other government facility for the purpose of personal identification.
- 11.9.3. Blank stock of any CBP PACs will be secured in a locked container and remain under the positive control of the issuing official.
- 11.9.4. Each issuing official will maintain detailed accountability records of all PACs, to include:
- Issuance;
 - Returns;
 - Loss;
 - Destruction;
 - Unused stock on hand; and
 - Confirmation of suitability.
- 11.9.5. Destroying CBP PACs
- All CBP PACs will be returned to the issuing office for destruction;
 - All issuing offices are responsible to develop destruction control processes which will include as a minimum:
 - Maintain log with card holder's name, card number and date returned and date destroyed;
 - Destruction logs will be maintained for a period of no less than 5 years;
 - All identification pass/badges will be destroyed by shredding, utilizing a GSA approved shredder.

11.10. VISITORS

- 11.10.1. Control of the internal movements of personnel within a facility is necessary to ensure that only authorized persons are permitted in secured areas and that visitors do not wander through the facility unescorted.
- 11.10.2. All visitors will be issued a visitor's badge/card or pass for the purpose of escorted or unescorted authorization to visit in a CBP controlled facility/space/area. Each facility will establish an internal Visitor Control procedures and criteria for visitor badging and maintain positive control of all visitors, as a minimum:
- A unique visitor's temporary or hard badge/card or pass will be developed indicating:
 - Name of facility;
 - Visitor badge/card or pass number; and
 - Visitor escort or unescorted status.
 - Visitor badge/card will be strictly controlled and inventoried;

- Visitor badge/card issuance shall not exceed 12 hours;
- Visitor's logs will be maintained indicating, as a minimum:
 - Visitors' time in and time out;
 - Visitor's full name printed and their signature;
 - Visitor's government-issued photo ID source for identification purpose;
 - Visitor's company/organization and contact number;
 - Visitor badge/card or pass number;
 - Sponsor's full name printed and their signature; and
 - Sponsor's contact number.

11.10.3. The CBP Visitor's identification badge/card or pass will be used for identification purposes only within CBP facilities where it was issued. A visitor badge/card or passes is required and the type utilized is based on the need of the facility and at the discretion of the DO to facilitate the entrance of employees and visitors requiring access into a CBP facility/space or area when the visitor is not authorized to receive of a Photo Access Card (PAC) identification badge.

- Types of visitors badges/cards or passes:
 - Disposable badge/card or pass;
 - Hard badge/card or pass;
 - Unescorted badge/card or pass; and
 - Escort required badge/card or pass
- Persons who may require a visitor badge/card or pass may include, but are not limited to:
 - Employees;
 - Visitors;
 - Construction workers;
 - Maintenance workers;
 - Vendors;
 - Friends, family; and
 - Foreign nationals.

11.10.4. Only a CBP employee, detailee or contractor with a CBP National Capital Region Photo Access Card (PAC) identification badge or other CBP facilities issued access badge can sponsor a visitor into a CBP facility.

- Sponsors are responsible for the control and conduct of their visitor(s) while the visitor(s) is on site;
- The CBP employee who signed the visitor in is ultimately responsible for their visitor even if they have turned control of the visitor over to another CBP employee, detailee or contractor.

- 11.10.5. If a disposable visitor badge/card or pass is issued, issuance will be maintained either by manual or electronic means:
- The badge/card or pass will have as a minimum the visitor's full name and date of expiration;
 - Identify visitor as requiring escort or unescorted status; and
 - Can be issued to employees who have lost or forgotten their National Capital Region Photo Access Card (PAC) identification badge or other CBP facilities-issued access badge:
 - The Security Liaison will verify the individual in the CBP Personnel Security Data Base (IABI):
 - Missing badge/card or pass (possibly due to loss or theft) must be immediately reported to the Security Liaison
- 11.10.6. If a visitor's hard badge/card or pass is used, a strict accounting of the issuance will be maintained either by manual or electronic means and the visitor procedures will include an exchange process for issuance for a piece of photographic government-issued identification.
- 11.10.7. Visitors are responsible for safeguarding their visitor's identification badge/card or pass from loss or misuse.
- 11.10.8. Lost or stolen visitor identification badges/cards/passes:
- Will be immediately reported to the Security Officer and the sponsor will provide written documentation of the loss if requested by the Security Liaison.
- 11.10.9. The Security Liaison will:
- Maintain documented records of lost visitor badges/cards or passes;
 - Complete a re-issuance of visitor badges/cards or passes when the number of badges lost exceeds ten percent of the overall number of badges issued:
 - If re-issuance is accomplished all obsolete badges/cards or passes will be destroyed and a destruction documented.
- 11.10.10. Visitor identification badges are only issued for the purpose of authorizing a visitor into a CBP facility, area or space for the purpose of meetings, briefs, etc or vendors supporting CBP activities.
- 11.10.11. Visitor identification badges must not be issued in place of the National Capital Region Photo Access Card (PAC) identification badge or other CBP facilities issued access badge to any person for the purpose of daily work in a CBP facility, area or space. The only exception to this is that a visitor's identification badge can be provided to CBP personnel who have reported their National Capital Region Photo Access Card (PAC) identification badge or other CBP facilities-issued access badge lost or stolen and submitted the required documentation.
- 11.10.12. See the Lost Badge or Credential Directive, [CD 5230-029A \(2002\)](#) for further details of this documentation process.

- Individuals denied a PAC based on suitability are not authorized access;
- This includes short term visitor access.

11.11. ESCORTS

- 11.11.1. All DHS Federal employees and contractors assigned escort responsibilities will have a valid CBP National Capital Region Photo Access Card (PAC) identification badge or other issued CBP facilities issued access badge and authorized entry into the areas in which they are performing escort duties.
- 11.11.2. All DHS Federal employees and contractors assigned escort duties are responsible to:
- Ensure visitors under escort have been properly screened and badged (IAW 11.7 & 11.8);
 - Not escort more than four (4) visitors at one time;
 - Ensure escorted visitors are under visual contact and positive control at all times;
 - Ensure escorted visitors return visitor identification upon departure (IAW 11.7);
 - Report any unauthorized activities by escorted visitors to the Security Liaison;
 - Never leave escorted required visitors unattended;
 - Never escort a visitor into a restricted, controlled or classified area unless prior approval has been granted by the Security Liaison; and
 - Ensure visitors are aware of visitor identification safe keeping including:
 - Report of loss of identification to sponsor;
 - Proper display; and
 - Return policy.

11.12. VISITOR PARKING

- 11.12.1. Where the facility is operated and managed by CBP the following will apply:
- No unauthorized direct access into any facility from a parking lot or parking structure by visitors;
 - Visitor spaces are not intended to accommodate the daily or personal needs of employees who work in or near the CBP facility;
 - Post signage and arrange for towing unauthorized vehicles:
 - Procedures should be established and implemented to alert the public to towing policies and the removal of unauthorized vehicles.
 - Spaces will be designated for the exclusive use of visitors and handicap persons;
 - Utilize effective lighting to provide added safety and deter illegal or threatening activities;
 - For further information, see [Chapter 7.5. Protective Lighting](#).
 - Twenty-four hour CCTV surveillance and recording is required at all locations as a deterrent:

- o Requirements will depend on assessment of the security level for each facility.
- Digital video recordings (DVR) are also highly valuable as a source of evidence and investigative leads; and
- Where the facility is operated and managed by GSA, [41 CFR §101-20.104](#) will apply.
- For further information, see [Chapter 8.12. CCTV](#).

11.13. ELECTRONIC ACCESS CONTROLS

- 11.13.1. For detailed information on access controls see Appendix (CCTV) and Appendix (IDS).
- 11.13.2. Plan for locking devices or controls at perimeter and interior doors, providing effective key control. Plan for protection; cleaning, and maintenance personnel and determine hours, locations, and levels of access for such personnel.
- 11.13.3. Vehicles and Traffic Control. If public vehicle entrances have gates, they will be electronically opened and closed.
 - Accommodations for handicapped visitors will be provided.
- 11.13.4. Vehicle entrances with restricted access at facilities associated with a high threat level will be equipped with electrical or hydraulic vehicle gates or movable barriers.
 - Vehicle barriers may be controlled by: (see [Appendix 7.2. Perimeter Security Barriers](#))
 - o Card readers;
 - o Biometric devices;
 - o Proximity tags;
 - o Electronic keypads;
 - o Remotely by line-of-sight or using CCTV; or
 - o For high traffic areas, one-way entry and exit lanes shall be created.
- 11.13.5. Access control systems will be provided at perimeter doors, public waiting and information areas, visitation areas, processing areas, sally ports, secure vestibule, loading docks, and entrances to restricted areas.
- 11.13.6. The access control system shall be HSPD-12 compliant, hardware, or computer based system.
- 11.13.7. A personnel-based access control system relies on a person to:
 - Positively identify individuals requesting access;
 - Determine if the access is authorized; and
 - Secure the access port ensuring only the individual(s) authorized have gained access.
- 11.13.8. GSA Schedule 70 approved automated access control systems are appropriate for large applications and may be required for programs associated with a high threat

level. Systems may be in the form of stand-alone, one or two door units, small networks for 8-16 doors, or larger multi-door, multi-tasking systems. Characteristics of this type of system are:

- All authorized users are provided with unique pass cards, tags or personal identification numbers (PINs);
- Audit trails are available;
- Electrical power is required at each control point;
- Individual users can be deleted from the system without the need to recover cards, tags, pins or keys; and
- These types of systems are ideal for areas with 25 or more users and large systems controlling interior and exterior access control readers.

11.14. SCREENING PROCEDURES

11.14.1. Entry security must follow ISC Security Standards for Leased Space (Sept. 24, 2004):

- A visitor control/screening system, acceptable to the Government, is required. At a minimum, the system shall require Security Guards to screen visitors;
- Security Guards for public lobbies and public entrances shall be required for such purposes as:
 - ID/pass control;
 - Manning X-ray and magnetometer equipment.
- Guards can be furnished via either:
 - Lessor-furnished operating agreement or
 - Full leasehold control methods.
- If guards are lessor-furnished, they shall be trained and licensed in accordance with Government standards;
- Guards manning magnetometers and X-ray equipment will be armed; and
 - Guards will direct the building population and visitors through the magnetometers.
 - See [Appendix 11.14. Screening Procedures](#), for more information.

11.14.2. Facility Security Standards:

- X-ray and magnetometer screening devices at all public entrances for the screening of visitors, contractors, etc., and all of their purses, bags, briefcases, packages, etc., are mandatory for Level IV facilities:
 - A standard based on facility evaluation by the SL and/or the building security committee for Level III facilities:
 - Is desirable for Level III facilities;
 - Is not applicable for Level I facilities.

- X-raying of all packages entering the building delivered by contractors, couriers, etc., is mandatory for Level IV facilities:
 - A standard based on facility evaluation by the SL and/or the Building Security Committee for Level III facilities:
 - Is desirable for Level II facilities;
 - Is not applicable for Level I facilities.

11.14.3. Mail and packages entering the building will be:

- Subject to X-ray screening;
- Visual inspection by armed Security Guards:
 - Packages, briefcases, and other containers in the immediate possession of visitors, employees, or other persons arriving on, working at, visiting, or departing from Federal property, are subject to inspection. A full search of a person and any vehicle driven or occupied by the person may accompany an arrest;
 - The Government may divert large truck shipments to a secondary location for screening purposes; and
 - The Government reserves the right to negotiate security enhancements necessary for securing any unsecured non-federal block of space with a separate entrance (e.g., ground floor retail) based on a Government Building Security Assessment.

11.14.4. Visitor screening procedures will be developed based on the facility security level (see [Chapter 6. Facility Protection](#), and [Appendix 14: Building-Specific Security Alert Plan](#).)

- The procedures will:
 - Consider the building design;
 - Rate and flow of visitors;
 - Threat level;
 - Personnel available; and
 - Types of technical equipment installed.
- Screening procedures will:
 - Maintain maximum desired security;
 - Provide access only to persons with legitimate need.

11.14.5. The use of walk-through metal detectors (WTMD) or hand-held metal detectors (HHMD), people-control barricades, and door controls will be incorporated into the facility access procedure. The procedure will include:

- Provisions for active inspection and thorough visual checks of the contents of all packages, briefcases, handbags and similar items; such packages that may be transported by:

- o A visitor requesting access;
- o A freight carrier;
- o An express package delivery firm;
- o The U.S. Postal Service; and
- o U.S. Government courier.
- Visual checks of carried items including passage utilizing a WTMD or inspection using a HHMD before allowing access into any CBP space.

11.14.6. Additional:

- Emergency power sources to critical systems (alarm systems, radio communications, computer facilities, CCTV monitoring, fire detection, entry control devices, etc) are required. See [Appendix 11.14, Screening Procedures](#), for more information.

11.15. PROHIBITED ENTRY NOTICE

11.15.1. The authority of a CBP Designated Official or Security Officer to take reasonable, necessary and lawful measures to maintain law and order and to protect personnel and property shall include the authority to issue a Prohibited Entry Notice:

- That authority also includes the removal from or the denial of access to, any CBP facility, site or space of individuals who threaten the orderly administration of the installation or site;
- That authority must not be exercised in an arbitrary, capricious, or discriminatory manner; and
- Removal or denial actions must be based on reasonable grounds and be judiciously applied.

11.15.2. [41 CFR §102-74.450](#) allows for the fining and possible prosecution of individuals who do not conduct themselves appropriately in Federal buildings. [41 CFR §102-74.390](#) also outlines the appropriate policy for disturbances in public buildings, stating:

- All persons entering in or on Federal property are prohibited from loitering, exhibiting disorderly conduct, or exhibiting other conduct on property that:
 - (a) Creates loud or unusual noise or a nuisance;
 - (b) Unreasonably obstructs the usual use of entrances, foyers, lobbies, corridors, offices, elevators, stairways or parking lots;
 - (c) Otherwise impedes or disrupts the performance of official duties by Government employees; or
 - (d) Prevents the general public from obtaining the administrative services provided on the property in a timely manner.

11.16. PROHIBITED ITEMS

11.16.1. Prohibited Articles. The following articles are prohibited from CBP facilities, unless approved by the designated Agency/local authority for security:

- Any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property;
 - (Reference [18 USC §930](#), Possession of Firearms and Dangerous Weapons in Federal Facilities, and [41 CFR §102-74.440](#).) Sites shall, at a minimum, employ administrative procedures to deter the introduction of explosives into facilities.
- 11.16.2. Leases shall state that the Government reserves the right to post applicable Government rules and regulations at each public entrance in a Federally-occupied facility for such things as, but not limited to, barring the unauthorized possession of firearms and dangerous weapons.
- 11.16.3. Controlled Articles. The following privately owned articles are not permitted/ authorized in CBP facilities without prior written authorization from the DO.:
- Recording equipment (audio, video, optical, or data);
 - Electronic equipment with a data exchange port capable of being connected to automated information system equipment (portable computer drives or other data storage devices);
 - Radio frequency transmitting equipment; and
 - Computers and associated media.
- 11.16.4. Controlled Substances (e.g., illegal drugs and associated paraphernalia, but not prescription medicine) are not permitted/authorized.
- 11.16.5. Other items prohibited by law.
- Alcoholic Beverages.
- 11.16.6. [18 USC §930](#) is reprinted at the end of this chapter for the convenience of the Security Officer.

11.17. NATIONAL CAPITAL REGION DHS/CBP PHOTO ACCESS CARD (PAC)

- 11.17.1. CBP National Capital Region Photo Access Card (PAC) identification badges or other CBP facilities issued access badge are intended for official use only (FOUO) and identify the bearer as a CBP Federal employee or contractor authorized admittance into a DHS/CBP facility.
- 11.17.2. Only CBP/IA/SMD is authorized to issue DHS/CBP National Capital Region Photo Access Card (PAC) identification badges.
- 11.17.3. CBP National Capital Region Photo Access Card (PAC) and visitor's identification badges/cards or passes will be visibly worn above the waist and below the neck with the photograph, if applicable, visible while in any CBP facility servicing the public and removed from public view upon departing the facility to avoid publicizing CBP affiliation. This identification badge/card or pass must be fully visible, outside of clothing, at all times.
- 11.17.4. The Designated Official (DO) is responsible for providing accurate and updated [CBP Form 346](#) identifying authorized signature authorities to SMD/IA.

11.17.5. National Capital Region Photo Access Card (PAC) identification passes will be returned to the SMD/IA badging office for destruction.

11.18. SIGNAGE

11.18.1. Interior and exterior signage is standardized by function; Information, Direction, Identification and Regulation and is required at CBP facilities. All signage shall follow the standards shown in the GSA Manual on the Design of Sign/Symbol Systems for Federal Facilities and [18 USC §871](#)

11.18.2. A well-designed site should use as few signs as possible. Signs should make the site clear to the first-time user by identifying multiple site entrances, parking and the main building entrance.

11.18.3. Conformity of signage and directions:

11.18.4. Signage should be clear to avoid confusion and direct users to their destination efficiently. If an escort service is available, signs should inform users; and

11.18.5. Signage should conform to [41 CFR §102-74](#), Rules and Regulations Governing Public Buildings and Grounds.

11.18.6. Generally, graphics and style of site signage should be in keeping with the signage used inside the building. Signs integrated with architectural elements can also be very effective. There shall be a consistency in the font style and color plus any directional symbology used in site and building signage. Signage placement can be an important detail element of the building design whether prominently displayed and tooled into the exterior building wall materials or as a freestanding component near the entrance to the facility.

11.18.7. Persons in and on property shall at all times comply with official signs of a prohibitory, regulatory, or directory nature and with the lawful direction of Federal Protective Officers and other authorized individuals.

11.19. PHOTOGRAPHY

11.19.1. Employees and visitors at CBP-controlled spaces are prohibited from using cameras and video recording devices. The senior CBP official on site in coordination with the site Security Officer may grant exceptions to this policy on a case-by-case basis in writing. This includes, but is not limited to:

- Television cameras;
- Telecasting;
- Video/audio tape equipment;
- Motion picture;
- Still analog or digital cameras;
- Filming; and
- Any other means of image capture.

11.19.2. See [CBP Public Affairs Directive 5410-001a](#) for further information on regulations

[RETURN TO TOP](#)

regarding photography.

11.20. SECURITY VIOLATIONS

11.20.1. Violation of these procedures constitutes a security violation; the Security Officer will comply with all required actions.

11.21. OTHER

11.21.1. Legal Name Change: Any CBP federal employee, or detailee requesting a new identification badge/pass due to a legal name change (e.g. marriage, divorce, etc) will:

- Notify PSD/records management and mission support specialist of legal name change;
- Provide PSD/records management legal documentation of name change for IAIB update; and
- Be issued new identification only after IAIB reflects legal name change.

11.21.2. Legal Name Change: Any CBP contractor requesting a new identification badge/pass due to a legal name change (e.g. marriage, divorce, etc) will:

- Notify their company of the legal name change:
 - o Company will make notification to CBP/PSD.
- Be issued new identification only after IAIB reflects legal name change.

11.21.3. Non National Capital Region CBP Federal employees, detailees or contractor requesting National Capital Region PAC identification badges will:

- Be assigned duties within the national Capital region for a period of 30 days or longer;
- Accomplish required PAC documentation;
- IABI data base verification by SMD/IA PAC issuing authority;
- Personnel not found in the IABI data base can utilize [DHS form 11000-5 Personnel Security Data Verification Request](#) for the transmission of their DHS status into IABI;
- Comply with PAC identification return policy for National Capital Region, detailed above in [Section 11.17](#), upon completion of detail or assignment.

11.22. REFERENCE

- [e-CFR library](#)
- [18 USC §930](#)
- [DHS Form 11000-5 Personnel Security Data Verification Request](#)
- [CBP Public Affairs Directives 5410-001a](#)
- [ISO/IEC 7810](#)
- [ISO/IEC 7816-4:2005](#)

- [ISO/IEC 14443](#)
- [FIPS 201](#)
- [HSPD-7](#)
- [Homeland Security Presidential Directive 12 \(HSPD-12\)](#), August 2004.
- [PIV-I](#)
- [NIST](#)
- [PIV-II](#)
- [Privacy Act of 1974](#)
- [E-Government Act of 2002](#)
- [Federal Information Processing Standard 201: Policy for a Common Identification Standard for Federal Employees and Contractors](#), February 2005.
- [CFR 41 §101-20.302](#).
- [41 CFR §102-74.70 for the Rules & Regulations Governing Conduct on Federal Property](#)
- [Walk-through metal detector \(WTMD\)](#)
- [Hand-held metal detector \(HHMD\)](#)
- [OIA/CBP Guidelines to Report a Lost/Stolen Badge of Credential](#);
- Photo Access Card (PAC) identification badge(s) [Form CBP-242.pdf](#)
- [CBP Form 346](#)
- [\(GSC-IS V2.1\) Government Smart Card Interoperability Specification](#)
- [Schedule 70 for Products and Service Components](#):
- [Lost Badge Or Credential, Customs Directive 5230-029a \(2002\)](#)
- [41 CFR §101-20.104](#)
- [41 CFR §102-74. Subpart C](#). Prosecution of offenders is appropriate. Also see:
- [41 CFR §101-20.315 Penalties and other laws](#):
- [41 CFR §101-20.305 Disturbances](#): Any loitering, disorderly conduct,
- [18 USC §930](#)
- Signage should conform to [41 CFR §101-203.3](#),
- [CBP Public Affairs Directives 5410-001](#)

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE

CHAPTER 44 - FIREARMS

Section 930. Possession of firearms and dangerous weapons in Federal facilities

- (a) Except as provided in subsection (d), whoever knowingly possesses or causes to be present a firearm or other dangerous weapon in a Federal facility (other than a Federal court facility), or attempts to do so, shall be fined under this title or imprisoned not more than 1 year, or both.
- (b) Whoever, with intent that a firearm or other dangerous weapon be used in the commission of a crime, knowingly possesses or causes to be present such firearm or dangerous weapon in a Federal facility, or attempts to do so, shall be fined under this title or imprisoned not more than 5 years, or both.
- (c) A person who kills any person in the course of a violation of subsection (a) or (b), or in the course of an attack on a Federal facility involving the use of a firearm or other dangerous weapon, or attempts or conspires to do such an act, shall be punished as provided in sections 1111, 1112, 1113, and 1117.
- (d) Subsection (a) shall not apply to—
 - (1) the lawful performance of official duties by an officer, agent, or employee of the United States, a State, or a political subdivision thereof, who is authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of law;
 - (2) the possession of a firearm or other dangerous weapon by a Federal official or a member of the Armed Forces if such possession is authorized by law; or
 - (3) the lawful carrying of firearms or other dangerous weapons in a Federal facility incident to hunting or other lawful purposes.
- (e)
 - (1) Except as provided in paragraph (2), whoever knowingly possesses or causes to be present a firearm in a Federal court facility, or attempts to do so, shall be fined under this title, imprisoned not more than 2 years, or both.
 - (2) Paragraph (1) shall not apply to conduct which is described in paragraph (1) or (2) of subsection (d).
- (f) Nothing in this section limits the power of a court of the United States to punish for contempt or to promulgate rules or orders regulating, restricting, or prohibiting the possession of weapons within any building housing such court or any of its proceedings, or upon any grounds appurtenant to such building.
- (g) As used in this section:
 - (1) The term “Federal facility” means a building or part thereof owned or leased by the Federal Government, where Federal employees are regularly present for the purpose of performing their official duties.

- (2) The term “dangerous weapon” means a weapon, device, instrument, material, or substance, animate or inanimate, that is used for, or is readily capable of, causing death or serious bodily injury, except that such term does not include a pocket knife with a blade of less than 2 1/2 inches in length.
- (3) The term “Federal court facility” means the courtroom, judges’ chambers, witness rooms, jury deliberation rooms, attorney conference rooms, prisoner holding cells, offices of the court clerks, the United States attorney, and the United States marshal, probation and parole offices, and adjoining corridors of any court of the United States.
- (h) Notice of the provisions of subsections (a) and (b) shall be posted conspicuously at each public entrance to each Federal facility, and notice of subsection (e) shall be posted conspicuously at each public entrance to each Federal court facility, and no person shall be convicted of an offense under subsection (a) or (e) with respect to a Federal facility if such notice is not so posted at such facility, unless such person had actual notice of subsection (a) or (e), as the case may be.





CHAPTER 12: SERVICES

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

12.1. LAW ENFORCEMENT PROTECTION

12.1.1. The Federal Protective Service (FPS), Police Officers and local law enforcement officers, where response agreements are in effect, have primary responsibility for responding to criminal occurrences, incidents, and life threatening events at DHS facilities under the custody and control of GSA.

- In addition to protecting Federal government buildings, FPS is also responsible for the security and safety of Federal Government employees and visitors to Federal buildings;
- Occupants of facilities under the custody and control of GSA are responsible for promptly reporting all crimes and suspicious circumstances occurring on GSA-controlled property to the regional FPS Division (see [Chapter 20, Workplace Violence](#), for the address and phone number of FPS Regional Offices);
- FPS Inspectors and/or Physical Security Specialists (PSS) usually determine the placement and hours of operation of the guard posts in Federally-controlled facilities. They develop Post Orders for each post in coordination with tenant agencies and other key personnel;
- The implementation of security countermeasures, to include contract guards, are approved and paid for by the tenant agencies; and
- Physical security programs shall be administered within each region, center, and field activity based on CBP policy and guidance set forth in this handbook, to ensure the protection of CBP assets. These programs should be continually and effectively administered by the appropriate organizational security officer and monitored to ensure their integrity.

12.2. CONTRACT GUARD SERVICES

12.2.1. The U.S. Immigration and Customs Enforcement’s Federal Protective Service (FPS) shall “protect the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government.”

- FPS is responsible for acquiring and monitoring contract guard services;
- FPS law enforcement personnel are sworn Federal law enforcement officers and can make arrests on and off Federally-controlled property; and
- FPS law enforcement personnel exercise all the police powers of sheriffs and constables, with the exception of serving civil processes.

12.2.2. The authority to engage contract guard services for CBP rests with FPS. Any contract guard security must be coordinated with FPS. No CBP component may engage any private contract guard service independently or without direct coordination with FPS.

12.2.3. Non-uniformed Criminal Investigators (CIs) investigate crimes ranging from homicide to theft of Government property. They also investigate allegations of security guard misconduct on the job.

- Information provided to FPS investigators could be important to the successful

[RETURN TO TOP](#)

outcome of a criminal investigation;

- FPS uniformed and investigative personnel or local law enforcement will provide primary law enforcement support services; and
- Primary responsibilities of contract guard services are:
 - To control access to Federal property;
 - To assist in ensuring the safety of employees and visitors while on Federal property; and
 - To assist in ensuring the safety of Federal property.

12.2.4. Access control includes checking visitor and employee identification; operating security equipment such as X-ray machines and Magnetometers to screen for prohibited materials; operating or monitoring security cameras and/or alarms; and reporting crimes and incidents to the FPS MegaCenter.

12.2.5. Security Guards

- Help keep public order and prevent crime;
- Can detain individuals who are being seriously disruptive, violent, or suspected of committing a crime while on Federally controlled property, but they do not have the authority to arrest a suspect as police. Their duties mainly concern preventing and detecting crime rather than investigating and solving crimes;
- As part of their assigned duties, security guards are expected to:
 - Control access to specific areas of a facility;
 - Enforce property rules and regulations;
 - Detect and report criminal acts;
 - Stop and if possible, detain persons engaging in criminal activities;
 - Provide security against loss from fire or mechanical equipment failure;
 - Respond to emergency situations involving the safety and security of the facility; and
 - Act occasionally as a crowd monitor to maintain order.

12.2.6. Delegations of GSA Authority

- The Memorandum of Agreement dated June 2006 by and between the Department of Homeland Security (DHS) through U.S. Immigration and Customs Enforcement's Federal Protective Service (ICE/FPS), and the General Services Administration (GSA) charged DHS with protecting buildings, grounds, and property that are owned, occupied, or secured by the Federal Government (including any agency, instrumentality, or wholly owned or mixed-ownership corporation) and the persons on the property. The Secretary of DHS further delegated these functions to ICE/FPS. As outlined in the agreement DHS ICE/FPS will provide security and law enforcement services to facilities under the custody and control of GSA.
- In facilities where GSA has delegated its authority to the occupant agency, it may

[RETURN TO TOP](#)

also delegate most or all of its enforcement powers. Generally, GSA has reserved its investigative and prospective powers;

- When jurisdiction is delegated by the FPS, an agreement must be negotiated with the local police to provide law enforcement response.

12.2.7. Determining Need

- A guard force is an integral and effective element in a facility's physical security program. The effectiveness of alarm devices, physical barriers, and intrusion detectors depends ultimately on a response by a skilled guard force;
- Guard services, as delegated by DHS MOA, can be provided by FPS Federal Police Officers; and
- The Federal Protective Service is responsible for delivering a comprehensive physical security and law enforcement program in all Federally-owned or leased facilities.

12.2.8. Criteria for Determining Need

- As cited in the handbook titled "[Department of the Interior Facility Security Standards Appendix B.](#)" evaluating a facility for security guard requirements to include a security guard patrol is desirable for security Level II facilities;
- This evaluation may be a standard based on a Building Security Committee facility evaluation for security Level III facilities, and is a minimum-security standard for Level IV facilities.

12.2.9. The number of guards at any given time will depend on the size of the facility, the hours of operation, and current risk factors. Guard services are recommended under, but are not limited to, the following circumstances:

- At Security Level III and IV facilities, to meet visitor control and screening requirements;
- The mission of the facility is particularly critical;
- High level/volume of sensitivity of information handled at the facility, e.g., National Security Information (NSI);
- An in-house response capability is needed, e.g., the facility contains alarmed vaults or other sensitive operations, and off-site guards or police are not close enough for quick response;
- The facility is vulnerable to theft or damage, e.g. a facility location is in a high crime area;
- Pedestrian or automobile traffic is heavy or congested and requires special controls; and
- Moderate to large volume of public functions and/or moderate to large volumes of mail and packages, which require screening or inspection.

12.3. COST FACTORS

12.3.1. As with any expenditure of funds for security, the annual costs of guard services

[RETURN TO TOP](#)

normally should not exceed the monetary value, replacement or critical loss value of the protected items.

- 12.3.2. Costs for guard services are recurring and funding sources must be obtained from the beginning of the project for the duration of the contract.
- 12.3.3. A substantial expense for guard services may be required for crowd or traffic control, for safeguarding highly classified or sensitive information, or for protecting material or functions which have high intrinsic rather than monetary value.
- 12.3.4. This is especially true as applied to the safety of employees since it is impossible to put a dollar value on human lives or peace of mind.
- 12.3.5. A guard post in a high crime area may yield substantial benefits in terms of improved safety, higher employee morale, increased productivity, and a better image of DHS/ CBP.

12.4. GUARD DUTIES

12.4.1. Any decision about whether to utilize a guard force of any size must consider the following duties that guards may properly perform:

- Entrance Control
 - Operate and enforce a system of access control, including inspection and identification of packages.
- Roving Patrol
 - Patrol routes or designated areas such as perimeters, buildings, vaults, and public areas.
- Traffic Control
 - Direct traffic (vehicular and pedestrian), control parking, check permits, and issue citations.
- Key Control
 - Receive, issue, and account for certain keys to the building and its internal areas.
- Security and Fire Systems
 - Monitor, operate, and respond to triggered intrusion or fire alarm systems or protective devices.
- Utility Systems
 - Monitor, record data, or perform minor operations for building utility systems.
- Lost and Found
 - Receive, process receipt for, and store found items.
- Flying of the U.S. Flag
 - Observe flag flying procedures.
- Reports and Records

- o Prepare reports on accidents, fires, thefts, and other building incidents.
- Response to Emergencies
 - o In case of any emergency (fire, bomb threat, assault or civil disturbance), respond, summon assistance, administer first aid, and assist public safety personnel.
- Law and Order
 - o Maintain law and order within the area of assignment.
- Hazardous Conditions
 - o Report potentially hazardous conditions and items in need of repair;
 - o When necessary, supervisors and/or managers may be invited to participate in Building Security Committee (BSC) and Occupant Emergency Plan (OEP) Committee meetings.

12.5. PERSONNEL REQUIREMENTS

12.5.1. Manpower

- The number of full-time guard posts for a facility is determined by the Security Officer and the site manager. The decision should be based on a comprehensive physical security survey. The number of guard posts will be determined by the local crime rate, number of entrances, alarm systems requiring response, and other factors particular to each facility. The Security Officer must calculate the total number of posts and hours of coverage. The bidding contractor will be responsible for calculating the total number of guards required, taking into account the number and duration of shifts, reliefs, sick leave, training, vacation, and other administrative factors.

12.5.2. Armed Guards

- Guards operating magnetometer and X-ray screening devices are required to be armed to appropriately respond to all possible threats and volatile situations. At Level IV facilities, the use of magnetometer and X-ray screening devices at public entrances is a mandated standard;
- Guards should be armed only when there are compelling reasons. If guards are armed for a deterrent effect, i.e., to prevent crime or other unauthorized activity, responsible officials must weigh that advantage against such disadvantages as the danger to innocent personnel if a firearm is used by a guards; the possibility of an accidental discharge; and the possibility, no matter how remote, of irrational behavior on the part of a guard in a weak moment or under pressure;
- Firearms may be used only defensively and only for the protection of life and property;
- When making a decision as to whether guards at a facility should be armed, the senior facility manager and the servicing Security Officer should give strong consideration to the factors below. If contracting, every possible effort should be made to include requirements in the contract Statement of Work that will task the

[RETURN TO TOP](#)

contractor with providing properly selected and trained personnel and maintaining appropriate level of performance and conduct standards. These factors apply whether hiring guards directly or dealing with a contractor:

- o Firearms training including judgment shooting and firearms safety;
- o Knowledge of criminal activities and proper law enforcement response procedures;
- o Judgment and emotional stability;
- o Experience and demonstrated ability to retain composure under pressure and
- o A personal history free of arrests or other criminal activity.

12.5.3. Supervision

- Supervision of contract guards is the responsibility of the Contracting Officer's Technical Representative (COTR). Agency Technical Representatives (ATR) are to be appointed at every location where contract guards are assigned within a CBP facility. ATRs are responsible to work with the COTR and ensure services contracted are being performed in a professional manner. Supervision is required for all guard posts and is usually requested at a ratio of one hour of supervision for each eight productive hours on post. COTRs are responsible for oversight of this activity;
- On small contracts with three or fewer posts or at isolated sites, the use of roving supervisors may be the only practical or cost-effective method of supervising the contract;
- At sites where there will be eight or more posts, an on-site supervisor should be required, at least during the hours of heaviest traffic and greatest productivity on post. After-hours supervision can be performed at the one to eight ratio by roving supervisors. Large forces and facilities generally require more supervision; a contract with thirty or more shifts per week should have full time supervision; and
- Supervision is required for all guard posts and is usually requested at a ratio of one hour of supervision for each eight productive hours on post.

12.5.4. Federal Protective Services (FPS) Physical Security Responsibilities

- FPS is responsible for delivering a comprehensive physical security and law enforcement program in all Federally owned or leased facilities. This involves providing law enforcement and security for more than a million Federal workers and visitors at over 8,300 buildings nationwide. FPS enforces laws and regulations governing public buildings, maintains law and order, and protects life and property in Federally controlled work places;
- FPS partners with other Federal, State and local agencies throughout the Nation to develop specific solutions to challenges, assists with police emergency and special security services, and offers police and security support to law enforcement departments during high-profile National special security events. To make Federal facilities safer, FPS also consults with building owners and tenants to advise on physical security measures. FPS provides crime prevention

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

education for agencies and individuals, and recommends strategies to keep everyone safer, both on and off the job. The organization is comprised of the Headquarters and eleven Regions. Services fall into eight components:

- o Management;
 - o Law Enforcement;
 - o Criminal Investigations;
 - o Physical Security;
 - o Communications;
 - o Security Systems;
 - o Security Guard Services; and
 - o Administrative Support
- FPS management, both at the Headquarters and at regional level, is responsible for developing and providing programs, policies, leadership, guidance, and oversight for FPS personnel;
 - In many facilities owned, operated or leased by GSA, the guard force may be FPS Police Officers. FPS officials will work with the Facility Security Officer representing the prime tenant (agency with the greatest number of employees in a building or facility) to ensure the security needs of the occupants are met; and
 - FPS has developed a formula to determine the extent of guard services required for a given building or facility based on a number of factors including building size and population, sensitivity of operations, and crime rate in the building and the surrounding area. The agency pays FPS for the determined amount of protective services as a percentage of the rent (formerly Standard Level User Charge, or SLUC) for the facility. In other words, the agency pays FPS a certain cost per year, per square foot of usable space, for basic protective services. Additional protective services must be reimbursed by the requesting agency. See [Chapter 6.2, Planning Facility Protection](#), for facility protection in GSA-owned or leased facilities. Ensure that reimbursements are issued to FPS and not to GSA.

12.6. RESPONSIBILITIES BY FACILITY TYPE

12.6.1. GSA-Owned, Operated or Leased Facilities

- In facilities owned, operated, or leased by GSA, FPS officials may decide to contract for guard services. In such cases, a Contracting Officer (CO) of the appropriate FPS regional office will procure and maintain guard services for each facility. The contract will normally be managed by a Contracting Officer's Technical Representative (COTR), an FPS official with physical security expertise who maintains contact with the prime tenant's security officials to determine their needs and execute the terms of the contract;
- In many larger facilities, a representative of the prime tenant agency, an Agency Technical Representative (ATR) will work directly with FPS' COTR and CO to develop the contract, write post orders, and monitor performance of the contract.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

FPS periodically offers guard contract management training for ATRs; and

- FPS officials are responsible for security and suitability processing of all contract guard personnel, as well as training and certification. It is advantageous for the ATR to work closely with FPS officials to provide input as necessary and to monitor the required processing. DHS and CBP suitability requirements must be followed.

12.6.2. DHS Facilities with FPS Delegations of Authority

- In DHS facilities where FPS has delegated protection authority to the agency or prime tenant, some protection responsibilities are transferred to the agency, including procurement and management of guard contracts. Normally, FPS will retain responsibility for physical security surveys, mobile patrols, monitoring of alarms, response to incidents, and requests for criminal investigations. FPS will provide such services at no charge to the agency beyond the protection portions of the rent. Under the delegation, the accepting agency is responsible for providing services formerly administered by FPS.

12.6.3. Procurement and Management of Guard Services

- The senior facility manager, in consultation with the FSO, is responsible for working with the appropriate COs to procure and manage guard services.

12.6.4. Security Clearances

- If the contract is to be classified, the guards will require security clearances. The clearance request procedures are outlined in the Defense Industrial Security Program regulation, as implemented by [SM 440.3.11](#). [DHS MD 11045](#).

12.6.5. Crime Prevention Assessments

- The senior facility manager may elect to request FPS or a local law enforcement agency to conduct these assessments.

12.6.6. Maintenance and Response to Security Systems in Place

- Local contractors are generally available to perform such maintenance and response, or FPS may be able to provide such services on a reimbursable basis in metropolitan areas.

12.6.7. Reporting of all Serious Criminal Incidents to FPS

- FPS requires that all serious criminal incidents be reported to the appropriate FPS Office.

12.6.8. DHS-Owned and Leased Facilities

- In DHS owned and leased facilities to include leased space from other Federal agencies, many protection responsibilities are transferred to the agency. In addition to those items listed above in 9.2.E(2), DHS will also be responsible for physical security surveys and monitoring of alarms. Normally, FPS will retain responsibility for mobile patrols, response to incidents, and requests for criminal investigations. Many security services may be provided by FPS on a reimbursable basis. Contact your regional FPS office as cited in [Chapter 20.6](#).

[RETURN TO TOP](#)

[FPS Regional Offices](#), for additional information.

12.6.9. Guard Services Contracting

12.7. FEDERAL PROTECTIVE SERVICES

12.7.1. In recent years, the basic FPS concept of protection has evolved from the guard on a fixed post to a response mode using mobile patrols. As a result, GSA-owned or operated buildings normally are not assigned guard posted at sentry doors. Instead they are policed by roving patrols in the buildings or rely on FPS patrols for response to incidents, at least in the 12 major cities with an FPS presence.

12.7.2. Crime Prevention Assessments. The senior facility manager may elect to request FPS or local law enforcement agency to conduct these assessments.

- Maintenance and Response to Security Systems in Place. Local contractors are generally available to perform such maintenance and response, or GSA may be able to provide such services on a reimbursable basis in metropolitan areas;
- Reporting of all Serious Criminal Incidents to GSA. GSA requires that all such incidents be reported to the appropriate Federal Protective Service office as identified at <http://www.ice.gov/about/fps/contact.htm#region11>.

12.8. OTHER LAW ENFORCEMENT

12.8.1. Federal Bureau of Investigation (FBI)

- The FBI is the investigative arm of the Department of Justice (DOJ) whose investigative authority is given by 28 USC §533. The FBI investigates crimes such as those pertaining to civil rights, organized crime and other Federal crimes.

12.8.2. United States Marshal Service

- The U.S. Marshals Service is the component of the DOJ charged with, among other missions, judicial security, investigating fugitives, witness protection, and administering the DOJ's seized asset forfeiture program.

12.8.3. Drug Enforcement Administration (DEA)

- The DEA is the DOJ component charged with enforcing the controlled substance laws and regulations.

12.8.4. Bureau of Alcohol, Tobacco and Firearms (ATF)

- ATF is the DOJ component charged with enforcing Federal laws regulating firearms and explosives.

12.8.5. United States Secret Service

- The Secret Service is a DHS component with the dual missions of protecting national and foreign leaders or heads of state, and investigating financial crimes such as counterfeiting.

12.8.6. United States Postal Inspection Service (USPIS)

- Through its Inspection Service, the USPS protects the mail, postal funds, and

[RETURN TO TOP](#)

property. The USPIIS investigates internal conditions and needs that may affect its security and effectiveness; apprehends those who violate the postal laws; and audits financial and non-financial operations.

12.8.7. State, County, and Municipal Agencies

- Each State maintains agencies for the enforcement of its laws within its jurisdiction. These may include State police and highway patrol as well as investigative and enforcement entities at the State and local level;
- The sheriff's office or Police Department in each county normally has the responsibility for enforcing county laws and in cooperation with State and municipal agencies certain State penal laws, such as the State criminal code.

12.9. AUTHORITIES/REFERENCES

- The Homeland Security Act of 2002, PL 107-296, enacted November 25, 2002
- Department of Justice Vulnerability Assessment of Federal Facilities, June 1995
- US Code: 40 CFR §1315, Law Enforcement authority of Secretary of Homeland Security Protection of Public Property
- MD 11000 Office of Security
- MD 11030.1 Physical Security of Facilities and Real Property
- MD 11035 Industrial Security Program
- MD 11042.1 Safeguarding Sensitive but Unclassified (For Official Use Only) Information
- MD 11044 Protection of Classified National Security Information Program Management
- MD 11049 Security Violations and Infractions
- MD 11050.2 Personnel Security and Suitability Program
- MD 11055 Interim Guidance- Suitability Screening Requirements for Contractors
- FPMR 101-20.103-3
- PBS P 5930.17C, Office of Federal Protective Service Policy Handbook, February 28, 2000.
- Homeland Security Presidential Directive (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors
- Memorandum of Agreement Between the Department of Homeland security and the General Services Administration (MOA DHS/GSA), date June 1, 2006
- Memorandum for The Heads of Departments and Agencies, Verifying the Employment Eligibility of Federal Employees, dated August 10, 2007
- Department of Homeland Security, Federal Protective Service, Security Guard Information Manual (SGIM), July 2006 Revised
- Memorandum For All DHS Components, Acquisition of Contract Guard Services, dated July 2, 2007





CHAPTER 13: PROGRAM DEVELOPMENT AND STRATEGIC PLANNING

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

13.1. GENERAL

- 13.1.1. The work of Customs and Border Protection (CBP) is vital to the Nation's defense and security. Accordingly, CBP must ensure appropriate levels of protection from loss or theft of classified material or Government property, as well as prevent any acts of unauthorized access, theft, diversion, sabotage, espionage, or other hostile activities.
- 13.1.2. Security countermeasures are an integral system of physical protection. These countermeasures are designed to deter, prevent, detect, and respond to unauthorized possession, usage, or sabotage of property or information.
- 13.1.3. CBP uses security programs to define, develop and implement its responsibilities under Federal statutes, Executive orders and other directives for the protection of classified and sensitive information or materials, and for the protection of CBP and CBP contractor facilities, property, information and personnel.
- 13.1.4. CBP offices designate in writing a Security Officer or Security Liaison in their organization that will facilitate all the security and awareness training requirements.
- 13.1.5. Key Program Elements
- Levels of protection appropriate to particular security interests are provided through the development and execution of comprehensive security countermeasures and security programs. This chapter establishes the responsibilities for managing and implementing the protection of security interests, and sets forth the framework for documents which define the policies, baseline requirements and responsibilities specific to the major elements of the Security Program. The key program elements are:
 - o Strategic Planning;
 - o Program Management and Administration;
 - o Personnel Development and Training; and
 - o Incident Reporting and Management.

13.2. STRATEGIC PLANNING

- 13.2.1. Purpose
- The purpose of strategic planning is to prepare comprehensive procedures, processes and information allowing CBP to apply sound risk management principles and enhance the protection of the people, facilities, property and information.
- 13.2.2. Objectives
- Strategic planning promotes sustainable improvements in physical security to effectively protect the people, facilities, property, and information that make up the CBP. CBP is dedicated to applying sound risk management principles and implementing principles and security practices using applicable laws, regulations, strategies, policies and guidelines.

13.2.3. Required Timelines and Resources

- Strategic Planning is long-range planning and not the type of operational planning that most facility administrators are accustomed to doing. It is NOT intended to answer such questions as “How many projects will each supervisor have next year?” or “How much money should be budgeted?” The focus of strategic planning is on answering the question, “Given the needs we serve and the trends we see around us, what should we strive to become in the future?” This raises two related considerations:
 - Timelines: Strategic plans and budgets must be revisited annually so as to adapt to changing priorities, unforeseen trends, opportunities, or challenges. Focus is placed on the current role of the facility and its future level of responsibilities within CBP;
 - Resources: Practical and realistic plans are needed to account for multiple contingencies. Sources of funding and resources may change on an unpredictable basis.

13.3. PROGRAM MANAGEMENT AND ADMINISTRATION

13.3.1. General

- Risk Management identifies, assesses, communicates and addresses the risks facing an organization, ensuring that objectives will be met. There is some level of risk inherent in any activity which must be accepted. Determination of the appropriate level of protection shall take into account:
 - The nature of the threat;
 - The vulnerability of the potential target; and
 - The potential consequences of an adversarial act.
- Site-specific countermeasures and security programs must be based on vulnerability/risk analyses. A rational and responsible balance is obtained through the planning and execution of comprehensive security programs. These programs are designed to provide a high degree of assurance that threats will be deterred, denied, contained, mitigated or neutralized as appropriate. Risk associated with countermeasures and security vulnerabilities must be reduced even where not mandated by specific requirements, when such reduction is consistent with the CBP mission and when supported by appropriate cost/benefit analyses;
- Planning for security is an integral part of any function or project undertaken within CBP. The most efficient and cost-effective method of instituting security measures into any facility or operation is through advance planning and continuous monitoring throughout the project or program. Selecting, constructing, or modifying a facility without considering the security implications of employee safety and protection of assets will result in costly modifications and lost time;
- Site-specific programs must have individual countermeasures and security programs tailored to address their specific characteristics. The site-specific

[RETURN TO TOP](#)

countermeasures and security planning process enables field managers working with Directors of Security to design and implement protection programs tailored to their respective operational needs, recognizing ongoing programs, current threat guidance, current policy, technology, and unique site-specific requirements. Site-specific protection programs must be documented in site security plans. The residual risks to be accepted by CBP are identified through vulnerability/risk analyses;

- These security programs are based on policy set forth in this handbook. These programs must be continually and effectively administered and monitored to ensure their integrity. At a minimum a physical security program will include:
 - A physical security survey of each facility occupied by CBP, to evaluate the security conditions in place to protect CBP personnel and assets, including classified or sensitive information;
 - Periodic inspections of facilities to ascertain whether a security program meets pertinent Federal, departmental, and CBP standards or regulations;
 - A comprehensive and continuing awareness security training program to ensure understanding of security awareness with employees, contractors, consultants, and visitors;
 - Procedures for taking immediate, positive and orderly action to safeguard life and property during an emergency;
 - Management reviews of security programs including:
 - Detailed briefings on the countermeasures and security posture of the facilities in each individual’s area of responsibility;
 - Assessment of findings and recommendations from oversight activities such as inspections and evaluations, security surveys, self-assessments, General Accounting Office audits and other internal and external evaluation functions.
 - Reviews must provide sufficient data and information to permit a determination of the current status of countermeasures and security baseline throughout the organization by the individual assuming responsibility for the organization.
- On-site visits will be conducted in accordance with the strategic plan.

13.4. PERSONNEL DEVELOPMENT AND TRAINING

- 13.4.1. CBP will ensure their Security Education, Training and Awareness (SETA) programs are in compliance with the [DHS SETA Program DHS MD 11053](#).
- 13.4.2. The CBP SETA Coordinators will share resources with other organizational units as necessary to increase the quality of security awareness.

13.5. PHYSICAL SECURITY TRAINING

- 13.5.1. For basic training, the Security Officers/Security Liaison will review and familiarize

themselves with the contents of this handbook and the applicable Federal, departmental, and CBP security regulations referenced herein.

- In most Instances, formal basic security training will not be necessary. Should basic physical security training be required, the responsible supervisor shall make arrangements to provide this training;
- At the discretion of the responsible supervisor the Security Officers/Security Liaison are encouraged to attend training courses on a variety of security subjects offered by a number of different agencies.

13.6. SECURITY AWARENESS, TRAINING AND EDUCATION (SATE) PLANS.

13.6.1. A Security Awareness, Training and Education plan is a critical factor in building and maintaining a facility's security defenses.

NOTE: A Security Awareness, Training and Education (SATE) plan is NOT the same as a Security Education, Training and Awareness (SETA) program

13.6.2. Starting a SATE Program can be simple. Managing and maintaining the SATE Program can often be the most challenging aspect of implementing any security strategy.

- The Security Officers/Security Liaison must plan an effective program of Instruction, making efficient use of training material provided for specific training purposes;
- At a minimum all employees will be provided formal security awareness training annually.
- All DHS personnel who have not fulfilled the requirements of the SATE Program are precluded or restricted from unescorted access to DHS security areas and/or from access to classified information until the requirements are met; and
- The Security Officers/Security Liaison may also tailor presentations to the organization and solicit other security professionals to speak on their areas of responsibility, training and expertise. For example, a local police representative could address crime prevention. Also, the Federal Protective Services (FPS) offers posters and pamphlets with helpful security hints and will provide on-site crime prevention seminars.

13.6.3. Security Education, Training, and Awareness programs will include but are not limited to dissemination of information concerning the following:

- Applicable DHS security directives and procedures and an overview of DHS security disciplines to include personnel security information security, and physical security;
- Site-specific (and/or operations-specific) security policy, procedures, and requirements that include local access control procedures, escort requirements, prohibited articles, along with reporting and notification requirements;
- Criminal, civil, and administrative sanctions imposed for incurring a security infraction or committing a violation;

- Other matters relating to security including but not limited to recent espionage cases, approaches, and recruitment techniques employed by an adversary of any nature, as well as foreign intelligence service threats to sensitive and classified information;
- Countermeasures against security threats and/or vulnerabilities to include protection of Government property;
- SETA programs will also include but are not limited to developing and presenting four briefings:
 - Security Orientation Briefing. The Training Briefing will be provided within the first 30 days of assignment. All DHS personnel will attend a DHS Security Orientation Briefing at the earliest possible date;
 - Initial Security Briefing. All DHS personnel who are assigned to duty positions that require a clearance, are in possession of a clearance, or are eligible or in processing for a security clearance, will receive an initial security briefing. Prior to being granted access to classified information, individuals shall receive a comprehensive briefing to inform them of their specific safeguard and security responsibilities. If relocated to a new building or position, individuals will receive a new briefing;
 - Refresher Briefing. All DHS personnel must receive annual refresher briefings to reinforce and update awareness of security policies and their responsibilities. Refresher briefings are mandatory for all DHS employees and must be implemented each calendar year at approximately 12-month intervals; and
 - Termination Briefing. Personnel will receive termination briefings to inform them of their continuing security responsibilities after their access authorizations are terminated. A termination briefing shall be implemented on the individual's last day of employment, the last day the individual possesses an access authorization, or the day it becomes known that the individual no longer requires access to classified information.
- Documentation Requirements
 - Records will be maintained to identify all individuals who have received briefings by type and date of briefing;
 - The name and contact information of the person doing the briefing (or the source of briefing information) will also be maintained;
 - Record-keeping systems must provide an audit trail. Statistics pertaining to total population and numbers that have received security briefings will be maintained and provided to the DHS Office of Security when requested.



**CHAPTER 14: INCIDENT RESPONSE AND
THE HOMELAND SECURITY ADVISORY SYSTEM (HSAS)**

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

14.1. GENERAL

- 14.1.1. The purpose for developing emergency plans is to provide emergency management guidelines for managers and employees to reduce the effects of incidents and emergencies that could harm employees and/or deny access to or prevent damage to a facility.
- 14.1.2. This is accomplished by providing a standardized approach to planning, documenting, and implementing increased security measures for all CBP buildings during heightened alert levels due to emergency situations such as terrorist attack, natural disaster, or civil unrest.
- 14.1.3. All employees should be aware of the Homeland Security Advisory System (HSAS) which uses color-coded alerts to indicate the general level of security. Specific responses at each level will vary by locality and facility.

14.2. INCIDENT RESPONSE

- 14.2.1. An incident reporting program is an essential element in any security program. The timely reporting of thefts, losses, damage of property and the tampering or unauthorized disclosure of information is crucial.
- 14.2.2. A timely report increases the possibility of recovering the property, minimizing damage and apprehending the assailant.
- 14.2.3. Any employee who discovers, witnesses, or has knowledge of a criminal, dangerous, or unauthorized practice or condition, or a violation of security regulations shall immediately report the matter to the appropriate authorities.
- 14.2.4. Reporting serious incidents, unusual events and emergency conditions
 - The senior official at a facility is responsible for reporting serious incidents, unusual events, or emergency conditions that affect CBP operations.
- 14.2.5. Reporting incidents to law enforcement agencies
 - [FPMR 101-20.103-3](#) requires the prompt reporting of all crimes and suspicious circumstances occurring on GSA-controlled property to the local Federal Protective Service (FPS). In most cases, the FPS will dispatch a U.S. Federal Police Officer to record the incident;
 - The [FPS Form 3155](#), Offense/Incident Report, is the standard reporting form. The Security Officer may use this form when FPS police officers are not available in the general area. The form requests information such as date, time and location of incident, details regarding lost stolen or damaged items, nature of the incident and any suspects involved. Supplies of the form can be obtained from the FPS Regional Office or building manager; and
 - Reports of theft or loss of explosive materials (blasting agents and detonators) also shall be reported within 24 hours of discovery by telephone and in writing to the nearest Bureau of Alcohol, Tobacco and Firearms (ATF) office.
- 14.2.6. Administrative Reporting

- The incident reporting requirements stated herein are not a substitute for nor do they eliminate the need for compliance with any additional reporting requirements prescribed in Federal and Departmental Regulations and in the Administrative Manual pertaining to motor vehicle incidents and to the loss, damage and mishandling of Government property;
- The Commissioner's Situation Room serves as CBP's 24-hour, 7 days a week, reporting and information coordination center. It facilitates communication between CBP Headquarters and the CBP field offices by serving as the entry point for reporting of significant incidents from field offices. The Situation Room provides complete, accurate, and timely reporting to the Commissioner and senior CBP management and will provide connectivity to the Department of Homeland Security, Homeland Security Operations Center and other interagency entities for information on significant events impacting CBP operations.

14.3. REPORTING PROCEDURE

14.3.1. Initial notifications will be made to the Commissioner's Situation Room prior to other established reporting entities. This does not eliminate any office or divisional reporting requirements. The Commissioner's Situation Room is the primary point of contact for significant incident reporting for all CBP field offices, to include ports of entry, sectors, stations, air and marine branches, and international offices.

14.3.2. Keeping in mind the safety of our employees and the integrity of operations within the different disciplines of CBP, the reporting procedures are as follows:

All CBP events related to terrorism or potentially related to terrorism must be reported telephonically immediately and in writing immediately thereafter via Significant Incident Report (SIR) to the Commissioner's Situation Room. Section 7 of this Directive delineates types of incidents that should be considered related or potentially related to terrorism;

All other incidents of a sensitive or timely nature will be reported telephonically to the Commissioner's Situation Room within 2 hours of occurrence and followed by written notification within 4 hours. More serious events which occur over an extended time period will require regular updates; and

- Once a reference number has been provided to field personnel, a written report must be filed with the Commissioner's Situation Room within the time frame specified above in 14.3.2.a. Failure by field offices to file written reports in the required time frame will be tracked and reported to the relevant Headquarters office for review and remedial action.

14.3.3. The telephone numbers for the Commissioner's Situation Room are 1-877-748-7666, 202-344-3886 and 202-344-3920. Reports are to be faxed directly to the Commissioner's Situation Room at 202-344-3886. For classified reports, fax directly to 202-344-3911. For electronic submission of SIRs, SIR-HQBOR or cbp.sitroom@dhs.gov should be used as appropriate

14.4. INCIDENT REPORTING

14.4.1. The [Significant Incident Report \(SIR\) CBP Form 6](#) (01/05) is intended to be used to transmit information pertaining to the partial, entire, temporary, or permanent loss or potential loss of CBP assets. Assets for the Agency include information, property, facilities and personnel (including lost-time injuries or other incidents). Activities that have the potential for loss of assets such as violations of security policies, procedures, and practices are included.

14.4.2. This form is to be used by Headquarters, Regional, District, Sector, and subordinate component Security Officers, Collateral Duty Security Officers, Managers, and security guards as an initial report of a loss. This report may also be shared with logistics officers, property custodians, Federal and local law enforcement agencies, and facility managers as necessary.

14.4.3. Reporting persons shall complete an Event Report for the following types of occurrences: [CBP Directive NO: 3340-025C](#). Commissioner's Situation Room Reporting, has an extensive list of reportable items.

- | | |
|-----------------------------------|---|
| TERRORIST RELATED | SUICIDE ATTEMPT |
| EMPLOYEE ARRESTED | MEDIA INTEREST |
| EMPLOYEE ASSAULTED | CREW DESERTERS |
| EMPLOYEE DEATH | ESCAPE |
| EMPLOYEE INJURED | OTHER: NON-EMPLOYEE INJURY/DEATH |
| RADIATION DETECTION EVENT | MISSING PROPERTY |
| SHOTS FIRED AT OR BY EMPLOYEE | NATURAL DISASTER |
| CANINE INCIDENT | OFFENSE AGAINST PERSON |
| SIGNIFICANT SEIZURE | PROPERTY OFFENSE |
| SIGNIFICANT ARREST/DETENTION | SECURITY POLICY/PROCEDURE |
| RESCUE | VIOLATION |
| SIGNIFICANT AGRICULTURAL EVENT | SERIOUS INJURY |
| CONVEYANCE/AIRCRAFT INCIDENT | When directed by Post orders, General |
| FOREIGN MILITARY/POLICE INCURSION | Orders, Special Orders, or as directed by the |
| BOMB THREAT | COTR or their designated representative (for |
| FACILITY DISRUPTIONS | Security Guards). |
| TECHNOLOGY DISRUPTIONS | Any other event of a security concern |

14.5. EVENT REPORT COMPLETION

14.5.1. The following guidelines should be followed to the extent practical. The table below provides instructions by field number and name for completing the Significant Incident Report.

- Instructions for [Completing Significant Incident Report Form 6](#)
 - Provide the date, time and exact location of the significant incident. Provide the date, time and name of person in the Commissioner’s Situation Room to whom the incident was reported telephonically. When telephonically reporting significant incidents to the Commissioner’s Situation Room, you must obtain a Commissioner’s Situation Room (CSR) number. Place this number in the top right hand box on the report form.

14.5.2. Once a CSR number has been provided to field personnel, a written report must be filed with the Commissioner’s Situation Room within the time frame specified in Section 4.4 of [CBP Directive NO: 3340-025C](#). Failure by field offices to file written reports in the required time frame will be tracked and reported to the relevant Headquarters office for review and remedial action.

- Provide the Designated Field Office, Port of Entry, Sector, Station, Air and Marine Operations Branch, or International Office that is submitting the report. Provide the name and telephone number of the person submitting the report. Provide a point of contact and telephone number in the event additional information not contained in the report is needed;
- Check the appropriate box as to the type of incident and if it involved CBP personnel, indicate whether it happened on or off duty;
- Provide a brief synopsis of the incident to include the names of individuals involved, commodity, weight, and value (if known) of items seized. If an arrest is made, indicate the number, sex, and citizenship of those arrested. It is important that the questions; who, what, where, when, and why are answered;
- Indicate notifications made either telephonically, by fax or E-mail (i.e. telephonic to Commissioner’s Situation Room, Office of Field Operations by fax). Provide the date, time, and telephone number;
- List the names of fatalities or those injured. Include, if known, the name of the next of kin and the status of the notification process (planning/in progress/ completed); and
- Indicate what action has been taken as a result of the incident (i.e., in the case of a narcotic seizure, “turned over to U.S. Immigration and Customs Enforcement for controlled delivery”). In the event of serious injury of employees, indicate the name and phone number of the hospital involved.

14.6. EMERGENCY PREPAREDNESS PROGRAM

14.6.1. General

- The U. S. Customs and Border Protection (CBP) Emergency Preparedness

Program (EPP) provides requirements for a viable EPP in compliance with Presidential Decision Directive 67 (PDD 67) and Federal Preparedness Circular 65 (FPC 65);

- The Emergency Preparedness Program provides guidance to all CBP personnel on emergency preparedness matters and establishes policy to facilitate the orderly continuation of CBP essential functions in the event of a serious incident. The [Emergency Preparedness Program 5290-010B](#) policy is applicable agency-wide.

14.6.2. Policy

- All CBP locations will perform the following:
 - Maintain effective, coordinated, integrated, and responsive emergency preparedness procedures and practices intended to maximize continuity of priority mission essential functions and the safety of CBP personnel. As such, all CBP facilities shall have a Continuity of Operations (COOP) Program/Plan and an Occupant Emergency Program/Plan (OEP). See [Chapter 15, Occupant Emergency Plans](#), for more information;
 - All office location Occupant Emergency Program/Plans (OEP) shall be in accordance with established guidelines set forth by the Office of Finance and compliant with state, local and tribal ordinances, as applicable.
- Shelter-in-Place (SIP):
 - One of the instructions you may be given in an emergency where hazardous materials may have been released into the atmosphere is to shelter-in-place (SIP). This is a precaution aimed to keep you safe while remaining indoors. (This is not the same thing as going to a shelter in case of a storm.) Shelter-in-place means selecting a small, interior room, with no or few windows, and taking refuge there. It does not mean sealing off your entire home or office building. If you are told to shelter-in-place, follow the instructions provided in this Fact Sheet;
 - Why you might need to shelter-in-place: Chemical, biological, or radiological contaminants may be released accidentally or intentionally into the environment. Should this occur, information will be provided by local authorities on television and radio stations on how to protect you and your family. Because information will most likely be provided on television and radio, it is important to keep a TV or radio on, even during the workday. The important thing is for you to follow instructions of local authorities and know what to do if they advise you to shelter-in-place;
 - Partnering with local authorities is critical because OEPs should not conflict with the plans of local community first responder protocol. In many locations, particularly outside major population centers, local officials may not recommend SIP planning because the risks in these areas do not justify this course of action.
 - Shelter in place resource links:

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- <http://redcross.tallytown.com/library/ShelterInPlaceAtYourOffice.pdf>
- <http://www.fema.gov/plan/prevent/saferoom/index.shtm>
- <http://www.ready.gov/business/plan/shelterplan.html>
- [National terror alert.com-shelter in place \(SIP\)](#)
- <http://www.opm.gov/emergency/>
- All Continuity of Operations (COOP) Plans, as well as office-specific COOP Implementation Plans, shall be developed using the Department of Homeland Security (DHS) Continuity of Operations template and instructions available on the Federal Emergency Management Agency's (FEMA) website at: <http://www.fema.gov/government/coop/index>;
- COOP/Program/Plans, including office-specific COOP Implementation Plans, shall be universal in outlining response and recovery strategies for any catastrophic incident, to include pandemic, in compliance with Federal Preparedness Circular (FPC-65); and
- COOP/Programs/Plans as well as office-specific COOP Implementation Plans shall be marked "For Official Use Only" (FOUO) and stored at the relevant Headquarters or field office location, emergency relocation site (ERS), Tele-work site and/or alternate work site (AWS) as appropriate to ensure continued availability if the primary location is rendered inaccessible. A copy must also be forwarded to the appropriate Headquarters Emergency Preparedness Coordinator (EPC). [Emergency Preparedness Program 5290-010B.](#)

14.7. EMERGENCY COMMUNICATIONS

- 14.7.1. This subsection describes available methods of communication that the CBP will use during an emergency.
- 14.7.2. Government Emergency Telecommunication Service (GETS). [CBP GETS Cards FAQs](#)
 - A Government Emergency Telecommunications Service (GETS) card is issued to those individuals who perform essential functions to maintain continuity of government posture before, during and after crisis situations;
 - The Government Emergency Telecommunications Service (GETS) is a White House-directed emergency phone service provided by the National Communications System (NCS) in the Cyber Security & Communications Division, National Protection and Programs of the Department of Homeland Security. GETS supports Federal, State, local, and tribal government, industry, and non-governmental organization (NGO) personnel in performing their National Security and Emergency Preparedness (NS/EP) missions. GETS provides emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN). It is intended to be used in an emergency or crisis situation when the PSTN is congested and the probability of completing a call over normal or other alternate telecommunication means has significantly decreased;

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- GETS is necessary because of the increasing reliance on telecommunications. The economic viability and technical feasibility of such advances as nationwide fiber optic networks, high-speed digital switching, and intelligent features have revolutionized the way we communicate. This growth has been accompanied by an increased vulnerability to network congestion and system failures. Although backup systems are in place, disruptions in service can still occur;
- GETS uses these major types of networks:
 - The local networks provided by Local Exchange Carriers (LECs) and wireless providers, such as cellular carriers and personal communications services (PCS);
 - The major long-distance networks provided by Interexchange Carriers (IXCs) - AT&T, MCI, and Sprint - including their international services; and
 - Government-leased networks, such as the Federal Technology Service (FTS), the Diplomatic Telecommunication Service (DTS), and the Defense Switched Network (DSN).
- GETS is accessed through a universal access number using common telephone equipment such as a standard desk set, STE, STU-III, facsimile, modem, or wireless phone. A prompt will direct the entry of your PIN and the destination telephone number. Once you are authenticated as a valid user, your call is identified as an NS/EP call and receives special treatment.

14.8. WIRELESS PRIORITY SERVICE (WPS)

14.8.1. A [Wireless Priority Service \(WPS\)](#) is provided to those individuals who perform essential functions to maintain continuity of government posture before, during, and after crisis situations.

14.8.2. Purpose:

- The goal of the Wireless Priority Service (WPS) is to provide an end-to-end nationwide wireless priority communications capability to key National Security and Emergency Preparedness (NS/EP) personnel during natural or man-made disasters or emergencies that cause congestion or outages in the Public Switched Telephone Network (PSTN). Eligible users (see criteria at <http://wps.ncs.gov>) are key Federal, State, local, and tribal government and critical industry personnel who have NS/EP missions. WPS is complementary to, and can be most effective when used in conjunction with, (GETS) to ensure a high probability of call completions in both the wireline and wireless portions of the PSTN. WPS serves NS/EP communications needs while minimizing impact on consumer access to the public wireless infrastructure.

14.8.3. Background

- In 2000, the Federal Communications Commission (FCC) issued a Report and Order (R&O) for Priority Access Service (PAS) authorizing wireless carriers to offer the service on a voluntary basis and with much needed liability protections. Following the September 11 attacks, the White House directed delivery of a

[RETURN TO TOP](#)

wireless priority service to NS/EP leadership during emergency situations. WPS service began on a single carrier in limited areas in early 2002 and has since expanded to full nationwide coverage on most of the major cellular networks. The National Communications System has the responsibility for the day-to-day administration of WPS, with oversight responsibilities residing with the FCC.

14.8.4. Key issues

- Priority Treatment
 - WPS is an enhancement to basic cellular service that allows NS/EP calls to queue for the next available radio channel. Priority handling is provided from call origination, through the cellular and public telephone networks, and to the dialed destination.
- Access Authorization
 - WPS is invoked by dialing 272 prior to the destination number on cellular devices with the WPS feature.
- Ubiquitous Coverage: WPS is available nationwide in Global System for Mobile Communications (GSM) and in Code Division Multiple Access (CDMA) networks. For the latest information on WPS carriers and coverage areas, see “Carriers” on <http://wps.ncs.gov>.
- Service Authorization
 - To subscribe to WPS, see “First Time Requestor” on the WPS site shown above.
- Contact Information: Please e-mail Rebel.McFetridge@DHS.gov or Linda.A.Jenkins@cbp.dhs.gov for assistance. (Rebel McFetridge is the WPS point of contact at 703-921-7712 and Linda Jenkins is the alternate point of contact at 703-921-7474).

14.9. CBP EMPLOYEE EMERGENCY CHECK-IN PROCEDURES

- 14.9.1. See [CBP Employee Emergency Check-in Procedures](#) for detailed process information.
- 14.9.2. U.S. Customs and Border Protection (CBP) continues to stand committed to accounting for every employee and their immediate family and providing necessary assistance as quickly as possible after any significant incident. In addition to existing local reporting procedures and policies, CBP has developed a supplemental emergency incident toll-free number and employee check-in website. ([CBP Incident Employee Check-In Online Submission Site](#)) Through these procedures and systems, CBP employees are able to check-in, provide current contact information and report their availability to work. All affected CBP personnel are requested to check-in within 72 hours of an incident.
- 14.9.3. If you are directed or forced to evacuate your residence of record and relocate to an alternate site, please report your status and updated contact information as soon as possible.

[RETURN TO TOP](#)

- 14.9.4. During an incident, three options are available for check-in:
- 14.9.5. Local Reporting Procedures: Employees report their status utilizing existing local reporting procedures and policies. Your local managers will coordinate with headquarters to insure your information is populated into the master database. Reporting in via locally established procedures is always the preferred method.
- 14.9.6. When reporting in via locally established procedures is not feasible or possible for whatever reasons, you can now report your post incident status via the following supplemental options:
- Via CBP. gov “Employee Emergency Web Check-in”: (referenced above), employees report their status via the website check-in system. This is accessible 24 hours a day, 7 days a week at the U.S. Customs and Border Protection website (www.cbp.gov) and no special password is required. Online help is available with detailed instructions on how to complete the form;
 - If the Internet is not available, please proceed to the next option:
 - Toll-Free Call-In Number: 1-877-CBP-4804 or (1-877-227-4804)
These systems are monitored only during a declared emergency incident

14.10. EMERGENCY PLANNING AND RESPONSE

- 14.10.1. The purpose of this section is to give guidelines for threat conditions at any Customs and Border Protection (CBP) controlled facility.
- A threat condition is defined as “an operating posture that dictates an increase of the level of security.” The purpose of the threat condition system is to establish standardized protective measures for a wide range of threats and to facilitate disseminating appropriate, timely and standardized information for the coordination and support of CBP crisis or contingency activities.
- 14.10.2. To provide guidance on the implementation of the U.S. Customs and Border Protection (CBP) Threat Condition Protective Measures as they correlate to the five Threat Conditions outlined in the Homeland Security Advisory System (HSAS). Threat Condition Protective Measures as outlined below in [Section 14.15](#).
- 14.10.3. Policy
- It is the policy of CBP to thwart the operations of terrorist organizations by detecting, disrupting, and preventing the cross-border travel of terrorists, terrorist funding, and terrorist implements, including Weapons of Mass Destruction (WMD) and their precursors.
- 14.10.4. By Presidential Directive, the HSAS is binding on the Executive Branch. To implement the HSAS, CBP has developed a detailed plan with five Threat Conditions, related to the five Threat Conditions outlined below in [Section 14.15](#), to respond to security threats against the United States.
- 14.10.5. The five Threat Conditions identified in this manual are binding on all CBP offices. Each office shall carry out a plan of protective measures in accordance with this policy. These plans shall have several preplanned sets of responses to each

[RETURN TO TOP](#)

particular threat level to facilitate a rapid, appropriate, coordinated, and tailored response.

- 14.10.6. Threat Conditions are to be assigned by the Secretary, Department of Homeland Security (DHS).
- 14.10.7. Secretary DHS, is responsible for determining whether to publicly announce Threat Conditions, for ensuring that State and local government officials and law enforcement authorities are provided the most relevant and timely information, and for establishing a process to convey relevant information to Federal, State, and local government officials, law enforcement authorities, and the private sector.
- 14.10.8. The assignment of a Threat Condition shall prompt the implementation of an appropriate set of Protective Measures to reduce CBP vulnerability or increase CBP ability to respond during a period of heightened alert.
- 14.10.9. Each CBP office shall be responsible for taking all appropriate proactive steps to reduce the vulnerability of its personnel and facilities within its specific jurisdiction and increase ability to respond to specific and nonspecific threats.
- 14.10.10. By Presidential Directive, all Federal department and agency heads shall submit an annual written report to the President, through the Secretary, DHS, describing the steps they have taken to develop and implement appropriate Protective Measures for each Threat Condition.

14.11. DEFINITIONS

- 14.11.1. The terms “Threat Condition Green” and “Low Condition” as used in the HSAS and this manual, both refer to a Threat Condition in which there is a low risk of terrorist attacks against the United States Homeland.
- 14.11.2. The terms “Threat Condition Blue” and “Guarded Condition” as used in the HSAS and this manual, both refer to a Threat Condition in which there is a general risk of terrorist attacks against the United States Homeland.
- 14.11.3. The terms “Threat Condition Yellow” and “Elevated Condition” as used in the HSAS and this manual, both refer to a Threat Condition in which there is a significant risk of terrorist attacks against the United States Homeland.
- 14.11.4. The terms “Threat Condition Orange” and “High Condition” as used in the HSAS and this manual, both refer to a Threat Condition in which there is a high risk of terrorist attacks against the United States Homeland.
- 14.11.5. The terms “Threat Condition Red” and “Severe Condition” as used in the HSAS and this manual, both refer to a Threat Condition in which there is a severe risk of terrorist attacks against the United States Homeland. It is not intended for Protective Measures implemented at this threat level to be sustained for substantial periods of time.
- 14.11.6. For the purpose of this manual, “anti-terrorism” is defined as preventative measures; “counter-terrorism” is defined as investigative or proactive enforcement measures.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

14.12. PROCEDURES

14.12.1. Agency-wide procedures. Notification of changes to Threat Conditions and the implementation of Protective Measures will be made through the Office of the Commissioner in consultation with the Assistant Commissioner (AC) of the Office of Field Operations (OFO), the Chief, Office of Border Patrol (OBP), and other relevant offices. When possible, offices should coordinate the appropriate set of Protective Measures.

- All CBP communication plans and communication activities with Federal, State, and local law enforcement agencies and officials, the Congress, and the private sector, must be undertaken with approval from or in accordance with a determination by the Secretary, DHS, regarding dissemination of information regarding the threat. Communication with external entities will be conducted in accordance with CBP current policies.

14.12.2. Low Condition/Green (Agency): Under Low Condition, CBP may, at its discretion, institute the following general Protective Measures:

- Develop and deliver anti-terrorism training to CBP personnel;
- Review, update, and distribute office occupant emergency and evacuation plans; ensure compliance with Customs Directive 5290-010A, Emergency Preparedness – Notification and Coordination (9/21/2001);
- Assess and exercise joint standard operating procedures (SOPs) and support agreements with appropriate external agency partners;
- Review and revise security procedures and port or geographically specific (i.e., Northern Border, Atlantic Coast) threat assessments; and
- Perform weekly communication checks to ensure maximum operational capability.

14.12.3. Guarded Condition/Blue (Agency): In addition to the Protective Measures identified in the preceding level, CBP at its discretion may institute the following general Protective Measures:

- Disseminate heightened Threat Condition status to all CBP assets;
- Operate with a heightened awareness supported by focused intelligence reporting as available; and
- Plan for the potential deployment of personnel and other resources to critical locations should the threat level escalate.

14.12.4. Elevated Condition/Yellow (Agency): In addition to the Protective Measures identified in the preceding levels, CBP, at its discretion, may institute the following general Protective Measures:

- Coordinate Occupant Emergency Plans (OEPs) and Continuity of Operations Plans (COOPs) with other Federal, State, and local entities as necessary;
- Consider restrictions on nonessential travel by CBP employees;

- Consider canceling annual leave and placing personnel on “on-call” status;
- Consider suspension of nonessential programs, duties, training, and surveys;
- Coordinate heightened Protective Measures between CBP offices (i.e., OFO, Office of Information and Technology (OIT), Office of Intelligence, Office of Border Patrol (OBP)) and external agency partners (i.e., Immigration and Customs Enforcement (ICE), Transportation and Security Administration (TSA), and the U.S Coast Guard (USCG));
- Apply heightened security measures at CBP facilities commensurate with threat;
- Ensure critical tactical communications systems are operational and technical infrastructure is protected;
- Engage international counterpart agencies (including Canadian and Mexican counterparts) regarding heightened alert status and potential operational impact; and
- Institute Headquarters-directed, tailored communication plans to advise key congressional members and staff, the trade, media, and public of the elevated Threat Condition and the associated implications.

14.12.5. High Condition/Orange (Agency): In addition to the Protective Measures identified in the preceding levels, CBP, at its discretion, may institute the following general Protective Measures:

- Identify ports for potential closing; close as ordered by the Commissioner
- Restrict annual leave and nonessential travel as necessary;
- Activate part-time employees commensurate with threat;
- Restrict access to CBP facilities;
- Increase coordination with Federal, State, and local entities, including placement of temporary liaison assets with appropriate agencies;
- Identify increased threat areas in order to deploy personnel and inspection technology resources commensurate with the threat;
- Implement plans to augment personnel with other agency resources;
- Suspend nonessential programs, duties, training, and surveys;
- Perform communications checks with the National Law Enforcement Communication Center (NLECC)/SECTOR to ensure the integrity of the communication systems, as necessary; and
- Advise key congressional members and staff, the trade, media, and public of the elevated Threat Condition and the associated implications.

14.12.6. Severe Condition/Red (Agency): In addition to the Protective Measures identified in the preceding levels, CBP, at its discretion, may institute the following general Protective Measures:

- Close selected points of entry (POE) and potentially entire regions or borders (air, land, and sea), as ordered by the Commissioner;

- Implement maximum passenger inspections and cargo examinations-up to 100 percent of all passengers and cargo arriving and departing the U.S.;
- Implement Occupant Emergency Plans (OEPs) and Continuity of Operations Plan (COOPs) as appropriate;
- Further restrict access to CBP facilities to necessary personnel only.
- Redirect resources (personnel, tools & technology, and equipment) to high risk offices and ports of entry;
- Cancel annual leave for personnel; and
- Maintain regular communication with NLECC/SECTOR, field staff, media, trade, the Congress, and public to ensure all affected parties receive accurate and timely information.

14.13. RESPONSIBILITIES

- 14.13.1. The Commissioner shall have policy oversight regarding the CBP Threat Condition policy and procedures.
- 14.13.2. Within CBP, the Commissioner is the sole authority for closing Customs and Immigration ports of entry (POEs), unless otherwise delegated to appropriate officials.
- 14.13.3. The Director, Office of Anti-Terrorism (OAT), is responsible for the coordination of the CBP Threat Condition Protective Measures to achieve alignment with the HSAS.
- 14.13.4. The OAT will coordinate the annual review of CBP Protective Measures to the national HSAS and prepare a report for the Commissioner to submit to the President, through the Secretary, DHS.
- 14.13.5. The OAT will coordinate with relevant offices to develop specific Protective Measures for each Threat Condition level for implementation of this Directive.
- 14.13.6. The Office of Intelligence will be the point of contact, in coordination with the OAT, with the national intelligence community.
- 14.13.7. Designated Officials (DO) will ensure plans are initially developed in conjunction with Building Security Committees (BSCs) and are reviewed, updated, and re-signed by the Chair of the BSC at least as often as the periodic Building Security Assessment (BSA) is conducted. Regional Headquarters will maintain copies of the plans in such a manner as to facilitate and verify rapid implementation in case of an alert level change.
- 14.13.8. In accordance with established policy on memorandums of agreement and understanding, the DO may enter into informal and formal agreements with state and local law enforcement agencies to support actions required by the Plans.
- 14.13.9. DO will develop procedures to ensure plans are implemented when the alert level changes, including:
 - Notification to the BSC of changes to the Homeland Security Alert level and other conditions which merit a corresponding change in security measures;

[RETURN TO TOP](#)

- Coordination with BSCs and GSA with regard to implementing increased alert levels absent a declaration by the Department of Homeland Security;
- Notification of suppliers of services and equipment to be delivered upon implementation (e.g., notifying guard companies of an increased staffing requirement);
- Notification of state and local agencies supporting the Plan;
- Establishing appropriate contracting mechanisms to facilitate rapid delivery of services in support of the Plan;
- Providing other support as agreed to in the Plan to implement countermeasures (i.e., increased K-9 patrols, etc.);
- Verification that countermeasures have been implemented; and,
- De-escalation once the Alert Level is reduced.

14.13.10. FPS Inspectors. Inspectors will work with BSCs to determine and document specific actions that need to be taken at each building to implement the Alert Guidelines. Inspectors may also be responsible for verifying increased countermeasures have been implemented when the alert level is increased.

14.13.11. Building Security Committee (BSC). The BSC will work with the Inspector to develop the Plan. The BSC is responsible for signing the Plan, indicating concurrence with the actions to be taken. If the Plan requires funding to implement, such as increased guard presence, the BSC will be responsible for coordinating funding among tenant agencies in advance of implementation.

14.13.12. Delegation of responsibilities. The responsibility for development of these plans may be delegated to an agency in writing upon request and with concurrence of the region for a specific building or Headquarters for an agency-wide delegation.

14.13.13. Procedures. The following is guidance for countermeasures to be considered. As appropriate, each countermeasure should be addressed in the Plan. Some actions are minimum recommendations (X) for specific building security levels and others should be applied as deemed appropriate (*) based on the threat and personnel available.

14.13.14. Alert Level GREEN. Associated with the Low/Normal Condition identified by the Homeland Security Advisory System. The following protective measures apply to conditions involving a general threat of a possible emergency situation and warrant only a routine security posture.

14.14. BEST PRACTICES

14.14.1. In conjunction with the above CBP HSAS policy IA/SMD has provided in-depth facility protective measures based on the appropriate HSAS threat levels below. See [Section 14.15](#) for this detailed information.

14.14.2. Create a Building Specific Security Plan using this template as a guide along with CBP Policy CBP DIRECTIVE NO. 3340-026B, [CBP Threat Condition Protective](#)

Measures (HSAS).

14.14.3. Implement these best practices upon:

- Automatically in response to change in the DHS HSAS Alert Level nationally, locally, or with other respect to the facility (i.e., transportation sector);
- By the Commissioner of the CBP nationally or regionally; and
- At a specific facility(ies) upon recommendation of IA/SMD and with concurrence of the BSC chairperson OR Designated Official (DO) upon receipt of specific threat information regarding the building meriting its implementation (i.e., a planned demonstration).

14.14.4. A copy of each Plan will be maintained by the DO. The Plan will be marked and controlled as For Official Use Only, in accordance with DHS policy on Sensitive but Unclassified Information. It will also be marked “Law Enforcement Sensitive,” which although not a control mechanism, indicates the sensitivity and type of information in the plan.

14.14.5. Initial Plans for each building will be developed as part of the next Building Security Assessment (BSA) cycle following implementation of this policy. The plans will be reviewed with the BSC and revised as necessary as part of each recurring BSA or upon request of the BSC Chairperson.

14.15. PROTECTIVE MEASURES

14.15.1. Alert Level Green

Green Protective Measures	Building Security Level			
	I	II	III	IV
At regular intervals, remind agency representatives to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for suspicious vehicles on or adjacent to CBP property. Watch for abandoned parcels or suitcases and any unusual activity.	X	X	X	X
Ensure the building manager or representative has access to building plans and occupant emergency plans at all times. Ensure BSCs, property managers and tenant agencies periodically review and ensure the availability of building floor plans, Occupant Emergency Plans (OEPs), Continuity of Operations Plans (COOPs) and other essential emergency information.	X	X	X	X
Recommend buildings, rooms, and storage areas not in regular use be secured.	X	X	X	X
Review all plans and requirements related to introduction of higher security level.	X	X	X	X
Require US Government picture identification for Federal employees, contractors, and a current valid government picture identification (such as a drivers license, state identification card, passport, or immigration card) system for visitors.	*	*	*	X
Inspect and search all packages, handbags, and other containers, except those persons displaying US Government credentials. Deny entrance to all persons who refuse this inspection.	*	*	*	X
Check basement, engineering spaces, heating and air conditioning ducts, shrubbery, and potential entry points such as roof openings, steam and other utility tunnels, doors and windows.	*	*	*	X
Refine and exercise preplanned proactive measures. Ensure personnel receive training on Homeland Security Alert System (HSAS) and department or agency-specific protective measures. Regularly assess facilities for vulnerabilities and take measures to reduce them.	*	*	*	X
Consult local authorities on the threat and mutual antiterrorism measures.	*	*	*	*

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Green Protective Measures	Building Security Level			
	I	II	III	IV
Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.	*	*	*	*
After normal duty hours ensure exterior and parking areas floodlights are operating properly to discourage intruders.	*	*	*	*
Train personnel on Homeland Security Advisory System (HSAS), and CBP specific protective measures.			X	X
Regularly assess facilities for vulnerabilities and apply countermeasures.			X	X
Ensure IA/SMD Regional, District Security Officers have fluid Security Surveys of CBP facilities.			X	X
Occupants should note any suspicious vehicles on, near or adjacent to INS property; and report any unattended vehicles or items in the immediate area.			X	X
Should actual or suspected explosives in these vehicles or items be discovered, personnel should be advised to REPORT and DO NOT TOUCH.			X	X
Encourage occupants to secure rooms, doors, and windows of office suites that are not regularly used.			X	X
Increase security spot-checks of vehicles and persons entering property.			X	X

14.15.2. Alert Level Blue

- Alert Level BLUE is associated with the Guarded Threat Condition as identified by the Homeland Security Advisory System. These measures apply when there is a general threat of a possible emergency situation involving activity against tenants, visitors, and facilities; the nature and extent of the situation is unpredictable; and the circumstances do not justify full implementation of Alert Level Yellow. It indicates a general risk of terrorist attacks. These measures must be capable of being maintained indefinitely.

Blue Protective Measures	Building Security Level			
	I	II	III	IV
Continue, or introduce, all measures listed in Alert Level Green.	X	X	X	X
Review all plans and requirements related to introduction of higher security level.	X	X	X	X
Check communications with designated emergency response or command locations. Review and update emergency response procedures and provide the public with necessary information.	X	X	X	X
Review and coordinate security measures for high-risk personnel as appropriate.	X	X	X	X
Increase security spot checks of vehicles and persons entering CBP property.	*	*	*	X
Continue to apply the previous Threat Condition measures.			X	X
Check and/or establish communications with designated emergency response or command locations.			X	X
Review and update emergency response procedures.			X	X
Provide the CBP occupants with necessary information relative to the increase in security measures to avoid panic derived from rumors.			X	X
Keep all persons involved with Counter-Terrorism contingency plans or in key positions on call.			X	X

Blue Protective Measures	Building Security Level			
	I	II	III	IV
Increase scrutiny of visitors to CBP facilities.			X	X
Security Guards will:			X	X
• During normal duty hours, be alert for suspicious persons, packages and activity.			X	X
• During non-duty hours, deny access to persons who do not display appropriate Government identification.			X	X
• Ensure all doors to the facility are secured.			X	X
• Receive current threat information during guard mount.			X	X
• Enforce No Parking restrictions.			X	X
• Increase unannounced security spot checks (inspection of personal identification, vehicle registration, and the contents of items i.e. suitcases, briefcases and other containers).			X	X
• Randomly conduct in-depth inspections of deliveries.			X	X
• Move unchecked vehicles and objects at least 100 feet from building.			X	X
• Advise personnel to report the following to Security:			X	X
o Suspicious persons, specifically those carrying any type of container.			X	X
o Suspicious person surveilling, monitoring, photographing, or asking questions about facility operations and/or security processes, procedures, countermeasures.			X	X
o Unidentified vehicles parked or operated in a suspicious manner on or in the vicinity of the facility.			X	X
• Abandoned parcels or containers.			X	X
• Throughout the workday, inspect the interior and exterior of the facility.			X	X
• Site specific measures identified by IA/SMD will be implemented as directed.			X	X
• At regular intervals, check basement, engineering spaces, heating and air conditioning ducts, shrubbery, and potential entry points such as roof openings, steam and other utility tunnels, doors and windows for signs of unauthorized entry, tampering or intrusion.			X	X
• Increase security operations commensurate with the threat and plan for the potential deployment of personnel and other resources to critical locations should the threat level escalate.			X	X
Building Security Committees (BSCs) and tenant agencies will review and verify all local Occupant Emergency Plans (OEPs), Continuity Of Operations Plans (COOPs), and ensure that communications equipment and contact lists (i.e. radios, telephones, public address systems, and fax number lists) are up-to-date and functioning properly.			X	X
Tenant agencies brief appropriate employees of actions required under procedures contained in agency-specific OEPs and COOPs.			X	X

14.15.3. Alert Level Yellow

- Alert Level YELLOW is associated with the Elevated Threat Condition as identified by the Homeland Security Advisory System. These measures apply when there is an increased and more predictable threat of an emergency

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

situation. It indicates a significant risk of terrorist attack.

Yellow Protective Measures	Building Security Level			
	I	II	III	IV
Continue, or introduce, all measures listed in Alert Level Blue and warn tenants of any other potential form of terrorist attack.	X	X	X	X
Keep all personnel involved in implementing antiterrorist contingency plans on call.	X	X	X	X
Check plans for implementation of the next alert level.	X	X	X	X
At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.	X	X	X	X
In the early stage inform the Building Security Committees of actions to be taken. Explain reasons for actions.	X	X	X	X
Increase contacts with individuals responsible for activities such as child care centers, and agencies with a high amount of personal threat reporting, to build confidence among staff.	*	X	X	X
Make tenants aware of the general situation in order to stop rumors and prevent unnecessary alarm.	*	X	X	X
Move unchecked cars and objects (e.g. crates, trash containers) at least 100 feet from buildings. Use other measures where distance cannot be achieved.	*	*	*	X
Request personnel who handle mail and deliveries to scrutinize incoming material (above the regular examination process) for letter or parcel bombs.	*	*	*	X
Implement additional security measures for high-risk personnel as appropriate.	*	*	*	X
Consult local authorities on threat and mutual antiterrorism measures.	*	*	*	X
Increase surveillance of critical facilities.	*	*	*	X
After normal duty hours require all employees and visitors sign the building register upon entering and leaving the building.	*	*	*	X
Increase surveillance/counter-surveillance of critical locations.			X	X
Coordinate emergency plans with nearby jurisdictions.			X	X
Limit access points to the absolute minimum necessary for continued operations.			X	X
Access points to be determined by IA/SMD.			X	X
Increase security patrols to the maximum sustainable rate.			X	X
Place temporary barriers and obstacles to control traffic flow from persons and vehicles.			X	X
Verify the identity of all personnel entering the facility.			X	X
Inspect all building passes or identification for tampering or counterfeiting.			X	X
Visually inspect the interior of all vehicles and the exterior of all containers.			X	X
Increase frequency of detailed vehicle inspections (trunk, undercarriage, glove box).			X	X
Consult local authorities regarding street closures adjacent to facilities.			X	X
Restrict outside parking to 300 feet from building.			X	X
Visually inspect the interior of all vehicles parked within 30 yards of the CBP facilities.			X	X
Site-specific measures identified in the Site Security Plan/Program shall be implemented.			X	X
Other measures as identified by the Regional or Field Security Officer or CBP will be implemented as directed.			X	X
During all duty hours, CBP employees must personally escort visitors and will constantly remain responsible for their whereabouts for the duration of their visit.			X	X
Intensified vehicle and visitor inspections at all facilities as required by increased threat level.			X	X
Coordinate increased activities with Federal and local authorities and other area emergency agencies.			X	X
Review security procedures to ensure they are commensurate with the threat.			X	X
Inspect parking areas near the facility and instruct personnel to be alert to unattended vehicles, packages, portable containers or suspicious objects. Instruct personnel to challenge all individuals lingering in the vicinity of a facility to establish their purpose or determine if they have official business with building tenants.			X	X
Inform tenant agency representatives and Building Security Committees (BSCs) of actions to be taken.			X	X
Implement additional security measures for designated personnel as appropriate.			X	X

Yellow Protective Measures	Building Security Level			
	I	II	III	IV
FPS and CBP implement their own contingency and emergency plans as appropriate.			X	X
BSCs and tenant representatives, provide tenants information relative to the increase in security measures to prevent unnecessary alarm derived from rumors.			X	X
Require that Identification cards of individuals being screened to be touched by security personnel as part of the screening process.			X	X
<u>At frequent and irregular intervals, inspect the interior and exterior of occupied buildings for suspicious objects.</u>			X	X
Place all personnel involved in implementation of antiterrorist contingency plans on call.			X	X

14.15.4. Alert Level Orange

- Alert Level ORANGE is associated with the High Threat Condition as identified by the Homeland Security Advisory System. These measures apply when an emergency situation occurs and/or intelligence is received indicating that some form of emergency situation against tenants and facilities is likely. Implementation of measures in this alert level for more than a short period probably will create hardship, affect the operations of our tenants, and significantly increase operating costs. It indicates a high risk of terrorist attacks.

Orange Protective Measures	Building Security Level			
	I	II	III	IV
Continue, or introduce, all measures listed in Alert Level Yellow.	X	X	X	X
All FPS personnel are subject to emergency recall.	X	X	X	X
Limit facility access points to the absolute minimum.	X	X	X	X
Protect all designated vulnerable points.	X	X	X	X
Strictly enforce control of entry. Randomly search vehicles.	*	*	X	X
Increase patrol tempo of security guards, police officers, and Inspectors.	*	*	X	X
Erect barriers and obstacles to control traffic flow.	*	*	*	X
Consult local authorities about closing public streets that might make facilities more vulnerable to attacks.	*	*	*	X
Restrict outside vehicular parking to 300 feet of the facility. Use other measures where distance cannot be achieved.	*	*	*	X
Coordinate necessary security efforts with armed forces and other law enforcement agencies.	*	*	X	X
Coordinate necessary security efforts with armed forces and/or law enforcement agencies.			X	X
Prepare to continue operations at an alternate work site with a dispersed workforce.			X	X
Security Guards will:			X	X
Be alert for suspicious persons, packages and activities.			X	X
Deny building lobby access to persons who do not display an appropriate CBP building pass or suitable identification.			X	X
Visually check under and around all vehicles parked adjacent to any facility.			X	X

Orange Protective Measures	Building Security Level			
	I	II	III	IV
Observe all vehicles for suspicious persons or activities. Suspicious vehicles where no persons are noted to be in attendance or affiliation is established will be visually checked for evidence of explosives, incendiary, or biological devices, or other dangerous items.			X	X
Make arrangements to have the vehicle removed from the vicinity of the facility. If the vehicle is parked and in a public space, the Security Guard will request assistance from the appropriate law enforcement agency.			X	X
Security Guards may be augmented with additional personnel.			X	X
All persons including employees will walk through the metal detector.			X	X
All packages, briefcases, purses, or other containers being brought into the facility will be X-rayed or visually inspected to ensure no contraband or dangerous substance enters the facility.			X	X
During all hours, all doors will be secured.			X	X
Restrict access to essential personnel only.			X	X
If at all possible, increase temporary physical barriers to the entire perimeter of the facility.			X	X
Restrict all vehicles from stopping at any time adjacent to the facility (with the exception of traffic enforcement).			X	X
Site-specific measures identified in the Site Security Plan/Program will be implemented. Other measures as identified by the IA/SMD will be implemented as directed.			X	X
That Building Security Committees (BSCs) or agency representatives with real property authority may restrict public access to essential facilities. Consider restricting public events to agency occupants only.			X	X
Federal and local authorities and other area emergency agencies be contacted to coordinate increases in security activities.			X	X
Patrol frequency of security guards and police officers be increased as appropriate.			X	X
All previously designated vulnerability points must receive additional security and further limit access points to the facility. Limit facility access points to the absolute minimum.			X	X
Erect barriers and obstacles to control both the flow of individuals (particularly visitors) and vehicle access where appropriate.			X	X
Consult local authorities about the feasibility of closing public streets to minimize risks posed by car bomb attacks.			X	X
Where possible, restrict outside vehicular parking to as far as possible from the facility. Use other measures (i.e. towing) where distance cannot be achieved.			X	X
Where possible, implement counter-surveillance.			X	X
Personnel who handle mail and deliveries will scrutinize incoming material (above the regular examination process) for letter or parcel explosive devices or other hazardous material.			X	X
Inspect facilities for means of surreptitious access that could bypass security checkpoints; secure or apply adequate countermeasures accordingly.			X	X
Search all vehicles and their contents before allowing entrance into the building.			X	X
Pre-position and prepare any specially trained teams or resources for possible deployment or mobilization. FPS will pre-position specially trained teams as appropriate.			X	X

14.15.5. Alert Level Red

- Alert Level RED is associated with the Severe Threat Condition as identified by the Homeland Security Advisory System. These actions apply in the immediate area where an emergency situation has occurred and/or when intelligence has been received that an emergency condition against a specific location or person is imminent. It indicates a severe risk of terrorist attacks. Because these actions are normally only declared as a localized condition, each action is listed below as deemed appropriate based on the threat and personnel available.

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

Red Protective Measures	Building Security Level			
	I	II	III	IV
Continue, or introduce actions listed in Alert Level Orange.	X	X	X	X
Search all vehicles and their contents before allowing entrance to the building.	*	*	*	*
Control access and implement positive identification of all individuals with no exceptions.	*	*	*	*
Thoroughly search all suitcases, briefcases, and packages brought into the building.	*	*	*	*
Make frequent checks of the exterior of buildings and parking areas under GSA jurisdiction.	*	*	*	*
Coordinate the possible closing of public streets and facilities with local authorities.	*	*	*	*
Activate the facility OEP.	*	*	*	*
FPS should assign emergency response personnel and pre-position specialty trained teams. Monitor, redirect, and/or constrain transportation systems.	*	*	*	*
Increase and/or redirect personnel to address critical emergency needs.	*	*	*	*
Consider closing of facility to visitors or entirely	*	*	*	*
Assign emergency response personnel and pre-position specialty trained teams.			X	X
Monitor, redirect or constrain transportation systems.			X	X
Transport high-level employees to alternate work sites.			X	X
Augment security officers and/or security staff (guards) as necessary.			X	X
Allow only emergency vehicles into facility, and check those vehicles.			X	X
Control access and implement positive identification of all individuals (emergency essential at this point), no exceptions.			X	X
Cease processing additional visitors for entry.			X	X
All persons, including employees, shall walk through the metal detector. All packages, briefcases, handbags and other containers being brought into the building shall be X-rayed or visually inspected to ensure no contraband enters the building. Packages not inspected shall not be left with Security Guards or receptionists; the carrier shall remove such packages.			X	X
Activate the facility Occupancy Emergency Plan.			X	X
All persons shall sign in and out upon entering and leaving the building. In those facilities where card readers are installed, the record of the automated system will suffice.			X	X
All vehicle traffic to the garage will cease and the doors will be secured.			X	X
All loading dock activities (deliveries) will cease and the doors will be secured.			X	X
Site specific measures identified in the Site Security Plan/Program will be implemented. Other measures as identified by IA/SMD will be implemented as directed.			X	X
Security Guards shall visually check under and around all vehicles parked adjacent to the building. Security Guards shall observe all vehicles for suspicious persons or situations. In those cases where the presence of a vehicle can not be explained (owner is not present and the vehicle has no obvious affiliation), inspect the vehicle for explosive, incendiary, chemical, biological devices, or other dangerous items and arrange to have the vehicle removed from the vicinity of the facility, soft targets and other sensitive areas as soon as possible. If the suspicious vehicle is parked in public space, Security Guards shall take appropriate action, which may include requesting assistance from the appropriate law enforcement agency.			X	X
Require full access control and positive identification of all individuals with no exceptions.			X	X
Perform frequent checks of building exteriors and parking areas.			X	X
Mobilize or activate any specially trained teams or resources. Monitor, redirect, and/or constrain transportation systems as necessary.			X	X
As necessary, review and activate Safety and Security Plans. This includes but would not be limited to: Physical Security Plans, Information Security Plans, Occupant Emergency Plans (OEPs), COOPs, Disaster Response Plans and Emergency Responder Plans.			X	X
Consider closing the facility.			X	X

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

14.16. AUTHORITIES/REFERENCES

- o Homeland Security Presidential Directive-3
- o (HSPD) (Mar. 11, 2002) (as amended by HSPD-5, Feb.28, 2003);
- o 19 USC 1318 (2002);
- o Homeland Security Act of 2002, Pub. L. No. 107-96, 116 Stat. 2135;
- o Customs Directive 3340-021 Antiterrorism, 1/11/2000;
- o Customs Directive 5290-010A Emergency Preparedness, 9/21/2001;
- o Customs Directive 5410-001, Customs News Media Policy 10/10/1986;
- o CIS HB 1400-05A, Information Systems Security Policy and Procedures Handbook;
- o 15 CFR §730-774;
- o 18 U.S.C §831, §886, §841-848, §921-§922, §1028, §2331, §2332a-d, and §2339 A-B;
- o 19 USC§482, §318, §1461, §1581, §1582, §1644, and §2462 (b) (2) (F);
- o 19 CFR §4, §18, §101, §122-§123;
- o 22 U.S.C §401, §406, §408, §421-§422, §2349aa-2, §2349aa-8, §2349aa-9, §2371, §2778, §2780, §2797, §2798, §2799aa, and §2797a-b;
- o 26 USC §5801-§5802; 42 USC §262, §2077, §2099, §2111, §2122, §2133, §2138, §2156, and §2157;
- o 49 USC §44904 and §46312;
- o 50 USC §1701-1706;
- o 50 USC app.1-44.





CHAPTER 15: OCCUPANT EMERGENCY PLAN (OEP)

15.1. PURPOSE AND SCOPE

- 15.1.1. All Department of Homeland Security (DHS) CBP facilities are required to have an Occupant Emergency Plan (OEP) in place to provide for the safety and protection of DHS/CBP personnel, contractors and visitors across a wide range of potential emergencies. Emergency response guidelines also safeguard property, equipment, classified information, and vital records and data, as well as focusing on the continued execution of essential functions during a crisis. The OEP provides DHS/CBP personnel, contractors and visitors with information on how to prepare for, respond to, and recover from an emergency.
- 15.1.2. One common means of protection is evacuation to a predetermined area away from the DHS/CBP facility. The main objective of an OEP is to minimize danger to life and property during an emergency.
- 15.1.3. In GSA-controlled facilities, emergency procedures are normally provided by the GSA Building Manager or local officials of the FPS. If the procedures have not been provided, the DHS/CBP Designated Official (DO) and the facilities Occupant Emergency Coordinator (OEC) is responsible for providing the procedures. In multi-tenant buildings the organization will include representatives from all organizations. GSA shall assist in the establishment and maintenance of such plans and organizations. See the [GSA's Occupant Emergency Program Guide](#) for in-depth information.
- 15.1.4. In accordance with the Federal Property Management Regulations (FPMR) 101-20.103-4, "Occupant Emergency Program," immediate, positive and orderly action must be taken to safeguard life and property in Federal facilities during emergencies. An emergency can be any unexpected situation that requires prompt action to protect life and property. Examples of emergencies can include, but are not limited to: fires; explosions; bomb threats, civil disorders; chemical, biological, and radiological incidents; medical emergencies; natural disasters; structural failures; direct threat to a major computer facility; immediate threat of compromise of classified information; and accidental or man-made disasters.
- 15.1.5. The OEP will apply to all DHS/CBP personnel and other CBP occupants such as contractors and visitors occupying CBP space. The guidance in the OEP will cover normal operating hours and non-operational hours and provide specific emergency evacuation instructions to Federal building occupants. The OEP will provide a plan of action for an immediate and short-term response to an emergency and allow building occupants to evacuate quickly and safely. All buildings occupied by DHS/CBP employees will have a designated Occupant Emergency Coordinator. The guidelines provided within the facilities OEP will be reviewed and updated annually, as required by [41 CFR § 102-74.240](#).
- 15.1.6. [Ready.gov](#) is an Internet site hosting a Federal Employee's Emergency Guide, as is A Federal Employee's Family Preparedness Guide, and Federal Manager's/Decision Maker's Emergency Guide; all of these are guides for preparing for deliberate, accidental and natural emergencies at work and at home. In the event of an

[RETURN TO TOP](#)

emergency, all employees must attempt to remain calm, exercise sound judgment, follow emergency plans, and adhere to the orders of appropriate personnel, including supervisors, properly identified Monitors, fire and emergency medical personnel and security officers.

15.1.7. See the [OEP Guide](#) and [OEP Template](#), which are included in this policy handbook.

15.2. AUTHORITY/REFERENCES.

- [The Homeland Security Act of 2002, PL 107-296, enacted 11/25/02](#)
- Department of Justice Vulnerability Assessment of Federal Facilities, June 1995
- [29 CFR §1910](#), Occupational Safety and Health Standards
- [40 CFR §1315](#), Law Enforcement authority of Secretary of Homeland Security Protection of Public Property
- [41 CFR §101-20: Public Contracts and Property Management](#)
- [41 CFR §102-74.240 Facility Management](#)
- [41 CFR §102-74.360 Safety and Environmental Management](#)
- [41 CFR §102-80 Safety and Environmental Management](#)
- [GSA Occupant Emergency Program Guide, Mar 2002](#)
- [MD 11030.1 Physical Security of Facilities and Real Property](#)
- [MD 11042.1 Safeguarding Sensitive but Unclassified \(For Official Use Only\) Information](#)
- [MD 11044 Protection of Classified National Security Information Program Management](#)
- [Federal Employee's Family Preparedness Guide](#)
- [The US Office of Personnel Management Emergency Preparedness Guide](#)

15.3. RESPONSIBILITIES

15.3.1. OEPs are developed at the facility level, specific to the geographic location and structural design of the building. General Services Administration (GSA) owned facilities maintain plans based on the GSA OEP template.





CHAPTER 16: FIREARMS AND AMMUNITION

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

16.1. GENERAL

- 16.1.1. Only those CBP employees who are authorized in writing and issued a credential to bear firearms by the Commissioner of U.S. Customs and Border Protection (CBP) shall carry a firearm in the performance of their official duties. This authorization is granted only after the employees have successfully completed approved basic firearms training and have been issued the appropriate credential.
- 16.1.2. Physical Security Specialists, armed employees of the Security Management Division, as well as employees who perform inspections or other related duties (mixed tour, part-time, intermittent, seasonal, temporary and status quo), and any other armed CBP employees who do not complete basic firearms training, must attend an approved training course as specified by the Director, Firearms and Tactical Training Division (FTTD), Office of Training and Development (OTD). Authorization to carry a firearm cannot be granted until this requirement has been met.
- 16.1.3. The statutory authority for CBP employees to carry service-issued or service-authorized firearms is contained in [19 USC §1589a](#).

16.2. ASSIGNED FIREARMS

- 16.2.1. All firearms shall be held in a secure, locked, and safe storage area when not assigned to an employee, while awaiting repair, or other circumstance resulting in the firearms being in the custody of a firearms custodian. The following minimum guidelines should be followed when storing firearms and ammunition:
- Firearms should be stored in GSA-approved security containers, vaults, or Underwriters Laboratories (UL)-labeled safes or weapons cabinets;
 - Access to firearm storage containers should be limited to those employees designated to issue such firearms. The firearm storage area should be designated at least a controlled area to restrict unauthorized access to the area. If more than 35 firearms are stored, an alarm with a guard or police response is recommended. For further information, see [Appendix 10, Storage of Weapons and Ammunitions](#).

16.3. AUTHORITIES

- [Firearms and Use of Force Handbook \(HB 4500-01A, December 2001\)](#);
- [U.S. Customs Firearms and Use of Force Training Policy \(CD 4510-017A, December 2001\)](#);
- [Land Border Inspectional Safety Policy \(CD 5290-007A, June 2001\)](#); and
- [Airport and Seaport Inspectional Safety Policy \(CD 5290-006, June 1999\)](#).



CHAPTER 17: PROTECTION OF BUILDING DOCUMENTATION

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

17.1. GENERAL

- 17.1.1. In order to reduce or minimize the risk that sensitive paper and electronic building information will not be used for dangerous or illegal purposes, this chapter covers CBP security polices, procedures and responsibilities for the protection of Sensitive but Unclassified (SBU) paper and electronic building information and the dissemination of SBU paper and electronic building information; owned, leased, or delegated facilities.
- 17.1.2. [Information Security \(INFOSEC\)](#) programs and procedures already exist to protect information assets. However, information generally available to the public as well as certain detectable activities may reveal the existence of, and sometimes details about, classified or sensitive information or undertakings. Such indicators may assist those seeking to neutralize or exploit U.S. Government actions. For more information, refer to:
- [CBP Website: Sensitive Security Information \(SSI\) – Directive, Regulations, Quick Reference](#)
 - [CBP Website: Information Security/For Official Use Only \(INFOSEC/FOUO\)](#)
 - [National Security Decision Directive 298 - National Operations Security Program](#)
- 17.1.3. OMB requires safeguarding data and documents that are sensitive enough to require protection but that may not otherwise be designated as classified information. “Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information.”
- [OMB Circular A-130, Management of Federal Information Resources](#)
 - [Laws and Regulations Governing the Protection of Sensitive But Unclassified Information](#)
- 17.2. DEFINITIONS**
- 17.2.1. DUNS: [Data Universal Numbering System \(DUNS\)](#) is a unique nine-digit numbering system that is used to identify a business.
- 17.2.2. For Official Use Only. The caveat “FOR OFFICIAL USE ONLY” will be used to identify sensitive but unclassified information within the DHS community that is not otherwise specifically described and governed by statute or regulation. For reference, see [DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified \(For Official Use Only\) Information](#)
- 17.2.3. OMB. The Office of Management and Budget (OMB) is one of the agencies of the Executive Branch of the U.S. Government. Its predominant mission is to assist the President in overseeing the preparation of the Federal budget and to supervise its administration in Executive Branch agencies.
- 17.2.4. Sensitive but Unclassified (SBU)
- SBU is the formal designation for information that, by law or regulation, requires some form of protection but is outside the formal system of classification, in

accordance with [Executive Order 12958](#), Classified National Security Information as amended, and [DHS MD 11042.1](#) Safeguarding Sensitive But Unclassified (For Official Use Only) Information. This information may be exempt from public disclosure under the Freedom of Information Act (5 USC §552) and/or the Privacy Act (5 USC §552a).

17.3. TYPES OF INFORMATION FOR DOCUMENT SECURITY

17.3.1. *Sensitive but Unclassified (SBU) Building Information*

- SBU includes but is not limited to paper and/or electronic documentation of the physical facility information identified below. Building designs (such as floor plans), construction plans (site drawings/ blueprints) and specifications, renovation/alteration plans, equipment plans and locations, building operating plans, information used for building service contracts and/or contract guard services, or any other information considered a security risk, for all CBP-owned, leased, or delegated facilities, shall be considered covered under this category. Specifically (but not exclusively), it includes:
 - Location of secure functions in the facility; detainees' secure circulation paths (both vertical and horizontal); cell blocks; sally ports; parking; security areas and childcare; major computer processing areas or other customer sensitive processing areas (e.g. major photo or computer labs, etc);
 - Location of all utilities: heating, ventilation, air conditioning, information technology (IT) systems, location of air intake vents, water sources, gas lines, plumbing lines, building automation systems, power distribution systems, emergency generation equipment, Uninterruptible power sources (UPS), security and fire alarm systems, routes and annunciation panels;
 - Location and type of structural framing for the building and any information regarding structural analysis or building security, blast mitigation analysis, counter terrorism methods taken to protect the occupants and building; and
 - Information regarding security systems or strategies of any kind (i.e., CCTV, IDS locations) or security guards (e.g. number and location).

17.3.2. *Non-Sensitive Unclassified Building Information*

- Information regarding the building that may be made available for limited public dissemination under the following conditions:
 - Building elevation or other drawings of new or existing buildings will not show or label information defined under the SBU categories given above and in the Public Buildings Services (PBS) order [PBS 3490.1](#), Document Security for Sensitive But Unclassified Paper and Electronic Building Information;
 - Interior photographs that are limited to publicly accessible space or have been cleared for publication by CBP.
- Conceptual space planning drawings with floor layouts may be made available for:
 - Presentations to professional designers (architect/engineers, etc.);

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- o Professional schools for educational purposes;
- o Community planning groups participating in the design of new Federal space;
- o Professional print publications if specific SBU building information (structural columns, utilities, etc.) is not shown; and
- o Secure circulation routes, secure elevator locations, etc. are shown as generic space with no wall partitions (such as a block of unpartitioned space).
- Generic concept (bubble) diagrams may be shown to convey information for a non-specific building; and
- Detailed floor layout drawings of any kind for specific buildings will not be made available over the public internet or in public presentations or print media, such as brochures, magazines, books, etc.

Note: It is the responsibility of the disseminator to use good judgment and to apply the principle that the more open the forum, the more generic/conceptual the information must be.

17.4. ELECTRONIC MEDIA

- 17.4.1. Electronic media includes magnetic tape reels, disk packs, diskettes, compact discs, removable hard disks, disk cartridges, optical disks, paper tape, reels, magnetic cards, tape cassettes, micro cassettes, videotapes, and any other device on which data are stored and that normally is removable from the system by the user or operator.

17.5. MARKING/LABELING OF INFORMATION

- 17.5.1. In accordance with DHS MD 11042.1, information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of FOUO markings on materials does not relieve the holder from safeguarding responsibilities. Where the FOUO marking is not present on materials known by the holder to be FOUO, the holder of the material will protect it as FOUO. Other sensitive information protected by statute or regulation, e.g., Protected Critical Information Infrastructure (PCII) and Sensitive Security Information (SSI), etc., will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with the guidance provided for the type of information need not be additionally marked FOUO.
- 17.5.2. Prominently mark the bottom of the front cover, first page, title page, back cover and each individual page containing FOUO information with the caveat "[FOR OFFICIAL USE ONLY](#)."
- 17.5.3. All SBU building information, either in electronic or paper formats will have imprinted on the top of every page the following information:

**PROPERTY OF THE UNITED STATES GOVERNMENT
FOR OFFICIAL USE ONLY
Do not remove this notice
Properly destroy documents when no longer needed**

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- 17.5.4. The following paragraph, as set by Public Buildings Services (PBS) order [PBS 3490.1](#), will be included on the cover page of the information (such as the cover page on the set of construction drawings and on the cover page of the specifications) and on the label of all magnetic media:

**PROPERTY OF THE UNITED STATES GOVERNMENT
COPYING, DISSEMINATION, OR DISTRIBUTION OF THESE
DRAWINGS, PLANS, OR SPECIFICATIONS TO UNAUTHORIZED USERS IS PROHIBITED
Do not remove this notice
Properly destroy documents when no longer needed**

- 17.5.5. The previous two statements will be prominently labeled in bold type in a size appropriate for the document. On a set of construction drawings, for example, the statements shall be in a minimum of 14-point bold type.
- 17.5.6. Blueprints, engineering drawings, charts, and maps containing sensitive information will be marked "Sensitive But Unclassified - Building Information" or "SBU-BI" at the top and bottom of each page. If the blueprints, drawings, charts, or maps are large enough that they are likely to be rolled or folded, "Sensitive But Unclassified - Building Information" will be placed so that the marking is visible when the item is rolled or folded.
- 17.5.7. Materials being transmitted to recipients outside of DHS, for example, other Federal agencies, State or local officials, etc. who may not be aware of what the FOUO label represents, shall include the following additional notice on the front page of the document(s):

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 USC 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

- 17.5.8. Electronic Media, Computer storage media, i.e., disks, tapes, removable drives, etc., containing FOUO information will be marked "FOR OFFICIAL USE ONLY."

17.6. RESPONSIBLE CARE FOR DISSEMINATION OF SBU BUILDING INFORMATION

- 17.6.1. CBP personnel or others authorized to disseminate SBU building information (which includes flow down dissemination by prime/general contractors, subcontractors, suppliers, architects/engineers, Federal agencies, lessors, private sector plan rooms, State and local governments, print shops/reprographic firms, etc.) will obtain a signed copy of the Document Security Notice by authorized users of SBU building information agreeing to exercise reasonable care when handling SBU building

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

documents.

17.6.2. The Document Security Notice form may be found at the end of Public Buildings Services (PBS) order [PBS 3490.1](#).

17.6.3. “Reasonable care” is defined as:

- *Limiting Dissemination To Authorized Users.* Dissemination of information shall only be made upon determination that the recipient is authorized to receive it. The need-to-know criteria determine whether authorization is granted. Those with a need-to-know are other Federal Government agencies (who shall make requests through their agency management), and non-Government entities that are specifically granted access for the conduct of business on behalf of or with CBP. This includes DHS or other Federal agencies, organizations or individuals such as architects and engineers, consultants, contractors, subcontractors, suppliers, plan rooms, and others that the contractor deems necessary in order to submit an offer/bid or to complete the work or contract, as well as maintenance and repair contractors and equipment service contractors.

Note: It is the responsibility of the person or firm disseminating the information to assure that the recipient is an authorized user and to keep the Document Security Notice records of recipients.

17.6.4. Authorized users will provide identification as set forth below:

- Valid Identification for Federal government users. Valid identification of authorized government users receiving SBU building information shall be verification of government employment;
- Valid identification for non-government users. Authorized non-government users shall provide valid identification to receive SBU building information. Valid identification shall be all items (a) through (c), and including item (d), as necessary:
 - (a) A copy of a valid business license or other documentation granted by the state or local jurisdiction to conduct business;
 - (b) The license at a minimum will provide the name, address, phone number of the company, state of incorporation, and the name of the individual legally authorized to act for the company;
 - (c) The business will be of the type required to do the work;
 - (d) A general contractor’s license may be substituted for the business license in states that issue such licenses;
 - (e) In the rare cases where a business license is not available from the jurisdiction, the information will be provided and testified to by the submitter;
 - (f) Verification of a valid [Data Universal Numbering System \(DUNS\)](#) number against the company name listed on the business license or certification;

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

(g) Verification may be obtained by calling Dun & Bradstreet at 1-800-333-0505 or 703-807-5078 or to set up an account;

(h) A valid IRS tax ID number of the company requesting the information; and, as necessary:

- A valid picture state driver's license will be required of person(s) picking up SBU documents.

17.6.5. Prior to releasing any SBU building information the sender will verify that the individual(s) receiving or picking up the documentation are authorized by the company obtaining the documents.

17.6.6. SBU documents will not be released to any individual or firm who has not either previously or at the time of pickup supplied the required documentation as outlined above.

17.7. REPRODUCTION OF SBU INFORMATION

17.7.1. SBU documents may be reproduced without the permission of the originator to the extent necessary to carry out official CBP activities. Copies will be protected in the same manner as originals. In the event of a copy machine malfunction, the copy machine will be cleared and all paper paths checked for papers containing sensitive information.

17.8. STORAGE

17.8.1. All sensitive information existing in hard copy will be stored within a locked container in a limited or exclusion area, an access-controlled electronic environment or under the physical control of an authorized individual.

17.8.2. On occasions when an individual is traveling within the U.S. and limited or exclusion areas are not available, a locked container within a locked room will suffice (e.g., locked briefcase or suitcase within a locked hotel room or vehicle).

17.8.3. Sensitive information will not be taken outside the U.S., unless authorized by component authority.

17.8.4. Information handled electronically and transmitted over the network is at a higher risk of being released or altered. Sensitive information stored on the CBP network will be protected at a level that can ensure that only those who are authorized to view the information are allowed access (e.g., machine-generated passwords, encryption).

17.8.5. The CBP network systems shall maintain a high level of electronic protection (i.e., firewalls, intrusion detection, defense-in-depth, isolation of sensitive information, good practices network administration) to ensure the integrity of sensitive information and to prevent unauthorized access into these systems. Regular review of the protection methods used and system auditing are also critical to maintain protection of these systems.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

17.8.6. The physical elements of the network systems that store and transmit sensitive information or that have direct access to sensitive information will be secured within a restricted area. The more central the information resource is (e.g., a network or security system control room), the higher the level of access control that will be applied.

17.9. RECORD KEEPING

17.9.1. Individuals authorized to disseminate CBP SBU building information will require a signed Document Security Notice from individuals authorized to receive the information.

17.9.2. Records of the signed Document Security Notices will be maintained by the disseminator for 5 years.

17.9.3. At the completion of work, secondary and other disseminators will be required to turn over their Document Security Notice dissemination records to CBP.

17.9.4. Proprietary information owned by Architect/Engineers:

- All professional services consultants shall sign the Document Security Notice that documents containing SBU building information created under contract to the Federal government will be handled according to the procedures under this order;
- The Document Security Notice form may be found at the end of Protective Building Services' Order [PBS 3490.1](#).

17.9.5. Retaining and Destroying Documents

- The efforts required above will continue throughout the entire term of the contract and for whatever specific time thereafter as may be necessary;
- Necessary record copies for legal purposes (i.e., retained by the architect, engineer, or contractor) will be safeguarded against unauthorized use for the term of retention;
- Documents no longer needed will be destroyed:
 - After contract award;
 - After completion of any appeals process; and
 - Completion of the work.
- When a plan is revised, the old one is removed and destroyed and the current plan is filed in its place;
- Destruction will be accomplished by:
 - Burning or shredding hardcopy;
 - Electronic storage media shall be sanitized appropriately by overwriting or degaussing. Contact local IT security personnel for additional guidance;
 - Deleting and removing files from the electronic recycling bins;
 - Removing material from computer hard drives using a permanent erase

utility or similar software.

17.10. NOTICE OF DISPOSAL

- 17.10.1. For all contracts using SBU building information, the contractor will notify the CBP Contracting Officer that he and his subcontractors have properly disposed of the SBU building documents with the exception of the contractor's record copy at the time of release of claims to obtain final payment.

17.11. ENFORCEMENT

- 17.11.1. A violation may result in the cancellation of a person's conditional access to the information covered by the DHS Non-Disclosure Agreement, [Form 11000-6 \(08/04\)](#).
- 17.11.2. A record of violation may serve as a basis for denying an individual conditional access to other types of information, to include classified national security information.
- 17.11.3. Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information or other sanctions in accordance with applicable law and agency regulation.
- 17.11.4. The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.
- 17.11.5. Incidents involving FOUO in DHS IT systems will be reported to the organizational element Computer Security Incident Response Center in accordance with [MD 11042.1](#).
- 17.11.6. Employees or contractors who observe or become aware of the loss, compromise, suspected compromise or unauthorized disclosure of FOUO information will report it immediately, but not later than the next duty day to the originator and to CBP Internal Affairs (IA), CBP.Security@dhs.gov.

17.12. TRAINING

- 17.12.1. Although it is not mandatory, CBP offers a course on Awareness Training for Safeguarding Sensitive But Unclassified/For Official Use Only Information. A description of the training may be found on [the CBP web site](#). The course provides an overview for the safeguarding and handling of SBU information and supports Department-wide compliance with DHS Management Directive 11042.1 "Safeguarding Sensitive But Unclassified (For Official Use Only) Information."
- 17.12.2. Although not mandatory, CBP personnel who work with SBU are encouraged to complete this training to ensure information safeguarding requirements.
- 17.12.3. CUI Update: On May 9, 2008, the President issued a memorandum to the heads of all Executive Departments and Agencies titled "Designation and Sharing of Controlled Unclassified Information [CUI]." In the memorandum the President has ordered the adoption of CUI as the "...single, categorical designation henceforth

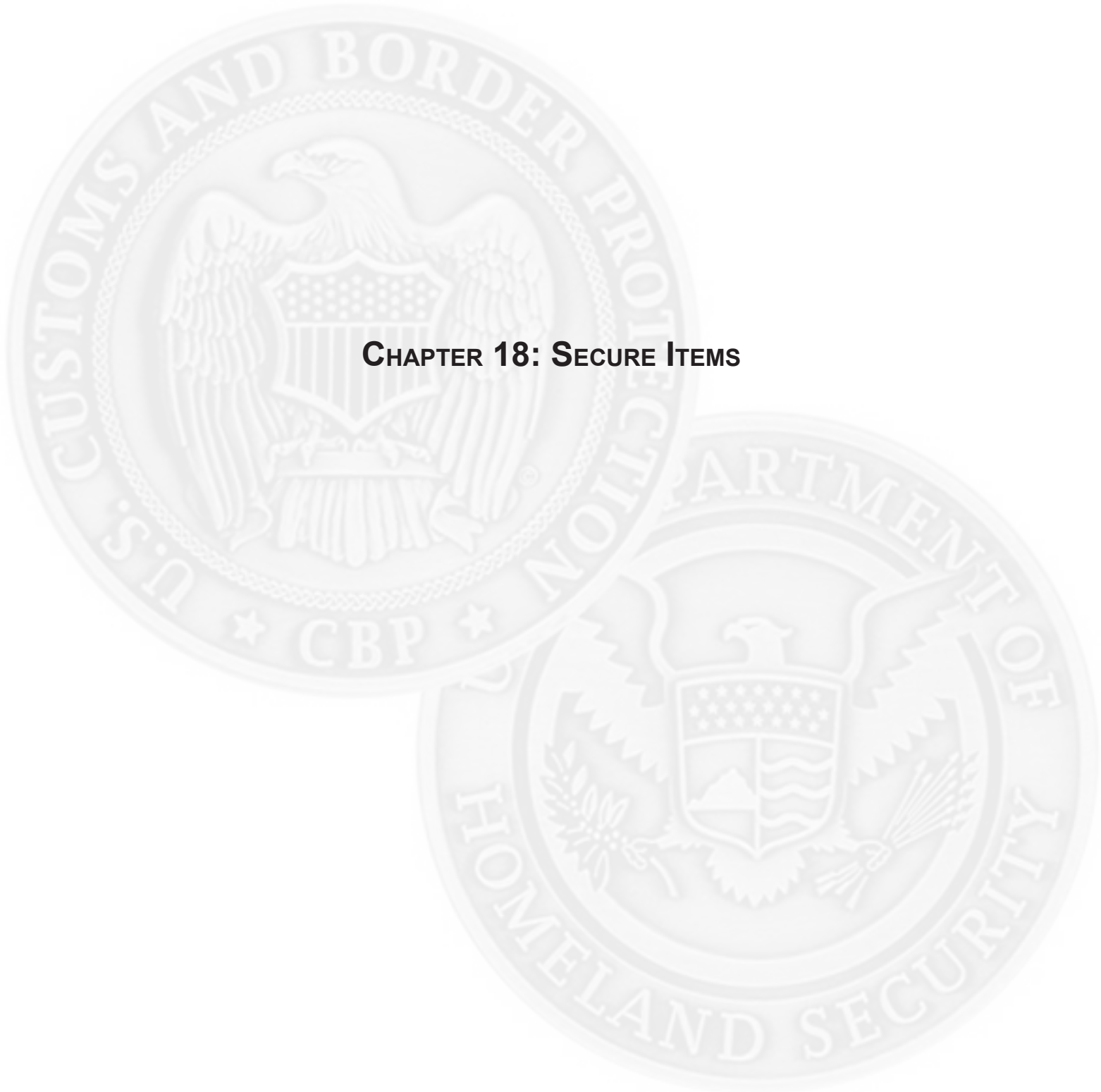
[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

throughout the executive branch for all information within the scope of that definition, which includes most information heretofore referred to as 'Sensitive But Unclassified' (SBU) in the Information Sharing Environment..." Over the coming days and months an inter-agency effort will commence under the leadership of the CUI Executive Agent, (the National Archives and Records Administration), and in coordination with a CUI Council consisting of senior representatives of all applicable Departments and Agencies (to include DHS), to define the CUI standards as reflected in the [President's memorandum](#), and publish CUI policy standards. Until such time as these policy standards are developed and published, it is important to emphasize that the manner in which we currently mark and safeguard information that is sensitive but unclassified, such as the use of the marking "For Official Use Only" as cited in DHS Management Directive 11042.1, will continue. The use of CUI and its associated markings shall not begin until appropriate policies have been published and those policies are supported by adequate training.

17.12.4. For further information on the Presidential Memorandum of May 9, 2008, see:

- [President's Memorandum Defining the Designation and Sharing of Controlled Unclassified Information \(CUI\) \(May 9, 2008\)](#)
- [Background on the Controlled Unclassified Information Framework \(May 20, 2008\) \(to Accompany Memorandum of May 9, 2008\)](#)
- [Memorandum: Establishment of the Controlled Unclassified Information Office Update to Memorandum of May 9, 2008 \(May 21, 2008\)](#)
- [DHS Controlled Unclassified Information \(CUI\) Implementation Plan \(April, 2008\)](#)
- [Controlled Unclassified Information \(CUI\) Framework](#) (Powerpoint Presentation). Updated May 12, 2008 (Office of the Chief Security Officer)



CHAPTER 18: SECURE ITEMS

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

18.1. GENERAL

- 18.1.1. CBP's missions include: processing of applicants for admission; issuing documents relating to the entry and status of an alien's right to enter, work or reside in the United States; and examining U.S. citizens. This chapter establishes CBP's uniform policy requirements for the physical security of items related to this mission.
- 18.1.2. Secure items include special formula inks, ink pads, stamps or any other designated items needed to perform the tasks outlined in 18.1. If lost or stolen, these items may intentionally be used to validate fraudulent entry into the United States. As such, they require strict control and must be secured to prevent loss, theft, fraud or counterfeiting.
- 18.1.3. It is the responsibility of every CBP employee to prevent or minimize the risk of loss, theft, fraud, counterfeiting, or compromise by providing oversight of the receipt, storage, issuance, and destruction of these secure items. It is the responsibility of each individual with access to and control of secure items to ensure that they are afforded the appropriate degree of protection as outlined in this chapter.
- Responsibilities
 - Headquarters Directors, Assistant Commissioners and Deputy Assistant Commissioners are responsible for coordination with the Director of Security, Internal Affairs/Security Management Division, on the development and execution of security procedures to safeguard secure items developed and used by their programs. In addition they are responsible for advising the IA/SMD Director of Security of any changes to the status of secure items;
 - The IA/SMD Director of Security is responsible for publication of procedures that provide comprehensive instruction on the security of secure items and oversight of the secure items program at all levels, to include locations and personnel involved in the manufacturing of secure items;
 - Directors of Field Operations (DFO) are responsible for the management and administration of the secure items program within their respective regions and ensuring resources are available to provide oversight at all subordinate levels.
 - DFOs are responsible for:
 - Ensuring that a Security Liaison or if one is not assigned, a collateral duty security officer is appointed to provide oversight of the secure items program.
 - Ensuring that accountable employees and sufficient alternates are trained and certification of appointments and training are maintained.
 - Providing IA/SMD and HQ OFO with designated authorized endorser and authorized requester positions per [section 18.3.1](#) of this chapter.
 - Regional Security Officer/ Security Liaison Responsibilities
 - Regional Security Officers (RSOs) are responsible for:
 - Ensuring policies and procedures relating to secure item accountability are

distributed and followed;

- Conducting periodic audits for receipt, accountability, storage, and disbursement of secure items; and
- Developing and managing a method for tracking and monitoring the conduct of other reviews, as provided below, conducted by the offices within their jurisdiction.
- Security Liaisons are responsible for:
 - Training newly appointed accountable employees and alternate accountable employees;
 - Ensuring appropriate safeguards are in effect for the safeguarding of secure items;
 - Ensuring appropriate audits and/or inventories as applicable, are performed as required;
 - Conducting a minimum of two unannounced reviews of the local secure items program during each fiscal year to ensure compliance with procedures;
 - Conducting a formal review of the local secure items program no later than September 30 of each year. The annual review will not count as one of the unannounced reviews.
- o Security Liaisons will ensure that instances of theft, loss, fraud, misuse, abuse, and negligence with regards to secure items are reported and investigated promptly, through channels, to IA/SMD. See [section 18.7.1](#).
- Accountable Employee (AE) Responsibilities
 - o Accountable employees and alternate accountable employees are responsible for knowledge and compliance with the requirements of this chapter and for maintaining the security and the integrity of the items for which they are responsible;
 - o Accountable employees and alternates will immediately report to their supervisor and the Regional Security Officer/ Security Liaison, any instance or suspected instance of theft, loss, fraud, misuse, abuse, or negligence with regards to the items they are responsible for or which are the responsibility of a coworker.
- Individual Responsibilities
 - o Supervisors are responsible for ensuring that all employees under their supervision who are authorized access to secure items, log books, automated auditing and tracking systems, databases, and other related materials, are fully cognizant of the applicable policies and safeguarding procedures. Supervisors are encouraged to include safeguarding of secure items as a critical element in an applicable subordinate's Performance Work Plan (PWP).
 - o Each employee authorized access to secure items, automated auditing and tracking systems and related materials:

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- Must comply with all policies and procedures, as stated in this chapter, concerning the protection and control of the items and materials to which they are authorized access;
- Must properly account for and safeguard all items and materials for which they are responsible, in accordance with the requirements of this chapter.
 - o May be subject to disciplinary action if, through negligence or willful disregard of procedures, they fail to properly account for and protect the items and/or materials to which they are authorized access, in accordance with the requirements of this chapter.

18.2. ACCESS

18.2.1. Prerequisites and Appointment of Accountable Employees

- Access to stock supplies of secure items is limited to specifically appointed and trained accountable employees that have a favorable adjudicated background investigation commensurate with their duty position. They shall be sufficiently trained on their responsibilities and officially appointed as the individual responsible for the protection, custody, or use of secure items. The accountable employees will ensure that all secure items issued, both used and unused, are accounted for at the end of each duty day.
 - o Accountable employee(s) and alternates will be designated in writing by the Director of Field Operations (DFO);
 - o An appropriately signed “Accountable Employee Certification” will be maintained on file by the appointing official for each appointee;
 - o Accountable employees and alternates will be provided training on the safeguarding and accountability aspects of secure items by the SL prior to assumption of duties and receive on the job training from an experienced accountable employee immediately upon assumption of duties;
 - o Accountable employees may issue a reasonable supply of items to the designated CBP officials or other persons responsible for the actual preparation of the items. The accountable employee will ensure that all secure items issued, both used and unused, are accounted for at the end of each duty day;
 - o Designated CBP officials and other persons issued secure items by the accountable employee will safeguard the items and maintain accountability until returned to the accountable employee;
 - o Security Liaisons will be afforded access in conjunction with the accountable employee, in order to carry out periodic and annual reviews;
 - o Automated database systems are not authorized as a primary means for the purpose of audit, tracking and inventory, but can be used in conjunction with logbooks and must be consistent with all logbook entries;
 - o Accountable employees will take necessary precautions to prevent unauthorized issuance, theft, or fraudulent use of the items and related

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

materials under their control;

- o No employee will concurrently have oversight, safeguarding, and processing responsibilities for secure items; and
- o Accountable employees and alternates will have sole access to the secure items and related materials for which they are responsible with the exception of those items and related items issued to CBP Designated Officials. (Refer to section 18.4 for specific storage requirements.)
- See [DHS Personnel Security and Suitability Program](#)
- See [CBP Personnel Security Handbook IA/PSD HB 1400-07 2006](#)

18.3. REQUISITION AND SHIPMENT

18.3.1. Requisition of Secure Items

- Only approved vendors identified by HQ Office of Field Operations (OFO) in coordination with IA/SMD shall be authorized to produce secure stamps and security ink;
- All routine requests for secure items will be made directly by the accountable employee using the [CBP Form 148](#); and
- The requisitioning officer will maintain copies on file of CBP Form 148, Request for Property or Services from the accountable employee for all secure items and related materials while the stamp is actively in use; the documentation will be filed after the stamp is no longer actively in use.

18.3.2. Shipment Procedures - Secure Items

- Shipment of secure items by the accountable employee:
 - o The accountable employee will coordinate shipment of the items with the approved vendor and by including:
 - Item number;
 - Serial number sequence (from/to);
 - Date of shipment;
 - Quantity being shipped;
 - Total number of cartons in shipment;
 - Address to which the shipment was sent; and
 - Expected shipment arrival.
 - o Upon receipt of all packages in the shipment, and verification that all items shipped were received, the accountable employee will ensure the packing slip (receipt) is signed and returned in the pre-addressed/postage paid envelope provided by the accountable employee;
 - o If a shipment is not received within 3 business days of the intended arrival date, the vendor will be contacted for confirmation of shipment and tracking action will be initiated with the shipping agent. Should a discrepancy exist,

[RETURN TO TOP](#)

refer to the reporting requirements provided in [section 18.7.1](#); and

- o If discrepancies exist, what was shipped and what was received must be immediately reconciled with the vendor. Should a discrepancy exist, follow reporting requirements provided in section 18.7.1.
- Shipment of secure items from an authorized and approved vendor:
 - o The accountable employee will fax a copy of CBP Form 148 marked “Advanced Notice of Shipment” to the intended recipient with the following information:
 - Item number
 - The serial number sequence (from/to)
 - Date of shipment
 - Quantity being shipped
 - Total number of cartons in shipment
 - Address to which the shipment was sent
 - Reasonable expectation of shipment time
 - o The vendor will include with the shipment the [CBP Form 148](#), Request for Property or Services. The CBP Form 148 will include the following:
 - Item number
 - Serial number sequence (from/to)
 - Quantity
 - Number of cartons in shipment
 - o Upon receipt of all packages in the shipment, and verification of contents against the CBP Form 148 has been completed, the recipient initial authorized requestor or endorser will sign the CBP Form 148 and return it to the accountable employee within 5 duty days following receipt.
 - o Bulk shipments of secure items received in the mail room may be:
 - Directly received for by the accountable employee;
 - The accountable employee shall conduct inventory upon receipt and re-seal shipment with a witness.

18.3.3. Shipment Methods

- Secure items will be appropriately packaged and secured with reinforced tape covering all seams to prevent inadvertent opening and provide evidence of tampering. The use of pilfer indicating tape, self voiding tape, and other chemically treated tamper indicating sealants is recommended;
- Packages will have no exterior markings, such as the item numbers and/or serial numbers that would provide an indication of the contents;
- All shipments of secure items must be by Registered Mail with return receipt requested, or U.S. Postal Service Express Mail and U.S. Postal Service

[RETURN TO TOP](#)

Registered Mail, as long as the Waiver of Signature and Indemnity block, item 11-B, on the U.S. Postal Service Express Mail Label shall not be completed; and cleared commercial carriers or cleared commercial messenger services. The use of street-side mail collection boxes is strictly prohibited;

- Shipment of security ink:
 - From the vendor:
 - Within the U.S. and to overseas possessions: Must be by a commercial means which allows for tracking, i.e., U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail, as long as the Waiver of Signature and Indemnity block, item 11-B, on the U.S. Postal Service Express Mail Label shall not be completed; and cleared commercial carriers or cleared commercial messenger services. The use of street-side mail collection boxes is strictly prohibited;
 - To offices located in Embassies and Consulates overseas for which there is an APO/FPO address, must be via U.S.
 - Registered Mail with return receipt:
 - To offices located overseas that are collocated with an Embassy or Consulate, but that do not have access to an APO/FPO system, must be via the responsible HQ program office for re-shipment via the Department of State Diplomatic pouch.
 - Shipment of security ink to offices that do not have access to a U.S. delivery system must be shipped to the parent District/Sector office and hand carried to the receiving office;
 - Shipment of security ink between CBP offices must be via U.S. Registered Mail with return receipt or diplomatic pouch.
 - Must contain an inventory receipt, [CBP Form 148](#).
 - Receiving office must sign the CBP Form 148 and fax it to the CBP National Mail Management Program.

18.4. STORAGE

18.4.1. Secure Items Storage

- Accountable Employee supply of secure items
 - Only accountable employee and their designated alternates shall have access to their supply of secure items. Containers used for the storage of secure items must not be accessible by persons other than the accountable employee or where the container is accessible by others, individual drawers must not be accessible. Each accountable employee's supply of secure items must be stored in at a minimum, one of the following:
 - GSA approved storage container used for the storage of high value items. (See [Chapter 10, Safes and Storage Equipment](#) of this handbook for more information on GSA-approved containers.)

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- Bulk Storage (Field Locations)
 - CBP offices that maintain a bulk storage supply of secure items where the size and/or quantity make storage in containers as stated above unfeasible, will store the items at a minimum in the following manner:
 - Multiple GSA approved containers within a secure area of a CBP facility or a strongroom. The strongroom must meet the following minimum standards: Please refer to Appendix 8.8 Strongrooms of this handbook for strongroom details and construction standards.
 - Storage of Other Security Items.
- Storage of logbooks, discs, reports and other hard copy data produced from an automated system; security ink; special formula stamp pads; and security stamps:
 - GSA approved storage container used for the storage of high value items. (For more information on GSA approved containers see [Chapter 10, Safes and Storage Equipment.](#))

18.4.2. Stand-Alone Storage Lockers for Designated Officials Issued Secure Items.

- Lockers and safes shall comply with the requirements of UL 1037 Anti-theft Alarms and Devices Residential Secure Containers. Safes shall be double walled minimum 20-gauge steel construction with a minimum 14-gauge steel door. Tilt-out drawers may be used for spaces where the depth of the lockers is a consideration. All secure items lockers shall have individual keyed dead bolt locks with one master key for all locks for the SLO;
- Safes may be securely mounted on the wall surface or recessed into the wall; and
- For items that must be secured in a desk or other location, a minimum 16-gauge metal safe with a combination dead bolt lock or key lock must be provided.

18.4.3. Accountability And Control

- The Security Liaison (SL) is responsible for storage of all security container combinations
 - Standard Form (SF) 700, Security Container Information, shall be used for this purpose;
 - Ensure the envelope is sealed and bears the accountable employee's signature and date across the seal;
 - Ensure the sealed envelopes are stored in a security container per [section 18.4.1](#) of this chapter;
 - Ensure the combinations are changed:
 - Annually;
 - Whenever there is a change in accountable employee(s);
 - When it has been necessary to effect access to the secure items and/or related materials in the case of an unforeseen absence of the employee;

[RETURN TO TOP](#)

or

- When the combination has otherwise been compromised.

- Keys:
 - Ensure the number of keys for each lock is entered in a log book;
 - Ensure extra keys are stored in the same manner as the combinations for the security containers.
- Re-key locks:
 - Whenever a key has been lost;
 - Whenever there is a possibility the key has been compromised; or
 - Upon change of accountable employee(s).
- Passwords to automated systems used for the inventory, tracking, and audit of secure items will be changed at a minimum every six months or when there has been a compromise or suspected compromise.

18.5. INVENTORY

18.5.1. General Requirements

- There is one acceptable method for maintaining an inventory of secure items, related materials, and security items:
 - Permanently bound book (logbook) consisting of manual, handwritten entries.
- CBP approved automated audit, tracking and inventory system are only authorized in conjunction with a permanently bound logbook and entries must be consistent with the entries in the logbook;
- A complete physical inventory of all secure items, secure stamps, security ink and pads, log books, and binders will be conducted:
 - Upon initial receipt of a shipment;
 - Upon appointment of a new accountable employee;
 - When loss, theft, abuse or misuse of the items is suspected; and
 - Monthly.
- Inventory
 - Inventories will be conducted by the SL in conjunction with the accountable employee(s) or alternate(s). Where the inventory is conducted due to a change in accountable employee, the SL and accountable employee, shall conduct the inventory;
 - Inventories of bulk storage items shall be conducted: The inventory official will inspect the box to ensure it has not been tampered with and place the date of the inventory and their initials directly on the box. This type of inspection will be completed with each subsequent inventory until the contents of the box are transferred, the box shows evidence of tampering or the box has been opened. In the latter instances a physical inventory by serial number of the

[RETURN TO TOP](#)

contents will be conducted; and

- o Upon receipt of bulk shipments and upon completion of an initial inspection to determine that all boxes sent were received and each box retains its original packing with no evidence of tampering, the boxes may be shrink-wrapped by pallet. The shrink-wrap must completely envelop the contents and be of such strength and resistance as to deter theft and show evidence of tampering should it occur. Where a bulk shipment is shrink-wrapped, the inventory may be done by pallet. Once the shrink-wrap is broken inventories will be done in accordance with policy described above.
- The date the inventory was conducted, the inventory results and the signature of the persons conducting the inventory will be entered in an inventory control logbook;
- Any discrepancies noted during the inventory will be investigated immediately. When discrepancies such as missing or illegible serial numbers are noted upon initial opening of a box that has not been opened since shipment from the approved authorized vendor, such as missing or illegible serial numbers, notification will be made within 72 hours to the AE through the applicable CBP office. Any discrepancy that can not be reconciled shall be reported in accordance with [section 18.7.1](#).

18.5.2. Accountability

- Accountable employees will maintain a handwritten record (logbook) of all secure items. The logbook requirements as stated below apply to user/issuance locations only.
- Logbook requirements system:
 - o Ensure logbooks are maintained in sequential order by each accountable employee. At a minimum, each log book will be identified by the secure item it pertains to and the time period covered.
 - o Ensure a separate book is maintained for:
 - Each type of secure item;
 - Security ink;
 - Special formula stamp pads; and
 - Each type of secure stamp.
- Ensure entries in the logbook are legibly written with permanent ink.
- All corrections must be initialed by the employee making the corrections.
- Logbook entries should include the following:
 - o Records of receipt for secure items, on the left hand side of the page, indicating:
 - Date received;
 - Quantity received;

- Serial numbers, if applicable;
- Total quantity in inventory; and
- Source of item.
- Records of receipt for security ink and special formula pads, on the left hand side of the page, indicating:
 - Date of receipt;
 - Quantity received; and
 - Source of shipment;
- Records of receipt for secure stamps, on the left hand side of the page, indicating:
 - Date of receipt;
 - Quantity received;
 - Source of shipment; and
 - Stamp number.
- Records of issuance of secure items, on the right hand side, indicating:
 - Date of issue;
 - To whom issued;
 - A-file number (if available);
 - Serial number of the item;
 - Pertinent distinguisher “M/D/V” (“M” indicates mailed; “D” indicates delivery; “V” indicates voided.); and
 - A space for who verified the issuance.
- Records of issuance of security ink and special formula pads, on the right hand side, indicating:
 - Date of issue;
 - Quantity issued; and
 - Recipient.
- Records of issuance of secure stamps, on the right hand side, indicating:
 - Date of issue;
 - Quantity issued;
 - Stamp number; and
 - Recipient.
- There should be a separate tab section in the back of the book for “Voids/ Destruction.”

18.5.3. Supervisory Verification

- Supervisors will verify on a weekly basis in the presence of the accountable

employee who completed the work:

- o Accuracy;
- o Validity;
- o Legibility of the information recorded in the logbook(s); and
- o That completed items are accounted for and/or properly disposed of
- Any discrepancies noted during the inventory will be investigated immediately. When discrepancies such as missing or illegible serial numbers are noted upon initial opening of a box that has not been opened since shipment from the authorized vendor such as missing or illegible serial numbers, notification will be made within 72 hours to the authorized employee through the applicable CBP office. Any discrepancy that can not be reconciled shall be reported in accordance with [section 18.7.1](#).

18.6. DESTRUCTION

18.6.1. Destruction Of Logbooks And Automated Products

- Logbooks will be considered active and will remain on site until every item recorded is retired, completely used, destroyed or no longer used to prevent theft or loss. Logbooks that no longer have any actively used item identified will be archived for historical purposes and will not be destroyed;

18.6.2. Disks

- Database inventory information is only utilized in conjunction with logbooks and any printed data may be purged and destroyed;
- See the [NSA/CSS Evaluated Products List for High Security Crosscut Paper Shredders](#).
 - o Discs containing secure items information and related materials data will be stored in accordance with the storage requirements identified in [section 18.4.1](#);
 - o Destruction of data bases, disc and hard drives will be destroyed, erased, or overwritten in accordance with HB 1400-05C [CBP HB 1400-05C Information Systems Security Handbook](#).
 - o Witnessing and a record of destruction will be prepared as specified in the following sections.

18.6.3. Destruction Of Secure Items

- Secure items will be destroyed by:
 - o Shredding;
 - o Burning; and
 - o Pulping or pulverizing.
- A record of the destruction will be maintained that includes:
 - o Name of the item;

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- o Item number;
- o Item serial number;
- o Signatures of the Security Liaison (SL) destruction official and witness;
- o Date of the destruction; and
- o Method of destruction.
- In the case of lifted/surrendered secure items include:
 - o Name of the individual to whom the item was issued.

18.6.4. Destruction Of Other Security Items

- Special formula ink will be destroyed as follows:
 - o Bulk inventories of special formula ink will not be destroyed without appropriate authorization of the accountable employee and SL;
 - o Destruction must be by dilution and disposing of the mixture in an environmentally safe manner. Destruction officials must contact local environmental officials to determine proper methods of disposal.
- Stamps will be destroyed by complete obliteration of the face of the stamp that renders the stamp unusable.
 - o Records of destruction will be maintained that include:
 - Brand name or manufacturer’s identification for special formula ink;
 - Ink color;
 - Volume (in fluid ounces) of ink;
 - Stamp type;
 - Stamp serial number;
 - Date of destruction; and
 - Signatures of destruction official and witness.

18.7. REPORTING REQUIREMENTS

18.7.1. Loss or Theft

- Responsibilities of Discoverer:
 - o The loss or theft of secure items will be reported by the person discovering it no later than the next duty day following discovery;
 - o The initial report will be made to the supervisor, the Security Liaison and the Regional Security Officer; and
 - o The discoverer will provide as many details as known and will not delay reporting in order to gather more information.
- Fraud, Abuse, Misuse Of Secure Items:
 - o Instances of fraud, abuse, and/or misuse of secure items by CBP employees must be reported to a supervisor, Security Liaison, Office of the Inspector General, as soon as it is suspected;

- o Persons receiving reports of fraud, abuse, or misuse by CBP employees will refer the complaint to the Joint Intake Center (JIC).
- Responsibilities of the Security Liaison:
 - o The Security Liaison receiving the initial report will immediately notify the following offices and initiate a preliminary inquiry. Immediate notification may initially be telephonic or via e-Mail and shall be followed up by e-Mail (for CBP notifications).
 - Head of the local CBP office;
 - Regional Security Officer;
 - CBP/IA/SMD;
 - Local FBI office; and
 - Local law enforcement authorities (Federal Protective Service (FPS) or civil law enforcement authorities, as applicable), if circumstances warrant. Circumstances that would warrant notification of local law enforcement authorities includes evidence of forced entry or other criminal activity.
 - Other agencies or offices as deemed appropriate by the security officer or as instructed by IA/SMD.
 - o Within 24 hours of the initial report, the Security Liaison will prepare a written preliminary report detailing the circumstances surrounding the loss or theft; notifications and contacts made since discovery of the loss or theft; and detailed information on the type, quantity, and serial numbers of the items lost or stolen, or missing;
 - o The Security Liaison will continue the preliminary inquiry until it has been determined that further inquiry will provide no additional information. The Security Liaison will prepare a final report and submit it to CBP/IA/SMD through the regional security office.
- Responsibilities of Regional Security Officers:
 - o If not conducting the preliminary inquiry, provide advice and assistance to the Security Liaison conducting the inquiry;
 - o Coordinate any actions required at the regional level.
- Responsibilities of CBP/IA/SMD:
 - o Provide advice and assistance to the Security Liaison conducting the inquiry;
 - o Review preliminary and final inquiry reports and coordinate further inquiry as deemed necessary;
 - o Coordinate additional actions and notifications with applicable CBP Headquarters program offices;
 - o Provide copies of inquiry reports to the Joint In Take Center (JIC); and
 - o Ensure CBP-wide Alerts are issued, per paragraph 2 below, by the Headquarters element of the program office responsible for the item in coordination with CBP/IA/SMD.

- The procedures for reporting the loss or theft of security ink, special formula pads, security stamps, and logbooks will be as stated above with the exception that notification will not be made to the local office of the FBI unless directed by CBP/IA/SMD.

18.7.2. Notification

- The DFO that experienced loss or theft, in coordination with CBP/IA/SMD shall immediately notify the (ICE) Office of Investigations 1-866-DHS-2-ICE and CBP Office of Internal Affairs (202-325-0110) CBP.Security@dhs.gov, of any attempt of any unauthorized persons to obtain information regarding the security features of the stamps or information on the stamps or process. The DFO and Security Liaison shall assist with any civil or criminal investigation and agrees to participate in Operation Bogus by immediately notifying ICE Forensic Document Laboratory telephone number (703-285-2482) of all attempts by unauthorized persons to obtain genuine stamps or similar reproductions;
- Operation BOGUS (Block Orders to Generate Unauthorized Stamps/seals) was initiated by the Forensic Document Lab (FDL) in 1988 to identify and prevent individuals and other entities from manufacturing, possessing or otherwise procuring fraudulent domestic and foreign stamps and seals relating to immigration or for use in obtaining an immigration benefit. The ICE prosecutes violations under [18 USC 1028](#), [18 USC 1546](#) and other applicable sections. Vendors (stamp and seal manufacturers) participating in Operation Bogus notify the FDL of any orders they receive that they suspect may be intended for fraudulent purposes; and
- The FDL is staffed 7 days-a-week (including holidays), Monday through Friday, between the hours of 6:00am and 8:30pm (Eastern Time), on Saturday, Sunday, and all Federal holidays from 10:00am to 6:30pm. For after-hours emergencies, contact the ICE Operations Center at (866) 514-2423.
 - o You can phone or fax the FDL at:
 - Phone: (703) 285-2482
 - Fax : (703) 285-2208

18.7.3. Alert Notices

- The Director of Field Operations (DFO) that experienced loss or theft, in coordination with CBP/IA/SMD, is responsible for preparing and dispatching the broadcast. A copy of the broadcast will be provided to CBP/IA/SMD for inclusion in the inquiry report;
- When deemed appropriate by CBP/IA/SMD, Alert Notices will be broadcast to all CBP activities having an interest in the loss or theft of secure items;
- At a minimum, the broadcast will identify the items that were lost or stolen, where they were lost or stolen, the item type, the serial numbers or stamp numbers, and total quantity.
 - o Provide copies of inquiry reports to the Joint intake Center (JIC)

- o JIC can be contacted:
- o Via e-mail: JOINT.INTAKE@cbp.dhs.gov
- o Toll Free: 1-877-246-8253
- o Local DC area: (202) 344-1016
- o Fax: (202) 344-3380 or 3390
- o Ensure DHS and or CBP broadcasts are issued
- When deemed appropriate, IA/SMD will request that the Commissioner's Situation Room send a CBP broadcast to all DFOs advising of the loss or theft of the secure item(s).
 - o Prepare a Significant Incident Report (SIR) Form 6.

18.7.4. Final Inquiry Reports

- The final inquiry report on the loss or theft of secure items, security ink, special formula pads, secure stamps and logbooks will, at a minimum, include the following:
 - o Serial number(s) of items, stamps, logbooks, as applicable;
 - o Date of the incident, if known;
 - o Date of discovery;
 - o Detailed narrative of the circumstances surrounding the loss or theft;
 - o Notifications made and actions taken by the inquiry officer and others involved in the incident;
 - o Cause of the incident (if it can be determined); and
 - o Recommendations to prevent similar incidents from occurring in the future.

18.7.5. Recovery Of Lost/Stolen Secure Items:

- Prepare an initial recovery report or a [CBP SIR Form 6](#) containing:
 - o Date of recovery;
 - o Circumstance surrounding the recovery;
- Immediately forward the initial recovery report to all offices originally notified;
- Prepare a follow-up report containing detailed information to all offices originally notified; and
- If the recovery was by an organization other than those authorities originally involved in investigation, obtain specific guidance regarding the handling of the items as evidence from IA/SMD.



CHAPTER 19: PROCEDURAL SECURITY

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

19.1. GENERAL

19.1.1. Purpose

- Physical security encompasses real and personal property including buildings, and the contents of a facility and its personnel. The provisions of this chapter apply to all CBP facilities that are CBP owned, as well as for GSA-leased space.

19.1.2. Scope

- All CBP employees are responsible for ensuring that Government property is safeguarded to the maximum extent feasible against damage, loss, or destruction. In addition, Designated Officials, senior CBP officials at a facility and Security Officers will institute security measures that they deem to be reasonable and prudent in protecting the welfare of CBP employees in the workplace. These security measures will be incorporated in Site Security Plans/Programs.

19.1.3. Objective

- The objectives are to implement security measures to minimize the loss, damage, or destruction of Government property to provide a safe and secure working environment for CBP employees.

19.1.4. Jurisdiction

- FPS is the primary law enforcement service for responding to incidents in Federal facilities under the charge and control of the GSA as an owned or leased facility. FPS offices are typically located in areas where there is a high concentration of Federal employees and is capable of providing timely responses to GSA owned or leased facilities in these areas. For immediate responses to GSA-owned or leased facilities in rural areas and/or areas with a small Federal presence, law enforcement officials from local jurisdictions should be contacted.

19.2. WORKPLACE SECURITY

19.2.1. All Government offices can be targets for unlawful entry, theft, kidnapping, bombing, forcible occupation or sabotage. Security Officials and/or Designated Officials will mitigate these threats through implementation of:

- Written site security plans/programs;
- Effective barriers, both physical and psychological;
- Employee training and awareness programs; and
- Annual program review and update.

19.2.2. Security Officials and/or Designated Officials are responsible to conduct a comprehensive crime prevention security assessments to determine:

- What is the target potential?
- What is the prevailing attitude toward security?
- How are security policies enforced?
- How current are existing emergency preparedness plans (OEP, fire, power

failure, disaster)?

- What resources are available locally and how rapid are response times for fire, police, and ambulance?
- What kind and how effective are the physical security systems and controls currently in place?
- Do the available security resources, procedures and policies meet the potential threat?

19.2.3. Effective site security plans/programs incorporate effective security information for employees use and action. Information covered can include but is not limited to:

- OEP (for further information, see [Chapter 15, Occupant Emergency Plan](#));
- Recall rosters;
- Emergency contact numbers:
 - Internal
 - Local
- Crisis communications;
- Key control; (see [Chapter 9, Locks and Keys](#));
- Facility access; (see [Chapter 11, Access to Facilities](#))
- Identifying & protecting high value/high theft property:
 - Cameras;
 - Personal audio devices;
 - Binoculars;
 - Power tools;
 - Televisions;
 - Video cassette recorders;
 - Laptop computers;
 - Government transportation requests; and
 - Postage stamps, etc.
- Checklists:
 - Bomb threats;
 - Telephone threats;
 - Fire;
 - Chemical spills;
 - Personnel injuries;
 - Theft;
 - Suicide;
 - Workplace violence;

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- o Suspicious mail/packages (see [Chapter 15, Occupant Emergency Plan](#));
- o Close of business practices:
 - Locking office doors;
 - Performing secure storage container checks;
 - Turning off electrical appliances;
 - Activating alarms; and
 - Checking for NSI left unsecured
- Emergency reporting procedures:
 - o Security incidents:
 - Break-ins:
 - The incident must be reported immediately to the proper authorities by the senior person-in-charge.
 - o Security violations; and
 - o Security incidents.

19.2.4. The Regional Security Officer will be notified of the circumstances pertaining to all Security incidents and the corrective action instituted to prevent a recurrence in accordance with the procedures outlined in [Chapter 6.11, Security Survey & Inspection Process](#), or a completed Security Assessment. CBP.Security@dhs.gov will be notified of all physical security incidents in which program security has been compromised in any division or office.

19.3. RANDOM SECURITY AWARENESS MEASURES (RSAMs)

19.3.1. The purpose of Random Security Awareness Measures (RSAM) is to identify a set of protective measures extracted from a higher threat condition than is the current posture of the facility and implement those measure(s) for a period of time.

- As an example: under a threat condition Yellow (Elevated Level), moderate posture, a protective measure identified under threat condition Red (severe risk of terrorist attacks, the maximum), such as performing detailed searches of all vehicles entering the facility, is implemented for all vehicles entering the facility from 1400 to 1800. This became effective on Monday, July 1, 1999.

19.3.2. The implementation of RSAMs has three purposes:

- They are used as a tool to test which measures have higher costs to a facility in terms of productivity. A RSAM program can help identify those measures that security personnel and the facility infrastructure are more capable of sustaining and those that will be unduly stressful on human and material resources;
- The RSAM program will provide security forces with training and simulation. By keeping the security force focused and alert, RSAM programs ensure constant preparation for any events; and
- RSAM programs change the security atmosphere surrounding a facility. Such

programs, when implemented in a truly random fashion, alter the external appearance or security “signature” of any facility.

19.3.3. Criteria for implementing a RSAM program are:

- RSAMs are implemented in a strictly random manner, never using a set time frame or day for a given measure;
- The on-duty security force must be capable of implementing the measure without the need for augmentation or special equipment;
- No set patterns or times will be implemented when scheduling security activities
 - Some RSAMs are only appropriate for implementation during certain time periods. For instance, a 100-percent search of hand-carried items should not be implemented during rush hours;
 - Vary K-9 activities, daily, weekly and never the same time frame.
- Flexibility must be maintained should an emergency arise where a RSAM cannot be implemented, or would cause a major disruption to agency operations;
- RSAMs should be tailored to ensure on duty security forces can accomplish them without augmentation, during day-to-day operations;
- Security forces are the key to implementing the RSAMs:
 - They must comprehend the need for the program and understand how effective application can confuse any surveillance activity and enhance security awareness at the facility;
 - Otherwise, the measures appear too casual and will not provide the effect intended.

19.3.4. Sample random security awareness measures:

- Search all hand-carried items including those carried by employees entering the agency for illegal explosives/ weapons;
- On a random basis, physically inspect hand carried items entering and/or exiting the facility, (e.g., every fifth person departing the facility would be inspected);
- Conduct random parking lot checks for suspicious or unauthorized vehicles;
- All personnel expecting a guest/visitor to the facility will comply with the facilities visitor procedures, this also includes deliveries, (see [Chapter 11, Access to Facilities](#));
 - Encourage community security awareness by reminding personnel to be suspicious and inquisitive about strangers particularly those carrying suitcases or other containers or unusual activities;
 - Be alert for unidentified vehicles on or in the vicinity of the facility and be alert for abandoned parcels/packages;
 - Implement 100-percent hands-on identification checks for all personnel entering the facility;
 - Randomly check facility exterior for suspicious packages and activities;

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- o Inspect all commercial deliveries; and
- o Examine all incoming mail/parcels for obvious signs of explosives or tampering.





CHAPTER 20: WORKPLACE VIOLENCE

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

20.1. GENERAL

- 20.1.1. Workplace violence is any physical assaults, threatening behavior or verbal abuse occurring in the work setting. These acts originating from any employee, employer or supervisor can cause a substantial risk of physical or emotional harm to individuals, or damage to government resources or capabilities.
- 20.1.2. One of the most common types of workplace violence is that among coworkers. Additionally, a high percentage of violent incidents are perpetrated by individuals from outside the workplace. This includes situations such as domestic violence, bomb threats, and violence by customers.
- 20.1.3. Studies indicate violent occurrences among coworkers rarely happen without some warning. Before actually becoming violent, there are patterns of behavior or other activities that may serve as warning signs of violence. The following are warning indicators of potential workplace violence:
- Intimidating, harassing, bullying, belligerent, or other inappropriate and aggressive behavior;
 - Bringing a weapon to the workplace (unless necessary for the job), making inappropriate references to guns, or making idle threats about using a weapon to harm someone;
 - Direct or veiled threats of harm;
 - Numerous conflicts with supervisors and other employees;
 - Statements showing fascination with incidents of workplace violence, statements indicating approval of the use of violence to resolve a problem, or statements indicating identification with perpetrators of workplace homicides;
 - Substance abuse;
 - Extreme changes in behaviors; and
 - Statements indicating desperation (over family, financial, and other personal problems) to the point of contemplating suicide.
- 20.1.4. Security Officers should be involved in all stages of the planning process during the development of an effective workplace violence prevention plan. Planning efforts should be coordinated with Employee Assistance Programs and personnel programs, as they can play a critical role in prevention, intervention or response to threatening situations.
- 20.1.5. This section will provide general ideas and considerations that can help those charged with workplace violence responsibilities to gain an understanding of some of the security issues such as jurisdiction. It is also intended to help those Federal offices that do not have in-house security or law enforcement to identify the appropriate organizations that can assist them.
- 20.1.6. For more information refer to DHS Memorandum - [Department of Homeland Security Workplace Violence Prevention Procedures](#) and Office of Personnel Management Publication – [Dealing with Workplace Violence - A Guide for Agency Planners](#).

[RETURN TO TOP](#)

20.2. SECURITY PLANNING

- Depending on the primary tenant, location of the office, and the type of incident or situation, jurisdiction may vary. The agency's own law enforcement organization, the Federal Protective Service (FPS), or Federal, State or local law enforcement, or a combination of these, may have jurisdiction. Gaps in law enforcement coverage can occur when issues of workplace violence arise. These gaps can be closed if the agency planning group (which would include any in-house security organization) works with the various law enforcement organizations in setting up workplace violence programs. The following are some suggestions for involving law enforcement in agency efforts to prevent workplace violence.

20.2.1. Jurisdiction

- The agency planning group should identify which Federal or local law enforcement agency or agencies have responsibility for its work-site. For example, the FPS is the primary law enforcement service for responding to incidents in Federal facilities under the charge and control of the GSA as an owned or leased facility. FPS offices are typically located in areas where there is a high concentration of Federal employees. This allows them to provide timely responses to GSA owned or leased facilities in these areas. For immediate responses to GSA owned or leased facilities in rural areas and/or areas with a small Federal presence, law enforcement officials from local jurisdictions should be contacted;
- Some facilities have in-house security and/or law enforcement organizations. Others have contracts with private security firms. It is not always clear who has jurisdiction, and who should be contacted when the need arises; and
- Sometimes meeting with the local police chief, county sheriff or state police is necessary to establish a plan or procedure regarding law enforcement response in the event of potential violence or hostile incidents. In remote locations, arrangements can be made for local police to handle certain situations until the appropriate Federal law enforcement officials arrive.

20.2.2. Liaison with Law Enforcement Agencies

- Successful response to potential workplace violence depends upon effective communications and preparedness with those law enforcement agencies responsible for their work site. The agency planning group and incident response teams should reach out to these law enforcement agencies to establish key contacts to ensure effective communication during any workplace violence. The agency should obtain the names and telephone numbers of law enforcement personnel to contact during emergencies. To ensure that those designated with coordinating and executing response to workplace violence are prepared, the agency should hold periodic meetings to engage and establish community network in promoting effective response.

20.3. SECURITY ASSISTANCE

20.3.1. During the planning phase, Security Officers can:

- Develop methods for threat assessment and processing;
- Identify types of situations they can address and when and how they should be notified of an incident;
- Indicate whether their officers have arrest authority;
- Identify their jurisdictional restrictions and alternative law enforcement agencies that may be able to provide assistance;
- Identify threat assessment professionals who can assist the agency in its efforts to protect threatened employees;
- Explain anti-stalking laws applicable in the agency's jurisdiction and how and when to obtain restraining orders;
- Suggest security measures to be taken for specific situations such as cases where Employee Assistance Program counselors or other mental health professionals warn the agency that an individual has made a threat against an agency employee;
- Arrange for supervisor/employee briefings or training on specific workplace violence issues such as:
 - Personal safety and security measures;
 - Types of incidents to report to law enforcement/security/authority;
 - Types of measures law enforcement/security may take to protect employees during a violent incident, e. g., Explanations of what it means to "secure the area," "secure the perimeter," and "preserve evidence";
 - Recommended steps on how to react to an armed attacker;
 - Suggestions for dealing with angry customers or clients;
 - Responses to suspicious packages;
 - Bomb threats;
 - Hostage situations; and
 - Telephone harassment and threats.

20.3.2. When potentially violent situations occur, Security Officers can work with the incident response team to:

- Provide an assessment of the information available to determine whether law enforcement intervention is immediately necessary; response can include a criminal investigation or consultation and threat assessment by a professional;
- Identify appropriate response for each type of incident; and
 - Determine who will gather what types of evidence.

20.4. PHYSICAL SECURITY MEASURES

20.4.1. General

- There are more than 1.2 million employees working in approximately 1,500 GSA owned buildings and 8,600 leased Federal buildings. GSA is the agency responsible for ensuring the safety and security of people while on Federal property that is owned or leased by GSA. This section contains recommendations and requirements for agencies in GSA controlled or leased space.

20.4.2. Regulations

- Federal Property Management Regulations 41 CFR §102-74 and Executive Order 12656 Part 18 specifically require GSA to provide standard protection services by coordinating a comprehensive Occupant Emergency Program (OEP), which is a short-term emergency response program establishing procedures for safeguarding lives and property during emergencies.
- For more information regarding the OEP refer to [Chapter 15, Occupant Emergency Plan](#).

20.4.3. GSA-Designated Official

- Each GSA owned or leased facility has a designated official who is the highest ranking official of the primary occupant agency of a Federal facility, or alternatively, a designee selected by mutual agreement of occupant agency officials. The designated official is responsible for developing, implementing, and maintaining an OEP, which consists of procedures developed to protect life and property in a specific Federally occupied space under stipulated emergency conditions. The designated official's responsibilities include establishing, staffing, and training an Occupant Emergency Organization, comprised of agency employees who have been designated to perform the requirements established by the OEP.
 - o According to the regulations, the GSA must assist in the establishment and maintenance of such plans and organizations. All agencies occupying a facility must fully cooperate with the designated official in the implementation of the emergency plans and the staffing of the emergency organization. GSA must provide emergency program policy guidance, review plans and organizations annually, assist in training of personnel, and to ensure proper administration of Occupant Emergency Programs. In leased space, GSA will solicit the assistance of the lessor in the establishment and implementation of plans.
- According to the regulations, decisions to activate the Occupant Emergency Organization shall be made by the designated official or by the designated alternate official. Decisions to activate shall be based upon the best available information including an understanding of local tensions, the sensitivity of target agencies, and previous experience with similar situations. Advice shall be solicited, when possible, from the GSA building manager, from the appropriate Federal Protective Service official, and from Federal, State, and local law enforcement agencies.

[RETURN TO TOP](#)

20.4.4. Physical Security Survey

- A major goal of the GSA's Federal Protective Service (FPS) is to provide better protection for Federal employees and visitors by identifying high-risk areas in Federal buildings where potential problems or emergency situations might occur. This is accomplished through a "Physical Security Survey" conducted by CBP/IA/SMD. The survey is a comprehensive, detailed, technical on-site inspection and analysis of the current security and physical protection conditions;
- If your agency does not have up-to-date security procedures in place, the head of your agency may want to ask a regional GSA FPS office or your agency's security office to conduct a physical security survey to ensure that employees are working in a safe and secure environment. There is a listing of FPS offices at the end of this section;
- The following are some examples provided by the FPS of ways to improve security in your office and/or building:
 - Post a security guard at the main building entrance or at entrances to specific offices;
 - Install a metal detector or CCTV (closed-circuit television), cameras or other device to monitor people coming in all building entrances;
 - Issue all employees photo identification cards and assign temporary passes to visitors who are required to sign in and out of the building. Under certain conditions, contract guards should be required to call Federal offices to confirm an appointment and/or to request an escort for all visitors;
 - Brief employees on steps to take if a threatening or violent incident occurs. Establish code words to alert coworkers and supervisors that immediate help is needed; and
 - Install silent, concealed alarms at reception desks.
- The following are some examples provided by the FPS of ways to improve security in "front-line" offices that serve the public:
 - Ensure that officers (or guards) have a clear view of the customer service area at all times;
 - Arrange office furniture and partitions so that front-line employees in daily contact with the public are surrounded by "natural" barriers (desks, counter tops, partitions) to separate employees from customers and visitors;
 - Provide an under-the-counter duress alarm system to signal a supervisor or security officer if a customer becomes threatening or violent;
 - Establish an area in the office for employees and/or customers to escape to if they are confronted with violent or threatening people;
 - Provide an access-control combination lock on access doors; and
 - Mount closed circuit television cameras for monitoring customer service activity from a central security office for the building.

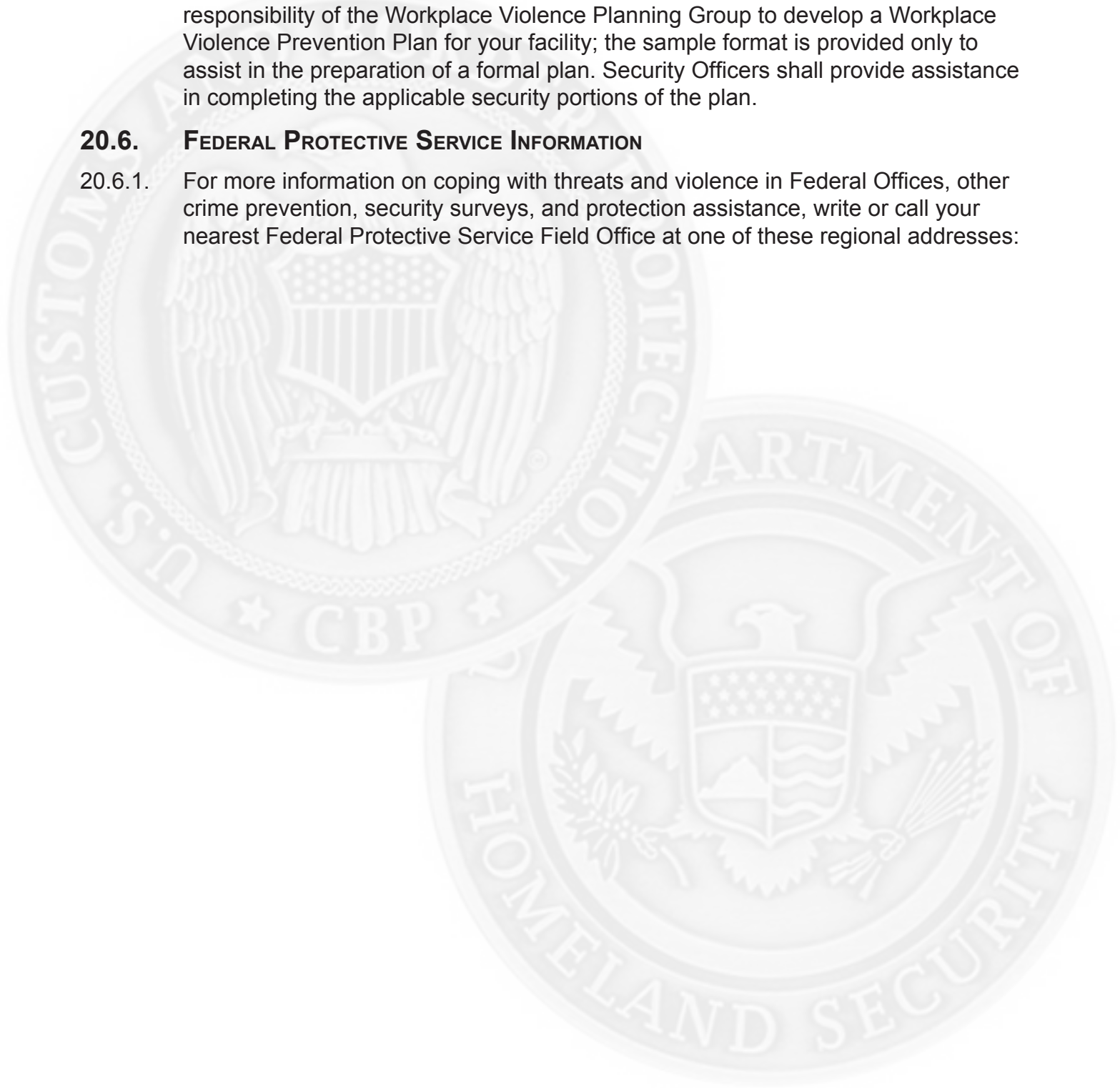
[RETURN TO TOP](#)

20.5. SAMPLE PLAN

20.5.1. Refer to [Appendix 20.5](#) to view a sample format of a Workplace Violence Prevention Plan. The document in this appendix is provided as a reference only. It is the responsibility of the Workplace Violence Planning Group to develop a Workplace Violence Prevention Plan for your facility; the sample format is provided only to assist in the preparation of a formal plan. Security Officers shall provide assistance in completing the applicable security portions of the plan.

20.6. FEDERAL PROTECTIVE SERVICE INFORMATION

20.6.1. For more information on coping with threats and violence in Federal Offices, other crime prevention, security surveys, and protection assistance, write or call your nearest Federal Protective Service Field Office at one of these regional addresses:



20.7. FPS CONTACT INFORMATION

Region 1-Boston, Massachusetts
10 Causeway Street
Room 935
Boston, MA 02222
Phone: 617-565-5772
Area of Responsibility: Massachusetts, Vermont,
New Hampshire, Maine, Rhode Island, and
Connecticut

Region 2-New York, NY
26 Federal Plaza
Room 17-130
New York, NY 10278
Phone: 212-264-4255
Area of Responsibility: New Jersey, New York,
Puerto Rico, and Virgin Islands

Region 3-Philadelphia, Pennsylvania
701 Market Street
Suite 4200
Philadelphia, PA 19106
Phone: 215-521-2161
Area of Responsibility: Delaware, Maryland,
Virginia, Pennsylvania, and West Virginia

Region 4-Atlanta, Georgia
Martin Luther King, Jr. Federal Building
Room 700
77 Forsyth St.
Atlanta, GA 30303
Phone: 404-331-3153
Area of Responsibility: Alabama, Florida, Georgia,
Kentucky, Mississippi, North Carolina, South
Carolina, and Tennessee

Region 5-Chicago, Illinois
Kluczynski Federal Building
Room 3540
230 South Dearborn Street
DPN: 35-5, mail room
Chicago, IL 60604
Phone: 312-353-1496
Area of Responsibility: Illinois, Indiana, Michigan,
Minnesota, Ohio, and Wisconsin

Region 6-Kansas City, Missouri
Federal Protective Service
601 E. 12th Street
Room 1712
Kansas City, MO 64106
Phone: 816-426-2155
Area of Responsibility: Iowa, Kansas, Missouri
and Nebraska

Region 7-Fort Worth, Texas
501 West Felix Building 3 (South End)
Ft. Worth, TX 76115
Phone: 817-900-5000
Area of Responsibility: Arkansas, Louisiana,
Texas, New Mexico, and Oklahoma

Region 8-Denver, Colorado
Denver Federal Center, Building 41
Room 258
West 6th Avenue & Kipling Street
Denver, CO 80225-0546
Phone: (303) 236-6707
Area of Responsibility: Colorado, Wyoming, South
Dakota, North Dakota, Montana, and Utah

Region 9-San Francisco, California
450 Golden Gate Avenue, 5th Floor
Room 5474
San Francisco, CA 94102
Phone: 415-522-3440
Area of Responsibility: California, Arizona,
Nevada, and Hawaii

Region 10-Federal Way, Washington
32125 32nd Avenue, South
Federal Way, WA 98001
Phone: (253) 815-4700
Area of Responsibility: Alaska, Washington, Idaho
and Oregon

National Capital Region (NCR-11)
1900 Half Street, SW
Suite 5000
Washington, DC 20536
Phone: 202-245-2300
Area of Responsibility: Washington DC, Virginia
and Maryland



CHAPTER 21: OFFICE AND LABORATORY EQUIPMENT

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

21.1. GENERAL

- 21.1.1. This Section is specifically prepared for Property Coordinators (PCs), Local Accountable Officers (LAOs), Local Property Coordinators (LPCs), Local Property Officers (LPOs), managers, and supervisors. However, it applies to all CBP personnel assigned property management duties and responsibilities.
- 21.1.2. This section provides information to establish appropriate physical security measures and property management guidelines to protect and account for office and laboratory equipment.
- 21.1.3. Equipment is defined as any property owned, leased, leased-to-own, borrowed, donated, forfeited, and retained for official use or otherwise in the possession of CBP:
- Office equipment includes office automation equipment, microcomputers, computer terminals, calculators, audiovisual equipment, telephone, facsimile machines, etc.;
 - Laboratory equipment includes the wide variety of scientific instruments used in CBP laboratories.
- 21.1.4. Local Accountable Officers (LAOs), Local Property Coordinators (LPCs), Local Property Officers (LPOs) and Property Coordinators (PCs) must determine the level of security needed, based on an assessment of threats to the equipment, to include a review of past incidents of theft and vandalism in the office/laboratory, building, and surrounding area.
- 21.1.5. For specific guidance on Property Management refer to [CBP Directive No. 5230-032](#), Personal Property Management; [CIS Manual 5200-13B](#), Personal Property Management Manual; and [DHS Management Directive No. 0565](#), Personal Property Management Directive.

21.2. THREAT DETERMINATION

- 21.2.1. Studies indicate that valuable and portable office and laboratory equipment are most commonly stolen or vandalized by semiskilled and unskilled burglars, employees or visitors. However, the security measures outlined in this chapter may also applied to mitigate illegal or unauthorized acts. For example, a lockable cabinet that protects a computer against theft also helps prevent unauthorized use of the equipment.
- 21.2.2. During security evaluations, the security officer or responsible custodial property officer should assess at the building and interior areas taking into consideration:
- What items are most likely to be stolen?
 - How could entry be gained?
 - Where could property be concealed for later removal?
 - Can exit with property be easily accomplished unchallenged?
 - Has the activity experienced equipment thefts during business and after business hours?
- 21.2.3. For specific guidance on Threat and Vulnerability Identification see [Chapter 14, Incident Response and the Homeland Security Advisory System](#) of this handbook.

[RETURN TO TOP](#)

21.3. SPECIAL SECURITY CONSIDERATIONS

21.3.1. In addition to the various protection measures discussed in this handbook, consideration should be given to provide additional protection to portable equipment. The security measures outlined below will mitigate the risk of tampering or removal of the equipment:

- Lock unoccupied offices and laboratories, especially after business hours;
- Lock small and valuable equipment in a cabinet or closet;
- Maintain tight control and accountability of keys, and keep keys in a secure place;
- Do not store unused equipment in isolated areas;
- Escort wandering or “lost” visitors to the right office;
- Establish a system to ensure that the last person to leave at night checks that all windows and doors are closed and locked;
- Ensure building package control procedures and property removal permits are strictly enforced;
- Establish entry control procedures or install access control equipment in high-risk environments commensurate with the sensitivity or value of the resources involved; and
- Install an Intrusion Detection System (IDS) that acts as a deterrent to intrusion and alerts security personnel of an actual intrusion. See [Chapter 8.9](#) for specific guidance.

21.4. KENNEL (K-9) FACILITIES

21.4.1. For information containing specific policies, procedures, responsibilities, and controls that govern the operations of the National Canine Enforcement Program (NCEP) refer to [CIS HB 3200-07A, Canine Enforcement Program Manual](#) and [Customs Directive No. 3290-015A, Canine Enforcement Program](#).

21.4.2. All explosive and chemical training materials (to include training materials used for certification/evaluation and field proficiency training) will be issued, handled, secured, stored, accounted for and returned or disposed of in accordance with established standard operating procedures as issued and approved by the NCEP.

21.5. CUSTOMS AND BORDER PROTECTION LABORATORY (CBPL)

21.5.1. The physical security of the CBPL shall be such that all seized property and controlled substances stored in their custody are protected from tampering and theft at all times.

- For physical security standards of laboratories refer to [CBP Directive No. 3290-010B, Physical Security Standard for Customs and Border Protection Laboratories](#).

21.5.2. The Laboratory and Scientific Services (OLSS) analyzes samples of seized or detained property. It also provides CBP Headquarters and Port Directors with

[RETURN TO TOP](#)

equipment standards for the procurement of scales, pill counters, and money counters.

- For guidance on the management of seized property, refer to the [Seized Asset Management and Enforcement Procedures Manual, CIS HB 4400-01A](#).





CHAPTER 22: MAINTENANCE

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

22.1. GENERAL

22.1.1. This directive establishes the U.S. Customs and Border Protection (CBP) policy and procedure for the maintenance of security systems, related subsystems, and components.

22.2. SCOPE

22.2.1. Security systems, related subsystems, and components shall be maintained in operable condition according to manufacturer specifications.

22.2.2. A regularly scheduled testing and maintenance program is required for optimal performance. Corrective and preventive maintenance should be balanced to provide a high degree of confidence that equipment degradation is identified and corrected, that equipment life is optimized, and that the maintenance program is cost effective.

22.2.3. System maintenance shall be applied in a graded fashion; consideration shall be given to:

- The interests/targets being protected;
- The identified threat; and
- Other protection measures afforded.

22.2.4. The physical protection program shall include a testing and maintenance program that encompasses security related components and subsystems.

22.3. CORRECTIVE MAINTENANCE

22.3.1. Corrective maintenance shall be initiated within 24 hours of the indication of malfunction of system elements determined to be critical for the protection of vital equipment, facilities and classified materials.

22.3.2. Compensatory measures shall be implemented immediately when any part of the critical system is out of service and shall be continued until maintenance is complete and the critical system is back in service.

22.3.3. Corrective maintenance of a non-critical system element protecting vital equipment, facilities and classified matter shall be initiated within 24 hours of detection.

22.3.4. The local authority responsible for safeguards and security shall determine corrective maintenance for a non-critical system protecting other assets. The local authority shall also determine if compensatory measures are necessary.

22.4. PREVENTIVE MAINTENANCE (PM)

22.4.1. Preventive maintenance is defined as a program in which wear, tear, and fatigue are anticipated, and continuous corrective actions are taken to ensure peak performance, efficiency, and minimize deterioration of equipment.

- PM involves a scheduled and controlled program of systematic inspection, adjustment, and replacement of components, as well as performance testing and analysis;

- The result of a successful PM program extends the life of the critical safeguards, security-related subsystems and components, and minimizes unscheduled downtime.

22.4.2. A preventive maintenance program should include:

- Non-destructive testing;
- Periodic inspection;
- Preplanned maintenance activities; and
- Maintenance to correct deficiencies found through testing or inspections.

22.4.3. The following system elements shall be included in a preventative maintenance program as prescribed by the manufacturer standards:

- Intrusion Detection Systems (see [Chapter 8.9, IDS](#));
- Primary Alarm Station/Secondary Alarm Station alarm annunciators;
- Protective force equipment;
- Personnel access control and inspection equipment;
- Package inspection equipment;
- Vehicle inspection equipment (see [Appendix 11.14, Screening Procedures](#));
- Security lighting (see [Chapter 7.5, Protective Lighting](#));
- Security system-related emergency power or auxiliary power supplies; and
- Any system, subsystem, or component not enumerated in this listing.

22.5. MAINTENANCE PERSONNEL ACCESS AUTHORIZATION

22.5.1. Personnel who test, maintain or service critical systems shall have access authorization consistent with the category of vital equipment, facilities and/or classified matter being protected. This level of authorization is not required when such testing and maintenance is performed as bench services away from the security area or is performed under the supervision of an appropriately cleared, knowledgeable custodian of the system and/or critical component.

22.5.2. Systems or critical components bench tested or maintained away from a security area by personnel without appropriate access authorization shall be inspected and operationally tested by qualified and cleared personnel prior to being put into service.

22.6. RECORD KEEPING

22.6.1. Records of testing and maintenance performed shall be retained by the custodian of the system or critical component for the effective life of the system or component.





APPENDIX 6.3: CBP MINIMUM STANDARDS

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

I. SITE PLANNING AND LANDSCAPE DESIGN

Vehicular Control				
Description	Levels of Protection			
	Min	Low	Medium	High
Distance			Minimum distance from a building to unscreened vehicles or parking is determined based on project-specific threat. Vehicle access control countermeasures include: <ul style="list-style-type: none"> • Perimeter barriers and street furniture; • Structural hardening and parking restrictions; • Relocation of vulnerable functions within or away from the building; and • Operational procedures, such as tighter access control. 	
Site Perimeter Barriers	NA	NA	Select a barrier that will stop the threat vehicle. Measures for the barrier system include: <ul style="list-style-type: none"> • Use various types and designs of buffers and barriers such as walls, fences, trenches, berms, ponds and water basins, plantings, trees, static barriers, sculpture, and street furniture; • Design site circulation to prevent high speed approaches by vehicles; • Offset vehicle entrances as necessary from the direction of a vehicle's approach to force a reduction in speed. • See Appendix 7.2. Barriers. 	
Perimeter Vehicle Inspection	NA	NA	If directed by the risk assessment, provide: <ul style="list-style-type: none"> • Space for inspection at a location to be specified that is separated from the building as much as practical (e.g., the curb line or outside the protected perimeter for gross amounts of explosives); • Design features for the vehicular inspection point that: <ul style="list-style-type: none"> o Stop vehicles, to stop 15,000 lbs vehicle at 30-50 MPH (K-4 thru K-12) at a minimum; o Prevent them from leaving the vehicular inspection area; and o Prevent tailgating. If screening space cannot be provided, other design features such as hardening, or other operational procedures such as finding alternative space for inspection, may be required.	
Site Lighting				
Description	Levels of Protection			
	Min	Low	Medium	High
Design Site Lighting to Perform the Required Functions.	NA		Effective site lighting levels include: <ul style="list-style-type: none"> • Vehicular and pedestrian entrances: (5 fc), horizontally maintained; • Perimeter, vehicular, and pedestrian circulation areas: (5 fc), horizontally maintained. In most circumstances, perimeter lighting should be: <ul style="list-style-type: none"> • Continuous/on both sides of the perimeter barriers with minimal hot and cold spots (1-2 fc); • Sufficient to support CCTV and other surveillance. However, for safety reasons and/or for issues related to camera technology, lower levels may be desirable. Other codes or standards may restrict site lighting levels. <ul style="list-style-type: none"> • Flag (20 fc); • Building perimeter (2 fc up to 10' high and 10' from the building); • Sally port – (20 fc); • Parking areas (1-2 fc); • Impound lots (5 fc); • Fuel island (20 fc); • Entry sign (20 fc); • Storage area (1-2 fc); • Site roadways (1-2 fc); • Vehicle maintenance parking (1-2 fc). Exterior lighting types should be assorted to prevent prolonged re-strike issues.	

Site Signage				
Description	Levels of Protection			
	Min	Low	Medium	High
Reduce Possible Confusion	NA	Reduce possible confusion over site circulation, parking, and entrance locations that can contribute to a loss of site security by: <ul style="list-style-type: none"> • Providing signage at entrances; • Having on-site directional signs, parking signs, and cautionary signs for visitors, employees, service vehicles, and pedestrians; and • Not posting signs that identify sensitive areas unless required by other standards,. 		
Landscaping				
Description	Levels of Protection			
	Min	Low	Medium	High
Landscaping Design Elements	NA	<ul style="list-style-type: none"> • Plants can deter unwanted entry; • Ponds and fountains can block vehicle access; • Site grading can limit access; and • Avoid landscaping that would permit concealment of criminals or obstruct the view of security personnel and CCTV. 		

II. ARCHITECTURE AND INTERIOR DESIGN

Planning				
Description	Levels of Protection			
	Min	Low	Medium	High
Location of Vulnerable Functions	NA	NA	Place offices of vulnerable officials so that occupants cannot be seen from an uncontrolled public area such as a street; whenever possible, these offices should face courtyards, internal sites or controlled areas. Alternative protective options for vulnerable functions include: <ul style="list-style-type: none"> • Locating and orienting the building away from possible vantage points; • Locating vulnerable functions further away from the exterior wall; • Blocking sight lines with barriers, berms, and trees; • Orienting windows and walls so they are oblique to the line of sight; • Minimizing the number of windows; and • Locating parking lots away from the building. If such forms of protection are not possible, provide suitable obscuring glazing or window treatment such as blast curtains, tinted glazing assemblies, film, or ballistic resistant glass. On design drawings and lists, number offices rather than referring to them by name, and provide a separate, protected key to room names.	
Mixed Occupancies	NA	If high-risk and low-risk offices are housed together, separate publicly accessible areas from high-risk offices and design additional solutions as required by the risk assessment.		
Public Toilets and Service Areas	If required by risk assessment, do not locate public toilets, service spaces, or access to vertical circulation systems in any non-secure areas, including the queuing area before screening at the public entrance.			
Refuge Provides Safe Area For Occupants If They Cannot Safely Exit the Building.	When deemed appropriate in high rise buildings, areas of refuge must be identified during the programming and design phases, with special consideration given to egress and related building support systems. Building's OEP must specifically cover the purpose and use of refuge areas during emergency.			

Planning				
Description	Levels of Protection			
	Min	Low	Medium	High
Loading Docks and Shipping and Receiving Areas.	If required by risk assessment, separate loading docks and receiving and shipping areas by at least 50 feet (15 m) in any direction from utility rooms, utility mains, and service entrances including electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc. Locate loading docks so that vehicles will not be driven into or parked under the building. If this is not possible, you must harden the surface for blast.			
Retail in the Lobby	While important to the public nature of buildings, the presence of retail and other mixed uses may present a risk to the building and its occupants and should be carefully considered on a project-specific basis during the risk assessment process. Retail and mixed uses may be accommodated, as required, through such means as separating entryways, controlling access, and hardening shared partitions, as well as through special security operational countermeasures.			
Stairwells	Stairwells required for emergency egress must be designed to meet applicable codes and must serve as an integral part of the OEP. Locate these stairwells as remotely as possible from areas where blast events might occur. Wherever possible, do not have stairs discharge into lobbies, parking or loading areas.			

Planning				
Description	Levels of Protection			
	Min	Low	Medium	High
Mail room	<ul style="list-style-type: none"> • Locate the mail room away from facility main entrances, areas containing critical services, utilities, distribution systems, and important assets; • Place it at the perimeter of the building with an outside wall or window designed for pressure relief; an area near the loading dock; • In some situations, an off-site location may be cost effective or several buildings may share one mail room; and • Provide adequate space for explosive disposal containers and equipment to examine incoming packages as directed by your risk assessment. 			

Exterior Entrances				
Description	Levels of Protection			
	Min	Low	Medium	High
Entrance Design	<ul style="list-style-type: none"> • The entrance design must balance security, operational, and aesthetic considerations. One strategy to reduce operational costs is to co-locate public and employee entrances, although this may make access control more difficult (see the risk assessment for project-specific directions). • Design entrances to avoid significant queuing. If queuing will occur within the building footprint, enclose the area in blast-resistant construction. If queuing is expected outside the building, provide a rain cover. • The following design measures can enhance protection at entrances: <ul style="list-style-type: none"> o Minimizing the number of doors; o Providing doors and skylights without transparent glazing; o Using bullet resistant door assemblies (see Army TM 5-853-3); and o If glazing in doors is required for other reasons, minimizing the size. • For wall types see criteria below (Lobby Doors and Partitions). 			
Forced Entry	For protection against limited hand tool attacks on the building, see swinging door, horizontal sliding door, wall criteria and window criteria. See Appendix 7.6, Doors .			
Equipment Space	NA	If required, provide space at public and employee entrances for immediate or possible future installation of access control and screening equipment, including walk-through metal detectors and x-ray devices, sensors, ID check, electronic access card, and turnstiles.		
	NA	NA	Space for equipment at public entrances and employee entrances (including space for possible installation of detection equipment currently under development). Note: Space to add equipment in times of heightened alert should also be provided for Low Protection.	
Entrance Co-location	Combine public and employee entrances if directed by your risk assessment.			

Exterior Entrances				
Description	Levels of Protection			
	Min	Low	Medium	High
Garage and Vehicle Service Entrances	If required by risk assessment, for all garage or service area entrances that are not otherwise protected by site perimeter barriers, provide devices capable of arresting a vehicle of the designated threat size at the designated speed. This criterion may be lowered if the access circumstances prohibit a vehicle from reaching this speed.			

Additional Features				
Description	Levels of Protection			
	Min	Low	Medium	High
Areas of Potential Concealment	If required by the risk assessment, reduce the potential for concealment of devices before screening points, avoid installing features that can be used to hide devices. If mail or express boxes or trash receptacles are used, restrict the size of the openings to prohibit insertion of packages.			
Roof Access	Design locking systems and other countermeasures to limit roof access to authorized personnel.			

Interior Construction				
Description	Levels of Protection			
	Min	Low	Medium	High
Lobby Doors and Partitions	Security procedures and Occupant Emergency Plans (OEPs) have a major impact on lobby design. Where screening and access control are performed, an adversary may bring a weapon into the pre-screening area. Consistent with project-specific risk assessment, make doors and walls along the line of security screening ballistic resistant per UL 752, "Standard for Safety: Bullet-Resisting Equipment" as follows:			
	N/A	UL Rating Level 3	UL Rating Level 8	
Critical Building Components	Increase the likelihood that emergency systems will remain operational during a disaster by locating critical building components away from main entrance, vehicle circulation, parking, or maintenance area or if such a location is not possible, critical components may need to be hardened. Examples of critical building components include: <ul style="list-style-type: none"> • Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; • Normal fuel storage; • Main switchgear and telephone distribution (LAN Room); • Fire pumps; • Building control centers and UPS systems controlling critical functions; • Elevator machinery and controls; • Shafts for stairs, elevators, and utilities; and • Critical distribution feeders for emergency power. 			

III. STRUCTURAL ENGINEERING

General Requirements				
Description	Levels of Protection			
	Min	Low	Medium	High
Designer Qualifications	For buildings designed to meet Medium or High Protection Levels, a blast engineer must be included as a member of the design team blast analysis are required in all new projects. He/she will have formal training in structural dynamics, and demonstrated experience with accepted design practices for blast resistant design and with referenced technical manuals.			
Design Narratives	A design narrative and copies of design calculations are required at each phase identifying the building-specific implementation requirements. Security requirements will be integrated into the overall building design starting with the concept and funding phases.			

General Requirements				
Description	Levels of Protection			
	Min	Low	Medium	High
Compliance	Full compliance with the risk assessment and this chapter is expected. Specific requirements should be in accordance with the findings of the facility risk assessment. Once the level of protection has been identified, the risk assessment should be conducted as early in the process as possible and in advance of project funding.			
New Techniques	Provided that the performance level is attained, alternative analysis and mitigation methods are permitted. New and untested techniques must be evaluated and approved by Headquarters CBP/IA/SMD.			
Methods and References	All building components requiring blast resistance must be designed using established methods and approaches for determining dynamic loads, structural detailing, and dynamic structural response.			
Structural and Non-Structural Elements	<p>To address blast, base the priority for upgrades on the relative importance of a structural or non-structural element, in the order below:</p> <ul style="list-style-type: none"> • Primary Structural Elements – the essential parts of the building’s resistance to catastrophic blast loads and progressive collapse, including columns, girders, roof beams, and the main lateral resistance system; • Secondary Structural Elements – all other load bearing members, such as floor beams, slabs, etc.; • Primary Non-Structural Elements – elements (including their attachments) that are essential for life safety systems, or elements that can cause substantial injury if failure occurs, including ceilings or heavy suspended mechanical units; and • Secondary Non-Structural Elements – all elements not covered in primary non-structural elements, such as partitions, furniture, and light fixtures. <p>Priority should be given to the critical elements that are essential to mitigating progressive collapse. Designs for secondary structural elements should minimize injury and damage. Consideration should also be given to reducing damage and injury from primary as well as secondary non-structural elements. Your risk assessment may specify protective measures for secondary, non-structural elements for Medium and High Protection.</p>			
Loads and Stresses	NA	NA	Structures must be designed to resist blast loads. The demands on the structure will be equal to the combined effects of dead, live, and blast loads. Blast loads or dynamic rebound may occur in directions opposed to typical gravity loads. For purposes of designing against progressive collapse, loads shall be defined as dead load plus a realistic estimate of actual live load. The value of the live load may be as low as 25% of the code-prescribed live load. The design should use ultimate strengths with dynamic enhancements based on strain rates. Allowable responses are generally post elastic. Data on materials properties and performance may be found in TM5-1300 and ASCE Design for Physical Security .	
Damage to the Structure and Exterior Wall Systems For Each Protection Level.	<p>Major damage:</p> <ul style="list-style-type: none"> • The facility or protected space will sustain a high level of damage without progressive collapse; • Casualties will occur and assets will be damaged; and • Building components, including structural members, will require replacement, or the building may be completely un-repairable, requiring demolition and replacement. 		<p>Moderate damage, repairable:</p> <ul style="list-style-type: none"> • The facility or protected space will sustain a significant degree of damage, but the structure should be reusable; • Some casualties may occur and assets may be damaged; and • Building elements other than major structural members may require replacement. 	<p>Minor damage, repairable:</p> <ul style="list-style-type: none"> • The facility or protected space may globally sustain minor damage with some local significant damage possible; and • Occupants may incur some injury, and assets may receive minor damage.

General Requirements				
Description	Levels of Protection			
	Min	Low	Medium	High
<p>Good Engineering Practice Guidelines – The following are rules of thumb commonly used to mitigate the effects of blast on structures. These guidelines are not meant to be complete, but are provided to assist the designer in the initial evaluation and selection of design approaches.</p>				
<ul style="list-style-type: none"> • For higher levels of protection from blast, cast-in-place reinforced concrete is normally the construction type of choice. Other types of construction such as properly designed and detailed steel structures are also allowed. Several material and construction types, while not disallowed by these criteria, may be undesirable and uneconomical for protection from blast. • To economically provide protection from blast, inelastic or post elastic design is standard. This allows the structure to absorb the energy of the explosion through plastic deformation while achieving the objective of saving lives. To design and analyze structures for blast loads, which are highly nonlinear both spatially and temporally, it is essential that proper dynamic analysis methods be used. Static analysis methods will generally result in unachievable or uneconomical designs; • Recognize that components might act in directions for which they are not designed. This is due to the engulfment of structural members by blast, the negative phase, the upward loading of elements, and dynamic rebound of members. Making steel reinforcement (positive and negative faces) symmetric in all floor slabs, roof slabs, walls, beams and girders will address this issue. Symmetric reinforcement also increases the ultimate load capacity of the members; • Lap splices should fully develop the capacity of the reinforcement; • Lap splices and other discontinuities should be staggered; • Ductile detailing should be used for connections, especially primary structural member connections; • There should be control of deflections around certain members, such as windows, to prevent premature failure. Additional reinforcement is generally required; • Balanced design of all building structural components is desired. For example, for window systems, the frame and anchorage must be designed to resist the full capacity of the weakest element of the system; • Special sheer reinforcement including ties and stirrups is generally required to allow large post-elastic behavior. You should carefully balance the selection of small but heavily reinforced (i.e., congested) sections with larger sections with lower levels of reinforcement; • Connections for steel construction should be ductile and develop as much moment connection as practical. Connections for cladding and exterior walls to steel frames shall develop the capacity of the wall system under blast loads; • In general, single point failures that can cascade, producing wide spread catastrophic collapse, are to be avoided. A prime example is the use of transfer beams and girders that, if lost, may cause progressive collapse and are therefore highly discouraged; • Redundancy and alternative load paths are generally good in mitigating blast loads. One method of accomplishing this is to use two-way reinforcement schemes where possible; • In general, column spacing should be minimized so that reasonably sized members can be designed to resist the design loads and increase the redundancy of the system. A practical upper level for column spacing is generally 9.1 m (30 ft.) for the levels of blast loads described herein; • In general, floor-to-floor heights should be minimized. Unless there is an overriding architectural requirement, a practical limit is generally less than or equal to 4.9 m (16 ft.); • It is recommended that you use fully grouted and reinforced CMU construction in cases where CMU is selected; • It is essential that you actively coordinate structural requirements for blast with other disciplines including architectural and mechanical; • The use of one-way wall elements spanning from floor-to-floor is generally a preferred method to minimize blast loads imparted to columns; and • In many cases, the ductile detailing requirements for seismic design and the alternate load paths provided by progressive collapse design assist in the protection from blast. You must bear in mind, however, that the design approaches are at times in conflict. These conflicts must be worked out on a case-by-case basis. 				
<p>Historic Buildings – Historic buildings are covered by these criteria in the same manner as other existing buildings.</p>				

IV. MECHANICAL ENGINEERING

Protection Against Airborne Contaminants – Protection against airborne chemical/ biological/radiological (CBR) contaminants can be achieved by using the devices listed below.				
Description	Levels of Protection			
	Min	Low	Medium	High
Particulate filters	<ul style="list-style-type: none"> Remove airborne solid or liquid substances including biological substances that exist in the form of aggregated molecules or particles; Radioactive particulates can also be removed; High efficiency particulate air (HEPA) filters are capable of removing a higher percentage and finer particles; and Particulate filters produce life cycle benefits that may exceed life cycle costs. 			
Adsorption filters	Remove certain gaseous chemicals from the air stream, primarily using activated carbon. Some are also capable of exchanging radioactive isotopes for stable ones.			
Biological or Radiological Contaminants	NA	Use MERV 13 filter or functional equivalent	Use HEPA filter or functional equivalent	Use HEPA filter or functional equivalent
	NA	NA	Design for future detection technology	
Chemical or Radiological Contaminants	Adopt NIOSH document recommendations			
	NA	None	Use gas absorber for outside air	Use gas absorber for outside air and return air
	NA	NA	Design for future detection technology	
Air System				
Description	Levels of Protection			
	Min	Low	Medium	High
Air Intakes	<ul style="list-style-type: none"> Raising air intakes makes the building ventilation system less accessible and therefore less vulnerable to threats that might introduce contaminants directly into the intakes; On buildings of more than 4 stories, locate intakes on the 4th floor or higher; On buildings of 3 stories or less, locate intakes on the roof or as high as practical; Locating intakes high on a wall is preferred over a roof location; When choosing secure locations for intakes in urban areas, take into consideration the vantage points offered to threats by nearby buildings and roofs; and Results of analyses using air plume models related to CBR clouds could affect the placement of intakes. If directed by your risk assessment, incorporate analysis results into your project's design. 			
Utility Protection – Protecting utility systems, locating them away from vulnerable areas, and restricting access helps assure that services will facilitate life safety and operations support after an event.				
Description	Levels of Protection			
	Min	Low	Medium	High
Utilities and Feeders	NA	NA	If required, locate utility systems at least 15 meters (50 feet) from loading docks, front entrances, and parking areas.	
Incoming Utilities	NA	NA	If required, within building and property lines, conceal incoming utility systems and give them blast protection, including burial or proper encasement, wherever possible.	
Water Supply	If directed by the risk assessment, consider using off-the-shelf countermeasures to enhance protection of the water supply that include: backflow preventers, central building water filtration and treatment systems, and point-of-use filters.			

Ventilation Systems – Pressurization is not necessary in buildings lower than 23 meters (75 feet) or six stories above or below grade, unless required by other criteria. For ventilation systems to function, electrical power must be available.				
Description	Levels of Protection			
	Min	Low	Medium	High
Smoke Removal Systems	<ul style="list-style-type: none"> • In the event of a blast or event-related fires, the ventilation system may be essential to smoke removal, particularly in large, open spaces; • Locate ventilation equipment away from high-risk areas such as loading docks and garages, and protect the system controls and power wiring to the equipment; • Connect the ventilation system to emergency power to provide the ability to selectively run one or several air-handling units for smoke removal; • Your facility’s multidisciplinary team should consider having separate HVAC systems in lobbies, loading docks, and other locations where the significant risk of internal event exists; • Provide smoke removal equipment with stand-alone local control panels that can continue to individually function in the event the control wiring is severed from the main control system; and • It may be appropriate to locate the panels with a fire alarm control panel. 			
Pressurized Stairways	NA	NA	<ul style="list-style-type: none"> • Stairway pressurization system should maintain positive pressure in stairways for occupant refuge, safe evacuation, and access by fire fighters; • The entry of smoke and hazardous gases into stairways must be minimized.. 	

V. ELECTRICAL ENGINEERING

Service and Distribution				
Description	Levels of Protection			
	Min	Low	Medium	High
Distributed Emergency Power	NA	<ul style="list-style-type: none"> • Emergency and normal electric panels, conduits, and switch gear should be installed separately, at different locations, and as far apart as possible; • Electric distribution should also run at separate locations; and • Emergency power is required for life safety, security systems, and critical components at a minimum, for all CBP facilities. 		
Normal Fuel Storage	These criteria increase the reliability of the building’s power distribution, fuel storage, generator, utilities, and feeders during an emergency. The focus is on separating power sources and locating electrical systems away from vulnerable areas.			
	NA	<ul style="list-style-type: none"> • The main fuel storage should be located away from loading docks, entrances, and parking. Access should be restricted and protected (e.g., locks on caps and seals). 		
Emergency Fuel Storage	NA	<ul style="list-style-type: none"> • The day tank should be mounted near the generator, given the same protection as the generator and sized to store approximately 120 hours of fuel; • A battery and/or UPS could serve a smaller building or leased facility. 		
Tertiary Power	A tertiary power source is intended for High Protection in buildings where operational continuity is critical. Conduit and line can be installed outside to allow a trailer-mounted generator to connect to the building’s electrical system; if this option is used, an operations plan must address this issue. Other tertiary power methods include generators and feeders from alternative substations.			
Emergency Generator	NA	<ul style="list-style-type: none"> • Locate the emergency generator away from loading docks, entrances, and parking. More secure locations include the roof, protected grade level, and protected interior areas; • If the emergency generator is installed outdoors at grade, it should be protected by perimeter walls and locked entrances. The generator should not be located in any areas that are prone to flooding; and • Provisions for refueling and shutoff valves in fuel lines within the building must be addressed. 		
Utilities and Feeders	NA	<ul style="list-style-type: none"> • Utility systems should be located away from loading docks, entrances, and parking. Underground service is preferred; • Alternatively, they can be hardened. 		

Power and Lighting				
Description	Levels of Protection			
	Min	Low	Medium	High
Site Lighting	Site lighting should be coordinated with the closed-circuit television (CCTV) system. Although CCTV cameras are available for low-light applications, operations are enhanced with higher uniform lighting levels. See Appendix 7.5, Protective Lighting , for further information.			
Restrooms	NA	NA	<ul style="list-style-type: none"> Emergency lighting in restrooms can facilitate evacuation and permit limited use during power outages when sheltering-in-place is required; Otherwise, emergency power for exit lights should be provided. 	
Stairways and Exit Signs	NA	NA	<ul style="list-style-type: none"> Self-contained battery lighting should be provided in stairwells and for exit signs as back up in case of emergency generator failure; As an alternative to battery powered lighting, handrails, stair treads, signs, and doors can be painted with phosphorescent paint; and Floor-level evacuation lighting systems should also be considered since a design event may fill corridors with dense smoke. 	

Communications and Security Systems				
Description	Levels of Protection			
	Min	Low	Medium	High
Redundant Communications	NA	NA	Base radio communication system with antenna should be installed, consistent with building codes, and portable sets distributed on floors. This is the preferred alternative.	
			NA	The facility could have a second telephone service to maintain communications in case of an incident.
Radio Telemetry	<ul style="list-style-type: none"> Wireless data transmission minimizes the risk of communications breakdowns due to wiring damage. Radio telemetry can be used for non-secure data that support the life safety system and other critical operations. 			
	NA	NA	NA	Distributed antennas could be located throughout the facility if required for emergency communication through wireless transmission of data.
Alarm and Information Systems	NA	NA	<ul style="list-style-type: none"> Alarm and information systems should not be collected and mounted in a single conduit, or even co-located. Having circuits follow different paths reduces the risk of total system failure during some events. Install circuits to various parts of the building in at least two directions and/or risers; Low voltage signal and control copper conductors should not share conduit with high voltage power conductors; and Fiber-optic conductors are generally preferred over copper. 	
Empty Conduits	NA	NA	<ul style="list-style-type: none"> Empty conduits and power outlets can be provided for possible future installation of security control equipment. This would eliminate the need for major retrofits and facilitate installing security equipment, including metal detectors, explosives detectors, sensors, and X-ray machines, as the need arises and technology advances; This criterion does not require installation of equipment. Some future technology may not require conduits 	
COMSEC	Refer to Attachment Q of DHS MD 4300B.			

VI. FIRE PROTECTION ENGINEERING

Fire Analysis				
Description	Levels of Protection			
	Min	Low	Medium	High
Fire Protection Engineering Analysis	Perform a fire protection engineering analysis whenever a blast analysis is required. In addition, a fire protection engineer should coordinate with the blast engineer on issues affecting life safety and building egress. Fire analysis is consistent with building codes and applies only to the design events of the Criteria.			
Active System - Protecting the water supply, dual fire pumps, and standpipe connection and/or locating them away from vulnerable areas helps ensure that services will provide life safety and operations support after an event.				
Description	Levels of Protection			
	Min	Low	Medium	High
Water Supply	The water system should be protected from single point failure. The incoming line should be encased, buried, or located 15 m (50 ft.) away from high threat areas. The exterior mains should be looped and sectionalized. When supported by the risk assessment, the interior standpipes should be cross-connected on each floor.			
Dual Fire Pumps: Electric and Diesel	To increase the reliability of the fire protection system for High Level Protection, a dual pump arrangement may be used, with one electric pump and one diesel pump. There should be a performance-based design to address the type and magnitude of failures the sprinkler/standpipe systems must withstand, along with the appropriate pump system in a building with multiple generators.			
Egress Door Locks	All security-locking arrangements on doors used for egress must comply with requirements of NFPA 101, Life Safety Code. See Appendix 7.6. Doors and Door Hardware .			
Operational System				
Description	Levels of Protection			
	Min	Low	Medium	High
Guard and Employee Training	<ul style="list-style-type: none"> • Create an OEP manual for use by security guards and employees that covers all locations in your facility; • Guards and employees should receive emergency training in the proper reporting and response to fires and other emergencies, and in the use of portable and built-in protection systems, including training in system maintenance. 			
Building Documents	Designate an area, preferably in the Operation Control Center, where the following building documents will be readily available: <ul style="list-style-type: none"> • Emergency instructions; • OEP manuals (see Chapter 15. Occupant Emergency Plan); and • Building plans for Medium and High Protection Levels. 			

VII. ELECTRONIC SECURITY

Control Centers and Building Management Systems				
Description	Levels of Protection			
	Min	Low	Medium	High
Operational Control Center (OCC) Fire Command Center (FCC) Security Control Center (SCC)	<ul style="list-style-type: none"> • Centralizing control center information through co-location can improve the reliability and effectiveness of life safety systems, security systems, and building functions; • If the control centers are co-located, you must specify operational requirements, especially a pre-designated chain of command to ensure that the most qualified leadership is in control for specific types of events; and • As an alternative to co-locating command centers for Minimum and Low Protection, provide secure information links between the SCC, OCC, and FCC. 			
Backup Control Center (BCC)	NA	NA	Provide a backup control workstation in a different location, such as a manager's or engineer's office. If feasible, consider an off-site location.	Install a fully redundant BCC.

Security for Utility Closets, Mechanical Rooms, and Telephone Closets - Control access to security system, emergency communication, and associated systems wiring and conduit, preferably by routing them through separate and secure closets.

Description	Levels of Protection			
	Min	Low	Medium	High
Key System	Use a key system with a method of recording times of entry and departure such as a watchman's clock system. For use with conventional keyed doors only.			
Monitored Access	NA	NA	Design for remote monitoring of access to mechanical, electrical, and telecommunication rooms. Access should be authorized, programmed, and monitored by the CCC through pre-identification of maintenance personnel. To design the doors, you may need details of the security system.	

Devices and Alarms

Description	Levels of Protection			
	Min	Low	Medium	High
Elevator Recall	<ul style="list-style-type: none"> Consistent with the facility OEP, provide a button on the Fire Control Center (FCC) to recall elevators to an alternative floor if the elevators could safely be used to evacuate disabled persons or if the normal evacuation route would involve traveling through a high risk area; Consider whether elevators should discharge personnel on the first floor (lobby) during some events. Consider the requirements of the Safety Code for Elevators and Escalators, ASME Standard A17.1. 			
Elevator Emergency Message	<ul style="list-style-type: none"> In conjunction with the recall system, install a pre-recorded message in the elevator cab speakers, notifying passengers of an emergency and explaining how to proceed; Provisions must be made for an override of recorded message with a live transmission with directions for the specific emergency. 			

Intrusion Protection System

Description	Levels of Protection			
	Min	Low	Medium	High
Door Locks	Special keying system not needed. Key lock when the facility is unoccupied	Security keying or card reader system.	High security keying or card reader system with provisions for a pin number. Key duplication should be made difficult and recorded. Electronic locking such as electromagnetic locks for fire exits, consistent with NFPA 101 requirements. A formal key control program shall be maintained. See Chapter 9, Keys and Locks .	
Intrusion Detection	Provide basic intrusion detection for entrances into the facility			
	Generally by means of balanced magnetic reed switches			
	NA	<ul style="list-style-type: none"> Basic intrusion detection for entrances into the facility; Interior door protection should be by means of balanced magnetic contact switch sets for locations at which magnet substitution is a vulnerability; Exterior door protection, especially at loading docks, should only be provided by balanced magnetic contact switch sets, to include all overhead/roll-up doors; Glass-break sensors shall be provided; and Requirements for roof intrusion detection should be reviewed. 		

Intrusion Protection System				
Description	Levels of Protection			
	Min	Low	Medium	High
Monitoring	Monitoring provided by a commercial central station. Under special circumstances, an on-site security central control center may be provided during normal business hours for low levels of protection.		Security systems monitored by an on-site, proprietary security control center. Commercial central stations may be used for after-hours or to supplement on-site monitoring.	Security systems monitored by an on-site, 24-hour proprietary security control center.
Closed Circuit TV (CCTV)	NA		<ul style="list-style-type: none"> Provide a color CCTV surveillance system with recording capability to view and record activity at the perimeter of the building; A mix of monochrome cameras should be considered for areas that lack adequate illumination for color cameras. Monitoring mainly at entrances, monitored exits, vehicular entrances into parking garages, and loading docks; The CCTV systems should be primarily for alarm assessment and access control automation purposes. The use of the CCTV system for general surveillance should be discouraged, with the occasional exception of automated video guard tours; All CCTV cameras should be on real-time and time-lapsed video recorders; and For deterrence as well as to aid post-incident investigations, key exterior areas (for Medium Protection) or most exterior areas (for High Protection), especially vehicle routes close to the facility, should be video recorded. The use of digital video systems should be considered by the designer. See Chapter 8.12, Closed Circuit Television Systems. 	
Duress Alarms or Assistance Stations	Provide call buttons at key public contact areas and as needed in the offices of managers and directors, in garages, and other areas that are identified as high risk locations by the project-specific risk assessment.			
	Alarms should report to the central station during normal business hours		<ul style="list-style-type: none"> Duress alarms should report to the security command center; Duress alarms are required for all guard posts and command centers. If CCTV coverage is available, automatic activation of corresponding cameras should be provided, as well as dedicated communications with security or law enforcement stations.	

VIII. PARKING SECURITY

Parking				
Description	Levels of Protection			
	Min	Low	Medium	High
Parking on Adjacent Streets	Parking is often permitted in curb lanes, with a sidewalk between the lane and the building. Where the distance from the building to the nearest curb provides insufficient setback, and compensating design measures do not sufficiently protect the building from the assessed threat, you must restrict parking as required by your risk assessment as follows:			
	Unrestricted parking	Government-owned and key employee parking only.		Use the lane for stand-off; use structural features to prevent parking. For typical city streets, this may require negotiating to close the curb lane.
Parking on Adjacent Properties	Adjacent public parking should be directed to more distant or better-protected areas, segregated from employee parking and away from the facility. One alternative to distance for blast is the acceptance of some higher degree of risk.			

Parking				
Description	Levels of Protection			
	Min	Low	Medium	High
Parking Inside the Building	Public parking with ID check	Parking for government vehicles and employees of the building only.	Parking for selected government employees only.	Parking only for selected government employees with a need for security.
On-Site Surface or Structured Parking	As directed by the risk assessment, adjacent surface parking must maintain a minimum stand-off of X meters. Parking within X meters of the building must be restricted to authorized vehicles.			
Parking Facilities				
Description	Levels of Protection			
	Min	Low	Medium	High
Natural Surveillance	<ul style="list-style-type: none"> • Maximize visibility across, as well as into and out of, the parking facility and openness to the exterior; • Use express or non-parking ramps that speeding the user to parking on flat surfaces; • Plan pedestrian paths to concentrate activity to the extent possible; • Limit vehicular entry/exits to a minimum number of locations; • Use long-span construction and high ceilings to enhance openness and aid in lighting the facility; • Avoid sheer walls, especially near turning bays and pedestrian travel paths. If they are required, improve visibility using large holes in sheer walls; • Eliminate dead-end parking areas, as well as nooks and crannies; • Landscaping should be done judiciously so as not to provide hiding places. It is desirable to hold planting away from the facility to permit observation of intruders; and • Locate attended booths, parking offices, or security stations so that activity at pedestrian and vehicle entry points to the facility can be monitored. 			
Perimeter Access Control	NA	NA	<ul style="list-style-type: none"> • Design a system of fencing, grilles, doors, etc., to completely close down access to the entire facility in unattended hours, or in some cases, all hours; • Any ground level pedestrian exits that open into non-secure areas should be emergency exits only and fitted with panic bar hardware for exiting movement only; • An intercom/car reader/keypad station at vehicle and pedestrian entrances (with optional installation at exit-only openings); and • Devices to allow for an audit trail of cards, electronic vehicle tags, or keypad codes that have been used to release electromechanical locks, activate roll-up service door motors, or otherwise permit entrance to a controlled parking area. • See Appendix 7.3, Fencing. 	

Parking Facilities				
Description	Levels of Protection			
	Min	Low	Medium	High
Stair Towers and Elevators	NA	NA	<ul style="list-style-type: none"> Stair tower and elevator lobby design must be as open as code permits. The ideal solution is a stair and/or elevator waiting area totally open to the exterior and/or the parking areas. Designs that ensure that people using these areas can be easily seen - and can see out - should be encouraged; If a stair must be enclosed for code or weather protection purposes, glass walls will deter both personal injury attacks and various types of vandalism; Potential hiding places below stairs should be closed off; nooks and crannies should be avoided; Elevator cabs should have glass backs whenever possible; Elevator lobbies should be well lit and visible to both patrons in the parking areas and the public out on the street; Where the means of egress must be protected, self-closing doors must be used; and Supporting systems (e.g., heat detectors or other sensors) should be considered. 	
Surface Finishes and Signage	NA	<ul style="list-style-type: none"> Paint interior walls a light color (i.e., white or light blue) to improve illumination; Signage should be clear to avoid confusion and direct users to their destinations efficiently; and If an escort service is available, signs should inform users. 		
Lighting	<ul style="list-style-type: none"> The lighting level standards recommended by the Illuminations Engineering Society of North America (IESNA) Subcommittee on Off-Roadway Facilities are the lowest acceptable lighting levels for any parking facility; A point-by-point analysis should be done in accordance with the IESNA standards. 			
Emergency Communications	NA	NA	<ul style="list-style-type: none"> Place emergency intercom/duress buttons or assistance stations on structure columns, fences, other posts, and/or freestanding pedestals and brightly mark them with stripping or paint visible in low light. These stations are to be used in conjunction with – and not as an alternative to – on-site monitoring; If CCTV coverage is available, automatic activation of corresponding cameras should be provided, as well as dedicated communications with security or law enforcement stations; It is helpful to include flashing lights that can rapidly pinpoint the location of the calling station for the response force, especially in very large parking structures; It should only be possible to re-set a station that has been activated at the station with a security key. It should not be possible to re-set the station from any monitoring site; and The horizontal distance on a floor to reach an emergency communication station shall not exceed 15 m (50 feet). 	
CCTV	NA	NA	<ul style="list-style-type: none"> Place color CCTV cameras with recording capability and pan-zoom-tilt drivers, if warranted, at entrance and exit vehicle ramps. Auto-scanning units are not recommended. The cameras should be oriented to record license plates of entering and departing vehicles, and to record pedestrians exiting or entering via vehicle ramps; Place fixed-mount, fixed-lens color or monochrome cameras on at least one side of regular use and emergency exit doors connecting to the building or leading outside. In order for these cameras to capture scenes of violations, time-delayed electronic locking should be provided at doors, if permitted by governing code authorities. Without features such as time-delayed unlocking or video motion detection, these cameras may be ineffective. 	

IX. DETERMINING BUILDING SECURITY LEVEL

- It has been determined by CBP/IA/SMD that all CBP facilities shall meet the Level III security requirements listed in the table below. A higher level of security may be assigned to a facility based on the risk assessment conducted.
- Determining the building security level in accordance with the ISC Standard, Facility Security Level Determinations for Federal Facilities, dated 21 Feb 2008, [ISC Security Design Criteria](#), defines the criteria and process to be used in determining the Facility Security Level (FSL) of a Federal facility. This categorization serves as the basis for implementing protective measures under other ISC standards. Consistent with the authority contained in [Executive Order 12977, “Interagency Security Committee,”](#) dated October 19, 1995, this Standard is applicable to all buildings and facilities in the United States occupied by Federal employees for non-military activities. These include existing buildings; new construction; major modernizations; facilities owned, to be purchased, or leased; stand-alone facilities, Federal campuses; and, where appropriate, special-use facilities.
- Federal holdings are divided into four out of the five security levels for this Physical Security Manual, based primarily on staffing size, number of employees, use, and the need for public access.

X. BUILDING SECURITY LEVELS

Factor	I	II	III	IV	Score
Mission Criticality	LOW	MEDIUM	HIGH	VERY HIGH	
Symbolism	LOW	MEDIUM	HIGH	VERY HIGH	
Facility Population	<100	101-250	251-750	>750	
Facility Size	<10,000 sq.ft.	10,000-100,000 sq. ft.	100,000-250,000 sq.ft.	>250,000sq.ft	
Threat to Tenant Agencies	LOW	MEDIUM	HIGH	VERY HIGH	
					Sum of above
Facility Security Level	I 5-7 Points	II 8-12 Points	III 13-17 Points	IV 18-20 Points	Preliminary FSL
Intangible Adjustment	Justification				+/- 1 FSL
					Final FSL

- Facility Security Level Determinations for Federal Facilities—An Interagency Security Committee Standard” (the Standard) defines the criteria and process to be used in determining the Facility Security Level (FSL) of a Federal facility.
- This categorization serves as the basis for implementing protective measures under other ISC standards. Consistent with the authority contained in Executive Order 12977, “Interagency Security Committee,” dated October 19, 1995, this Standard is applicable

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities. These include:

- o Existing buildings;
- o New construction, or major modernizations;
- o Facilities owned, to be purchased, or leased;
- o Stand-alone facilities;
- o Federal campuses;
- o Individual facilities on Federal campuses (where appropriate); and
- o Special-use facilities.

XI. SECURITY STANDARDS AND LAYERS OF SECURITY

- Security Standards. Security standards are discussed based on layers of security for a facility. These include:
 - o Perimeter Security. Perimeter security standards pertain to the areas outside government control. Depending on the facility type, the perimeter may include sidewalks, parking lots, outside walls of the building, a hallway, or simply an office door. The elements of perimeter security are: parking, closed circuit television monitoring, lighting, and physical barriers.
 - o Entry Security. Entry security standards refer to security issues related to the entry of persons and packages into a facility. The elements of entry security are: receiving/shipping, access control, and entrances/exits.
 - o Interior Security. Interior security standards refer to security issues associated with prevention of criminal or terrorist activity within the facility. This area concerns secondary levels of control after people or things have entered the facility. The elements of interior security are: employee/visitor identification, utilities, occupant emergency plans, and day care centers.
- Security Planning. Security planning standards refer to recommendations requiring long-term planning and commitment, as well as security standards addressing broader issues with implications beyond security at a particular facility. The elements of security planning are: intelligence sharing, training, tenant assignment, administrative procedures, and construction/renovation.
-

The following sections present security standards at each layer of security for the facility security levels.

- = Minimum standard ○ = Desirable ▲ = Standard based on facility evaluation
■ = Not applicable ● = CBP Minimum standard

XII. SECURITY STANDARDS BY LAYER OF SECURITY

Perimeter Security Standards		Facility Level		
Parking		III	IV	V
Control of Facility Parking	Access to government parking should be limited where possible to government vehicles and personnel. At a minimum, authorized parking spaces and vehicles should be assigned and identified.	●	●	●
Control of Adjacent Parking	Where feasible, parking areas adjacent to Federal space should also be controlled to reduce the potential for threats against Federal facilities and employee exposure to criminal activity.	▲	○	○
Avoid Leases Where Parking Cannot Be Controlled	Avoid leasing facilities where parking cannot be controlled. If necessary, relocate offices to facilities that do provide added security through regulated parking.	●	●	●
Leases Should Provide Security Control for Adjacent Parking	Endeavor to negotiate guard services as part of lease.	▲	▲	▲
Post Signs and Arrange for Towing Unauthorized Vehicles	Procedures should be established and implemented to alert the public to towing policies and the removal of unauthorized vehicles.	●	●	●
Identification System and Procedures for Authorized Parking	Procedures should be established for identifying vehicles and corresponding parking spaces (e.g., placard, decal, card key, etc.)	●	●	●
Adequate Lighting for Parking Areas	Effective lighting provides added safety for employees and deters illegal or threatening activities.	●	●	●
Closed Circuit Television (CCTV) Monitoring		III	IV	V
CCTV Surveillance Cameras with Time Lapse Video Recording	Twenty-four hour CCTV surveillance and recording is required at all locations as a deterrent. Requirements will depend on assessment of the security level for each facility. Time-lapse video recordings are also highly valuable as a source of evidence and investigative leads.	●	●	●
Post Signs Advising of 24-hr Video Surveillance	Warning signs advising of twenty-four hour surveillance act as a deterrent in protecting employees and facilities.	●	●	●
Lighting		III	IV	V
Lighting with Emergency Power Backup	Standard safety code requirement in virtually all areas. Provides for safe evacuation of buildings in case of natural disaster, power outage, or criminal/terrorist activity.	●	●	●
Physical Barriers		III	IV	V
Extend Physical Perimeter with Barriers	This security measure will only be possible in locations where the Government controls the property and where physical constraints are not present. Barriers should be made of concrete and/or steel.	●	○	○
Parking Barriers	Desirable to prevent unauthorized vehicle access.	▲	○	○

● = Minimum standard ○ = Desirable ▲ = Standard based on facility evaluation
 ■ = Not applicable ● (red) = CBP Minimum standard

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Entry Security Standards		Facility Level		
Receiving / Shipping (R/S)		III	IV	V
Review Current R/S Procedures	Audit current standards for package entry and suggest ways to enhance security.	●	●	●
Implement Modified R/S Procedures	After auditing procedures for R/S, implement improved procedures for security enhancements.	●	●	●
Access Control		III	IV	V
Evaluate Facility for Security Guard Requirements	If security guards are required, the number of guards at any given time will depend on the size of the facility, the hours of operation, and current risk factors, etc.	●	●	●
Security Guard Patrol		○	○	○
Intrusion Detection System with Central Monitoring Capability	See Appendix 8.9. Intrusion Detection Systems .	●	●	●
Upgrade to Current Life Safety Standards	Life safety standards include: fire detection and fire suppression systems.	●	●	●
Entrances/Exits		III	IV	V
X-Ray and Magnetometer at Public Entrances	Level III and IV evaluations would focus on tenant agencies, public interface, and feasibility.	○	○	●
Require X-Ray Screening of All Mail/Packages	All packages entering building should be subject to x-ray screening and/or visual inspection.	○	●	●
Peep Holes	Easy and effective visual recognition system for small offices.	○	■	■
Intercom	Communication tool that can be used in combination with peephole.	○	■	■
Entry Control with CCTV and Door Strikes	Allows employees to view and communicate remotely with visitors before allowing access. Not applicable for larger Levels III and above because of entry screening devices required at these Levels.	○	■	■
High Security Locks	Any exterior entrance should have a high-security lock as determined by GSA specifications and/or agency requirements.	●	●	●

● = Minimum standard ○ = Desirable ▲ = Standard based on facility evaluation
 ■ = Not applicable ● (red) = CBP Minimum standard

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

Interior Security Standards		Facility Level		
Employee/Visitor Identification		III	IV	V
Agency Photo Identification	Displayed at all times by all personnel.	●	●	●
Visitor Control/Screening System	Visitors should be readily apparent in Level III facilities. Other facilities may ask visitors to sign-in with a receptionist or guard, or require an escort, or formal identification badge.	●	●	●
Visitor Identification Accountability System	Stringent methods of control over visitor badges will ensure that visitors wearing badges have been screened and are authorized to be at the facility during the appropriate time frame.	●	●	●
Established Issuing Authority	Develop procedures and establish authority for issuing employee and visitor identification.	●	●	●
Utilities		III	IV	V
Prevent Unauthorized Access to Utility Areas	Smaller facilities may not have control over utility access, or locations of utility areas. Where possible, assure that utility areas are secure and that only authorized personnel can gain entry.	●	●	●
Provide Emergency Power to Critical Systems	CBP requires that all alarm systems, CCTV monitoring devices, fire protection systems, and entry control devices, etc., are required to be connected to emergency power sources. The tenant is responsible for determining which computer or communication systems require backup power.	●	●	●
Occupant Emergency Plans (OEPs)		III	IV	V
Examine OEP and Contingency Procedures Based on Threats	Review and update current OEP procedures for thoroughness. OEPs should reflect the current security climate.	●	●	●
OEPs in Place, Updated Annually, Periodic Testing Exercise	See Chapter 15, Occupant Emergency Plans .	●	●	●
Assign and Train OEP Officials	Assignment based on GSA requirement that largest tenant in facility maintain OEP responsibility. Officials should be assigned, trained and a contingency plan established to provide for the possible absence of OEP officials in the event of emergency activation of the OEP.	●	●	●
Annual Occupants Training	All occupants should be aware of their individual responsibilities in an emergency situation.	●	●	●
Day Care Centers		III	IV	V
Evaluate Whether to Locate Day Care Facility in Buildings with High Threat Activities	Conduct a thorough review of security and safety standards.	●	●	●
Compare Feasibility of Locating Day Care in Facilities Outside Locations	If a facility is being considered for a day care center, an evaluation should be made based on the risk factors associated with tenants and the location of the facility.	●	●	●

● = Minimum standard ○ = Desirable ▲ = Standard based on facility evaluation
 ■ = Not applicable ● (red) = CBP Minimum standard

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Security Planning		Facility Level		
Intelligence Sharing		III	IV	V
Establish Law Enforcement Agency/ Security Liaisons	Intelligence sharing between law enforcement agencies and security organizations should be established in order to facilitate the accurate flow of timely and relevant information between appropriate government agencies. Agencies involved in providing security must be part of the complete intelligence process.	●	●	●
Procedures for Intelligence Receipt & Dissemination	Determine what procedures exist to ensure timely delivery of critical intelligence. Review and improve procedures to alert agencies and specific targets of criminal/terrorist threats. Establish standard administrative procedures for response to incoming alerts. Review flow of information for effectiveness and time critical dissemination.	●	●	●
Uniform Security & Threat Nomenclature	To facilitate communication, standardized terminology for Alert Levels should be implemented (e.g., Normal, Low, Moderate, and High) See Chapter 14, Incident Response/HSAS .	●	●	●
Training		III	IV	V
Annual Security Awareness Training	Provide security awareness training for all tenants. At a minimum, self-study programs utilizing videos, and literature, etc., should be implemented. These materials should provide up-to-date information covering security practices, employee security awareness, and personal safety, etc.	●	●	●
Armed/Unarmed Guard Qualifications and Training Requirements	Liaison with the Federal Protective Service to ensure the standardized unarmed/armed guard qualifications and training requirements are being met. No CBP entity has contracting authority for guard service within DHS except FPS.	●	●	●
Tenant Assignment		III	IV	V
Co-locate Agencies with Similar Security Needs	To capitalize on efficiencies and economies, agencies with like security requirements should be located in the same facility if possible.	▲	▲	▲
Do Not Co-locate High/Low Risk Agencies	Low risk agencies should not take on additional risk by being located with high-risk agencies.	▲	▲	▲
Administrative Procedures		III	IV	V
Flexible Work Schedules	Establish flexible work schedule in high threat/high risk area to minimize employee vulnerability to criminal activity. Flexible work schedules can enhance employee safety by staggering reporting and departure times.	▲	●	●
Arrange for Employee Parking in or Near Building after Normal Work Hours	Minimize exposure to criminal activity by allowing employees to park at or inside the building after normal work hours.	○	○	○
Background Security Checks and Security Control Procedures	Conduct background security checks and/or establish security control procedures for service contract personnel.	●	●	●
Construction/Renovation		III	IV	V
Install shatter resistant material On All Exterior Windows (Shatter Protection)	Application of shatter resistant material to protect personnel and citizens from the hazards of flying glass as a result of impact or explosion. See Appendix 7.7, Windows .	●	●	●
Review Current Projects for Blast Standards	Designs and construction projects should be reviewed, to incorporate current technology and blast standards. Immediate review of ongoing projects may generate savings in the implementation of upgrading to higher blast standards prior to completion of construction.	●	●	●

Security Planning		Facility Level		
Review/Establish Uniform Construction Standards	Review, establish, and implement uniform construction standards as it relates to security consideration.	●	●	●
Review/Establish Uniform New Design Standards for Blast Resistance	In smaller facilities or those that lease space, control over design standards may not be possible. However, future site selections should attempt to locate in facilities that do meet standards. New construction of government-controlled facilities should review, establish, and implement new design standards for blast resistance.	●	●	●
Establish Street Set-Back for New Construction	Every foot between a potential bomb and a building will dramatically reduce damage and increase the survival rate. Street set-back is always desirable, but should be used in conjunction with barriers in Level IV and V facilities.	●	●	●

● = Minimum standard ○ = Desirable ▲ = Standard based on facility evaluation
 ■ = Not applicable ● = CBP Minimum standard

XIII. SECURITY STANDARDS BY FACILITY SECURITY LEVEL

LEVEL III Facility Perimeter Security Standards		Applicability			
		●	○	▲	■
Parking					
Control of Facility Parking	Access to government parking should be limited where possible to government vehicles and personnel. At a minimum, authorized parking spaces and vehicles should be assigned and identified.	●			
Post Signs and Arrange for Towing Unauthorized Vehicles	Procedures should be established and implemented to alert the public to towing policies and the removal of unauthorized vehicles.	●			
Identification System and Procedures for Authorized Parking	Procedures should be established for identifying vehicles and corresponding parking spaces (e.g., placard, decal, card key, etc.).	●			
Adequate Lighting for Parking Areas	Effective lighting provides added safety for employees and deters illegal or threatening activities.	●			
Control of Adjacent Parking	Where feasible, parking areas adjacent to Federal space should also be controlled to reduce the potential for threats against Federal facilities and employee exposure to criminal activity.			▲	
Avoid Leases Where Parking Cannot Be Controlled	Avoid leasing facilities where parking cannot be controlled. If necessary, relocate offices to facilities that do provide added security through regulated parking.	●			
Leases Should Provide Security Control for Adjacent Parking	Negotiate guard services through FPS as part of lease.			▲	
Closed Circuit Television (CCTV) Monitoring					
CCTV Surveillance Cameras with Time Lapse Video Recording	Twenty-four hour CCTV surveillance and recording is desirable at the entrance and egress all locations as a deterrent. Requirements will depend on assessment for each facility. Time-lapse video recordings are also highly valuable as a source of evidence and investigative leads. See Appendix 8.12, CCTV .	●			
Post Signs Advising of 24-hr Video Surveillance	Warning signs advising of twenty-four hour surveillance act as a deterrent in protecting employees and facilities.	●			

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

LEVEL III Facility Perimeter Security Standards		Applicability			
		●	○	▲	■
Lighting					
Lighting with Emergency Power Backup	Standard safety code requirement in virtually all areas. Provides for safe evacuation of buildings in case of natural disaster, power outage or criminal/terrorist activity.	●			
Physical Barriers					
Extend Physical Perimeter with Barriers	This security measure will only be possible in locations where the Government controls the property and where physical constraints are not present. Barriers should be made of concrete and/or steel. See Appendix 7.2, Barriers .			▲	
Parking Barriers	Desirable to prevent unauthorized vehicle access.			▲	


















● = Minimum standard ○ = Desirable ▲ = Standard based on facility evaluation
 ■ = Not applicable ● = CBP Minimum standard

LEVEL III FACILITY: Entry Security Standards		Applicability			
		●	○	▲	■
Receiving / Shipping					
Review Receiving & Shipping Procedures	Audit current standards for package entry and suggest ways to enhance security.	●			
Implement Receiving & Shipping Procedures	After auditing procedures for receiving & shipping, implement improved procedures for security enhancements.	●			
Access Control					
Evaluate Facility for Security Guard Requirements	If security guards are required, the number of guards at any given time will depend on the size of the facility, the hours of operation, and current risk factors, etc.	●			
Intrusion Detection System with Central Monitoring Capability	See Appendix 8.9, Intrusion Detection Systems	●			
Upgrade to Current Life Safety Standards	Life safety standards include: fire detection and fire suppression systems.	●			
Security Guard Patrol			○		
Entrances/Exits					
High Security Locks	Any exterior entrance should have a high security lock as determined by GSA specifications and/or agency requirements.	●			
X-Ray and Magnetometer at Public Entrances	Level III and IV evaluations will focus on tenant agencies, public interface, and feasibility.		○		
Require X-Ray Screening of All Mail/Packages	All packages entering building should be subject to X-ray screening and/or visual inspection.		○		
Peep Holes	Easy and effective visual recognition system for small offices.		○		
Intercom	Communication tool that can be used in combination with peephole.		○		
Entry Control with CCTV and Door Strikes	Allows employees to view and communicate remotely with visitors before allowing access. Not applicable for larger Levels III and above because of entry screening devices required at these Levels (e.g., "Airphone").		○		

● = Minimum standard ○ = Desirable ▲ = Standard based on facility evaluation
 ■ = Not applicable ● = CBP Minimum standard

LEVEL III FACILITY: Interior Security Standards		Applicability			
		●	○	▲	■
Employee/Visitor Identification					
Visitor Control/Screening System	Visitors should be readily apparent in smaller Level III facilities. Other facilities will make visitors sign-in with a receptionist or guard, or require an escort, and formal identification badge.	●			
Agency Photo Identification	Displayed at all times by all personnel. May not be required in smaller facilities.	●			
Visitor Identification Accountability System	Stringent methods of control over visitor badges will ensure that visitors wearing badges have been screened and are authorized to be at the facility during the appropriate time frame.		○		
Established Issuing Authority	Develop procedures and establish authority for issuing employee and visitor identification.		○		
Utilities					
Prevent Unauthorized Access to Utility Areas	Smaller facilities may not have control over utility access, or locations of utility areas. Where possible, assure that utility areas are secure and that only authorized personnel can gain entry.	●			
Provide Emergency Power to Critical Systems	CBP requires that all alarm systems, CCTV monitoring devices, fire protection systems, and entry control devices, etc., are to be connected to emergency power sources. The tenant is responsible for determining which computer or communication systems require backup power.	●			
Occupant Emergency Plans (OEPs)					
Examine OEP and Contingency Procedures Based on Threats	Review and update current OEP procedures for thoroughness. OEPs should reflect the current security climate.	●			
Oeps In Place, Updated Annually, Periodic Testing Exercise		●			
Assign and Train OEP Officials	Assignment based on GSA/FPS requirements that the largest tenant in facility maintain OEP responsibility. Officials should be assigned, trained and a contingency plan established to provide for the possible absence of OEP officials in the event of emergency activation of the OEP. See Chapter 15. Occupant Emergency Plans	●			
Annual Occupant Training	All occupants should be aware of their individual responsibilities in an emergency situation.	●			
Day Care Centers					
Evaluate Whether to Locate Day Care Facility in Buildings with High Threat Activities	Conduct a thorough review of security and safety standards.				■
Compare Feasibility of Locating Day Care in Facilities Outside Locations	If a facility is being considered for a day care center, an evaluation should be made based on the risk factors associated with tenants and the location of the facility.	●			

● = Minimum standard ○ = Desirable ▲ = Standard based on facility evaluation
 ■ = Not applicable ● = CBP Minimum standard

LEVEL III FACILITY: Security Planning		Applicability			
					
Intelligence Sharing					
Establish Law Enforcement Agency/ Security Liaisons	Intelligence sharing between law enforcement agencies and security organizations should be established in order to facilitate the accurate flow of timely and relevant information among appropriate government agencies. Agencies involved in providing security must be part of the complete intelligence process.				
Procedures for Intelligence Receipt & Dissemination	Determine what procedures exist to ensure timely delivery of critical intelligence. Review and improve procedures to alert agencies and specific targets of criminal/terrorist threats. Establish standard administrative procedures for response to incoming alerts. Review flow of information for effectiveness and time critical dissemination.				
Uniform Security & Threat Nomenclature	To facilitate communication, standardized terminology for Alert Levels should be implemented (e.g., Normal, Low, Moderate, and High - as recommended by Security Standards Committee).				
Training					
Annual Security Awareness Training	Provide security awareness training for all tenants. At a minimum, self-study programs utilizing videos, and literature, etc., should be implemented. These materials should provide up-to-date information covering security practices, employee security awareness, and personal safety, etc.				
Unarmed Guard Qualifications and Training Requirements	Liaison with the Federal Protective Service to ensure the standardized unarmed guard qualifications and training requirements are being met. No CBP entity has contracting authority for guard service within DHS except FPS.				
Armed Guard Qualifications and Training Requirements	Liaison with the Federal Protective Service to ensure the standardized unarmed guard qualifications and training requirements are being met. No CBP entity has contracting authority for guard service within DHS except FPS.				
Tenant Assignment					
Co-locate Agencies with Similar Security Needs	To capitalize on efficiencies and economies, agencies with similar security requirements should be located in the same facility if possible.				
Do Not Co-locate High/Low Risk Agencies	Low risk agencies should not take on additional risk by being located with high-risk agencies.				
Administrative Procedures					
Flexible Work Schedules	Establish flexible work schedule in high threat/high risk area to minimize employee vulnerability to criminal activity. Flexible work schedules can enhance employee safety by staggering reporting and departure times.				
Background Security Checks and Security Control Procedures	Conduct background security checks and/or establish security control procedures for service contract personnel.				
Arrange for Employee Parking in or Near Building after Normal Work Hours	Minimize exposure to criminal activity by allowing employees to park at or inside the building after normal work hours.				
Construction/Renovation					
Review Current Projects for Blast Standards	Designs and construction projects should be reviewed to incorporate current technology and blast standards. Immediate review of ongoing projects may generate savings in the implementation of upgrading to higher blast standards prior to completion of construction.				
Review/Establish Uniform Construction Standards	Review, establish, and implement uniform construction standards as it relates to security consideration.				

LEVEL III FACILITY: Security Planning		Applicability			
		●	○	▲	■
Review/Establish Uniform New Design Standards for Blast Resistance	In smaller facilities or those that lease space, control over design standards may not be possible. However, future site selections should attempt to locate in facilities that do meet standards. New construction of government-controlled facilities should review, establish, and implement new design standards for blast resistance.	●			
Install Shatter resistant materials on All Exterior Windows (Shatter Protection)	Application of shatter resistant material to protect personnel and citizens from the hazards of flying glass as a result of impact or explosion. See Appendix 7.7, Windows .		○		
Establish Street Set-Back for New Construction	Every foot between a potential bomb and a building will dramatically reduce damage and increase the survival rate. Street set-back is always desirable, but should be used in conjunction with barriers in Level IV and V facilities.		○		

● = Minimum standard ○ = Desirable ▲ = Standard based on facility evaluation
 ■ = Not applicable ● = CBP Minimum standard

LEVEL IV FACILITY: Perimeter Security Standards		Applicability			
		●	○	▲	■
Parking					
Control of Facility Parking	Access to government parking should be limited where possible to government vehicles and personnel. At a minimum, authorized parking spaces and vehicles should be assigned and identified.	●			
Post Signs and Arrange for Towing Unauthorized Vehicles	Procedures should be established and implemented to alert the public to towing policies and the removal of unauthorized vehicles.	●			
Identification System and Procedures for Authorized Parking	Procedures should be established for identifying vehicles and corresponding parking spaces (e.g., placard, decal, card key, etc.)	●			
Adequate Lighting for Parking Areas	Effective lighting provides added safety for employees and deters illegal or threatening activities. See Appendix 7.5, Lighting .	●			
Control of Adjacent Parking	Where feasible, parking areas adjacent to Federal space should also be controlled to reduce the potential for threats against Federal facilities and employee exposure to criminal activity.		○		
Avoid Leases Where Parking Cannot Be Controlled	Avoid leasing facilities where parking cannot be controlled. If necessary, relocate offices to facilities that do provide added security through regulated parking.	●			
Leases Should Provide Security Control for Adjacent Parking	Endeavor to negotiate guard services as part of lease through FPS.	●			
Closed Circuit Television (CCTV) Monitoring					
CCTV Surveillance Cameras with Time Lapse Video Recording	Twenty-four-hour CCTV surveillance and recording is desirable at all locations as a deterrent. Requirements will depend on assessment of the security level for each facility. Time-lapse video recordings are also highly valuable as a source of evidence and investigative leads.	●			
Post Signs Advising of 24-hr Video Surveillance	Warning signs advising of twenty-four hour surveillance act as a deterrent in protecting employees and facilities.	●			

LEVEL IV FACILITY: Perimeter Security Standards		Applicability			
		●	○	▲	■
Lighting					
Lighting with Emergency Power Backup	Standard safety code requirement in virtually all areas. Provides for safe evacuation of buildings in case of natural disaster, power outage, or criminal/terrorist activity.	●			
Physical Barriers					
Extend Physical Perimeter with Barriers	This security measure will only be possible in locations where the government controls the property and where physical constraints are not present. Barriers should be made of concrete and/or steel.		○		
Parking Barriers	Desirable to prevent unauthorized vehicle access.		○		

● = Minimum standard ○ = Desirable ▲ = Standard based on facility evaluation
 ■ = Not applicable ● = CBP Minimum standard

LEVEL IV FACILITY: Entry Security Standards		Applicability			
		●	○	▲	■
Receiving / Shipping (R/S)					
Review Current R/S Procedures	Audit current standards for package entry and suggest ways to enhance security.	●			
Implement Modified R/S Procedures	After auditing procedures for R/S, implement improved procedures for security enhancements.	●			
Access Control					
Evaluate Facility for Security Guard Requirements	If security guards are required, the number of guards at any given time will depend on the size of the facility, the hours of operation, and current risk factors, etc.	●			
Intrusion Detection System with Central Monitoring Capability	See Appendix 8.9. Intrusion Detection Systems.	●			
Upgrade to Current Life Safety Standards	Life safety standards include: fire detection and fire suppression systems.	●			
Security Guard Patrol			○		
Entrances/Exits					
Require X-Ray Screening of All Mail/Packages	All packages entering building should be subject to x-ray screening and/or visual inspection.	●			
High Security Locks	Any exterior entrance should have a high security lock as determined by GSA specifications and/or agency requirements.	●			
X-Ray and Magnetometer at Public Entrances	May be impractical for smaller Level III facilities, whereas, Larger Level III and IV evaluations would focus on tenant agencies, public interface, and feasibility. Link to X-ray		○		
Peep Holes	Easy and effective visual recognition system for small offices.				■
Intercom	Communication tool that can be used in combination with peephole.				■
Entry Control with CCTV and Door Strikes	Allows employees to view and communicate remotely with visitors before allowing access. Not applicable for Levels III and above because of entry screening devices required at these Levels.				■

● = Minimum standard ○ = Desirable ▲ = Standard based on facility evaluation
 ■ = Not applicable ● = CBP Minimum standard

LEVEL IV FACILITY: Interior Security Standards		Applicability			
		●	○	▲	■
Employee/Visitor Identification					
Agency Photo Identification	Displayed at all times by all personnel. May not be required in smaller facilities.	●			
Visitor Control/Screening System	Visitors are required to sign-in with a receptionist or guard. Visitors are required to be escorted and wear a formal identification badge.	●			
Visitor Identification Accountability System	Stringent methods of control over visitor badges will ensure that visitors wearing badges have been screened and are authorized to be at the facility during the appropriate time frame.	●			
Established Issuing Authority	Develop procedures and establish authority for issuing employee and visitor identification.	●			
Utilities					
Prevent Unauthorized Access to Utility Areas	Smaller facilities may not have control over utility access or locations of utility areas. Where possible, assure that utility areas are secure and that only authorized personnel can gain entry.	●			
Provide Emergency Power to Critical Systems	CBP requires that all alarm systems, CCTV monitoring devices, fire protection systems, and entry control devices, etc., are required to be connected to emergency power sources. The occupant is responsible for determining which computer or communication systems require backup power.	●			
Occupant Emergency Plans (OEPs)					
Examine OEP and Contingency Procedures Based on Threats	Review and update current OEP procedures for thoroughness. OEPs should reflect the current security climate.	●			
OEPs in Place, Updated Annually, Periodic Testing Exercise	See Chapter 15, Occupant Emergency Planning	●			
Assign and Train OEP Officials	Assignment based on GSA requirement that largest tenant in facility maintain OEP responsibility. Officials should be assigned, trained and a contingency plan established for emergency activation of the OEP in the place of OEP officials.	●			
Annual Occupant Training	All occupants should be aware of their individual responsibilities in an emergency situation.	●			
Day Care Centers					
Evaluate Whether to Locate Day Care Facility in Buildings with High Threat Activities	Conduct a thorough review of security and safety standards.	●			
Compare Feasibility of Locating Day Care in Facilities Outside Locations	If a facility is being considered for a day care center, an evaluation should be made based on the risk factors associated with tenants and the location of the facility.	●			

● = Minimum standard ○ = Desirable ▲ = Standard based on facility evaluation
 ■ = Not applicable ● = CBP Minimum standard

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

LEVEL IV FACILITY: Security Planning		Applicability			
Intelligence Sharing					
Establish Law Enforcement Agency/ Security Liaisons	Intelligence sharing between law enforcement agencies and security organizations should be established in order to facilitate the accurate flow of timely and relevant information between appropriate government agencies. Agencies involved in providing security must be part of the complete intelligence process.				
Procedures for Intelligence Receipt & Dissemination	Determine what procedures exist to ensure timely delivery of critical intelligence. Review and improve procedures to alert agencies and specific targets of criminal/terrorist threats. Establish standard administrative procedures for response to incoming alerts. Review flow of information for effectiveness and time critical dissemination.				
Uniform Security & Threat Nomenclature	To facilitate communication, standardized terminology for Alert Levels should be implemented (e.g., Normal, Low, Moderate, and High -as recommended by Security Standards Committee).				
Training					
Annual Security Awareness Training	Provide security awareness training for all occupants. At a minimum, self-study programs utilizing videos, and literature, etc., should be implemented. These materials should provide up-to-date information covering security practices, employee security awareness, and personal safety, etc.				
Unarmed Guard Qualifications and Training Requirements	Liaison with the Federal Protective Service (FPS) to ensure the standardized unarmed guard qualifications and training requirements are being met. No CBP entity has contracting authority for guard service within DHS except FPS.				
Armed Guard Qualifications and Training Requirements	Liaison with the Federal Protective Service to ensure the standardized armed guard qualifications and training requirements are being met. No CBP entity has contracting authority for guard service within DHS except FPS.				
Tenant Assignment					
Co-locate Agencies with Similar Security Needs	To capitalize on efficiencies and economies, agencies with like security requirements should be located in the same facility if possible.				
Do Not Co-locate High/ Low Risk Agencies	Low risk agencies should not take on additional risk by being located with high-risk agencies.				
Administrative Procedures					
Flexible Work Schedules	Establish flexible work schedule in high threat/high risk area to minimize employee vulnerability to criminal activity. Flexible work schedules can enhance employee safety by staggering reporting and departure times.				
Background Security Checks and Security Control Procedures	Conduct background security checks and/or establish security control procedures for service contract personnel.				
Arrange for Employee Parking in or Near Building after Normal Work Hours	Minimize exposure to criminal activity by allowing employees to park at or inside the building after normal work hours.				

LEVEL IV FACILITY: Security Planning		Applicability			
		●	○	▲	■
Construction/Renovation					
Install Shatter Resistant materials On All Exterior Windows (Shatter Protection)	Application of shatter resistant material to protect personnel and citizens from the hazards of flying glass as a result of impact or explosion. See Appendix 7.7. Windows .	●			
Review Current Projects for Blast Standards	Designs and construction projects should be reviewed, if possible, to incorporate current technology and blast standards. Immediate review of ongoing projects may generate savings in the implementation of upgrading to higher blast standards prior to completion of construction.	●			
Review/Establish Uniform Construction Standards	Review, establish, and implement uniform construction standards as it relates to security consideration.	●			
Review/Establish Uniform New Design Standards for Blast Resistance	In smaller facilities or those that lease space, control over design standards may not be possible. However, future site selections should attempt to locate in facilities that do meet standards. New construction of government-controlled facilities should review, establish, and implement new design standards for blast resistance.	●			
Establish Street Set-Back for New Construction	Every foot between a potential bomb and a building will dramatically reduce damage and increase the survival rate. Street set-back is always desirable, but shall be used in conjunction with barriers in Level IV and V facilities.	●			

● = Minimum standard ○ = Desirable ▲ = Standard based on facility evaluation
 ■ = Not applicable ● = CBP Minimum standard



APPENDIX 6.10: SECURE BORDER INITIATIVE

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

SECURE BORDER INITIATIVE

I. GENERAL

- A. This chapter establishes the policy for minimum security requirements for Secure Border Initiative (SBI) offices and SBI^{net} Tower sites necessary for the safety of CBP employees and the protection of Government property and information.
- B. The following SBI Construction minimum security requirements apply to all new construction, reconstruction, alterations, modifications, and repairs to existing SBI offices and SBI^{net} Tower sites. **OVERVIEW OF SECURE BORDER INITIATIVE:**
- C. SBI is one component of the Department of Homeland Security's Secure Border Initiative that will address the security challenges along the southern and northern land borders. SBI in coordination with the other border security missions conducted by ICE, USCIS, USGC, Intelligence, and the Department of Justice works to address our nation's immigration border security challenges.
- D. The scope of SBI provides DHS and CBP with the optimum mix of personnel, technology, infrastructure, and response platforms to detect, identify, classify, and respond to illegal breaches of international borders with Canada and Mexico and thereby bring the situations to the appropriate law enforcement resolution. SBI will employ next generation technology in the area of cameras, ground based radar, communications, unmanned aerial vehicles, underground sensors, and sophisticated software packages for terrain environments. SBI will integrate multiple state of the art systems and traditional security infrastructure into single comprehensive border security for the department.

II. SBI SUITE/INTEL ROOM MINIMUM CONSTRUCTION STANDARDS

- A. Heavy-duty builder's hardware shall be used in construction. All screws, nuts, bolts, hasps, clamps, bars hinges, and pins should be securely fastened to preclude unwanted entry. Hardware accessible from outside the SBI Suite/Intel must be peened, pinned, or spot-welded to preclude removal.
- B. Walls
 - 1. The perimeter walls, floors, and ceiling will be permanently constructed using slab to slab construction. Slab to slab construction (true floor to the true ceiling) is de-fined as walls that extend from the solid concrete floor to the underside of the roof slab above. All construction must be done in a manner as to provide visual evidence of unauthorized penetration.
 - 2. Walls will be constructed using reinforced Concrete Masonry Units (CMU) not less than 8 inches thick.

[RETURN TO TOP](#)

- (a) Masonry units will be solid brick or hollow type block and filled with concrete and metal reinforcement bars.
 - (b) When using hollow type blocks, they will be filled with concrete and reinforced with #5 rebar, a minimum of 5/8 inches in diameter. The reinforcing is to be anchored into the ceiling and floor to a minimum depth of one-half the thickness of the adjoining member.
3. Where a CMU wall is not feasible, the following alternate method can be used:
- (a) The inside walls will be constructed of 5/8-inch fire rated gypsum board and the outside walls with standard 5/8-inch gypsum board and a layer of 9-gauge expanded metal on the inside of the area.
 - (b) The expanded metal shall be in a 1½-inch x 2-inch diamond pattern, attached to metal studs and spot welded at 6-inch intervals. If wooden studs are used to attach the expanded metal, the studs shall be no less than 2 inches x 4 inches; otherwise it shall be securely anchored to the stud with stainless steel screws and washers. The screws shall be no less than 3 inches in length and installed at no more than 6-inch intervals. The expanded metal shall be affixed in a manner to prevent tampering and to show evidence of attempts at removal. Although less expensive to build this is not the preferred method for securing arms and ammunition. See Figure 1.
 - (c) To view the specifications for expanded metal mesh, see Section VII, Construction Standards: Expanded Metal Mesh Specifications.

C. Ceilings:

1. When walls are being constructed using the CMU method described above in III.2(b), and they do not extend to the true ceiling and a suspended (false) ceiling is created, the suspended (false) ceiling must be reinforced with a 9-gauge expanded metal to serve as the true ceiling. When expanded metal is used, it must overlap the adjoining walls and be secured in such a manner that removal will show evidence of tampering.
2. When constructing walls using the alternate method described above in paragraph III.3(b), and the walls do not extend from slab to slab and a suspended (false) ceiling is created, the suspended (false) ceiling must be reinforced with a 9-gauge expanded metal to serve as the true ceiling.
 - (a) When metal studs are used to construct the walls, the expanded metal must be spot welded at 6-inch intervals to the framing of the side panels so that any attempted removal will show evidence of tampering.

(b) When wooden studs are used to construct the walls, the expanded metal must be securely anchored to the stud with stainless steel screws and washers. The screws shall be no less than 3 inches in length and installed at no more than 6-inch intervals.

3. When the walls of an area do extend from slab to slab and a false ceiling is added it is not necessary to reinforce the false ceiling.

D. Floors:

1. For new construction, floors will consist of reinforced concrete with a minimum thickness of 8 inches. The concrete mixture will have a minimum compressive strength of at least 3,000 psi. Reinforcement will be accomplished with 2 grids of #5 rebar, a minimum of 5/8-inch diameter, positioned centrally and spaced horizontally and vertically 6 inches on center; rods will be tied or welded at intersections.
2. Existing floors not meeting the standards of new construction (minimum thickness of 8 inches) can be modified by the addition of steel plating, a minimum of 1/4-inch thick. The steel plates are to be welded at 6 inches on center, vertically and horizontally, with 1-inch welds to supporting steel members of a minimum thickness equal to that of the plate. If the supporting members are to be placed in a contiguous floor and ceiling of reinforced concrete, they must be either firmly anchored to and/or embedded into the floor and ceiling. If the floor and/or ceiling construction contains less than 8 inches of reinforced concrete, then a steel liner, a minimum 1/4-inch thick, must be installed on the inside floor and/or ceiling.

E. Doors/Door Hardware:

1. Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1 3/4 inches thick, and hung in 12-gauge hollow metal frames.
2. All doors to unclassified area(s) will be equipped as a minimum with a card reader/keypad and a Commercial Grade 1 – GSA approved High Security Lockset. Doors to classified areas must be equipped as a minimum with an FF-L-2890 compliant CDX-09 High Security Electromechanical Lock and a Commercial Grade 1 – Mortise High Security Lever Lockset. Keys must be off the building master in facilities that are not solely occupied by CBP.
3. Double doors must have one door secured with flush mount bolts at the top and the bottom. Astragals (overlapping molding, preferably metal) must be used to inhibit access to lock bolts.
4. Perimeter door hinge pins that are located outside the office area must be non-removable (peened, pinned, or spot welded). If the door swings outward, hinge side protection in the form of a dowel-pin and socket is required. Refer to [Figure](#)

[2 of Appendix 7.6: Doors and Door Hardware](#) for details. All perimeter doors must have a commercial grade pneumatic door closer and an anti-pry strip installed to prevent the door from being pried open.

5. All door hardware (e.g., hinges, lock hardware) must be secured to door frame with stainless steel screws at least 3 inches long.
6. For additional information on Doors and Door Hardware, refer to [Appendix 7.6. Doors and Door Hardware](#)

F. Windows:

1. SBI rooms shall have no exterior windows.

G. Miscellaneous Openings:

1. Where vents, ducts, registers, sewers, tunnels and other miscellaneous openings are of such size and shape (in excess of 96 inches square) and enter or pass through the area as to permit unauthorized entry, they should be protected with either steel bars or wire mesh grilles. If bars are used, they must be at least 3/8-inch diameter hardened steel, welded vertically and horizontally, six inches on center. If grilles are used, they must be of 9-gauge woven wire mesh.
2. For additional information on Miscellaneous Openings, refer to [Appendix 7.8. Openings](#). Incorporate a steel security wall system design in the project.

III. SBI MODULAR DESIGN STANDARDS OVERVIEW AND CONSTRUCTION METHOD

1. The modular SBI facility is being constructed of steel framing in lieu of wood or metal design to meet security. The proposed construction will be steel framed walls (in lieu of wood) for the modules. The proposed floor system will be a steel panel system of a “sandwich type” panel of two steel plates with foam insulation in between the plates. The panel is only 2 inches thick. Typical partition walls in the main station administrative areas will be steel studs with drywall.
2. The modular SBI facility design will be incorporating a composite wall, steel security wall system design in the project. The wall design would be double skinned, hollow metal panels with interlocking rabbeted edges that are manufactured from heavy gauge galvanized steel. The walls “2” thick panels, compared with 6” or 8” thick concrete wall systems, result in sizable weight reduction for the facility, greatly reducing footing and foundation requirements.
3. The steel composite wall panel system achieves the same Sound Transmission Class (STC) rating as an 8” block wall and meets the following ASTM requirements: ASTM 2322 (Physical Assault on Fixed Horizontal Barriers for Detention/Correction facilities), ASTM 1450-97 (Hollow Metal Swing Door), and

[RETURN TO TOP](#)

ASTM 1592-01 (Detention Hollow Metal Vision Systems) security level 1.

A. Access Control

1. Cardkey access systems or similar personal identification verification systems must be provided on all perimeter doors or doors leading from public areas to staff-restricted areas. The security system should use balanced magnetic switches, glass break sensors, balanced magnetic contact switch sets, a closed circuit television (CCTV) monitoring station, a color/ monochrome CCTV system, and a duress alarm. The access system must be designed in compliance with the Federal Information Processing Standard (FIPS) 201 Personal Identity Verification (PIV) for Federal Employees and Contractors. Homeland Security Presidential Directive (HSPD) 12 requires federal facilities to have secure personal electronic identification access include card readers and proximity card readers, as well as biometric readers.

B. Closed Circuit Television (CCTV)

1. At a minimum, CCTV will monitor the entrance and perimeter areas. The minimum components that the system must have is one color monitor and one high resolution digital video recorder (DVR), capable of recording a minimum of 30 days and playing back any camera view. All camera views associated with an alarm must be automatically recorded. CCTV images must be retrievable and operable over weekends and holidays.
2. For additional information on CCTV, refer to [Appendix 8.12, CCTV](#).

C. Duress Alarm

1. Duress Alarms generate a separate and distinct audible/visual alarm in the Control Center. Upon any activation of a duress alarm, a dedicated CCTV camera must “queue-up” to the SBI room entrance door/s and provide the Control Center with an immediate view of the situation. The duress button should be placed in an area out of immediate view of suspect individual. They are to be placed beneath workstations if possible. The duress button must be a recessed type thus preventing accidental activations.
2. The duress/panic alarm should sound in the building control center, if one exists, or at the local police station or at an approved Class A central station where appropriate response is assured.

D. Intrusion Detection System (IDS)

1. All SBI areas shall include an IDS and it shall be connected to a Class A Central Monitoring Station. At a minimum the IDS should include a UL 634 high security Level 2 balanced magnetic switch (BMS) on the door, motion detection sensors

[RETURN TO TOP](#)

inside the room and a card reader/keypad to track users. There must be a backup method of communication set up with the Central Monitoring Station (e.g. a wireless phone link, such as cellular or an extra analog/digital telephone line), so that if a telephone line is cut or otherwise interrupted, an alarm is activated at the Central Monitoring Station. Acknowledgement of an alarm condition by the Central Monitoring Station must take place within 30 seconds of the alarm. The Central Monitoring Station must dispatch the correct response (law enforcement, duty agent, CCC, etc.).

2. For additional information on IDS, refer to Appendix 8.9, Intrusion Detection Systems.

E. Sound Attenuation

1. Perimeter walls, ceilings and floors of the entire office space will have a Sound Transmission Class (STC) rating of 45, or better. STC of 45 or better is defined as loud speech that can be faintly heard, but not understood. Normal speech is unintelligible. The 9 gauge expanded metal used above the perimeter and other walls will have to be augmented with other building materials to ensure an approved STC rating.

F. Uninterrupted Power Source

1. All critical communications and monitoring equipment must have uninterrupted power supply (UPS) and should be connected to emergency power generators to maintain services during sustained power outages. Remote door release systems must have battery back up to allow control during emergencies and power failure. Emergency power systems must be adequate to sustain security lighting, CCTV, communications requirements, and other essential services required within a restricted and/or secured area, for a period of no less than 72 hours from the time of power failure. Emergency power systems will be tested quarterly to ensure the system will perform as needed and the test results will be recorded. Emergency power sources will start automatically. Battery powered lights and essential communications will be available at all times at key locations within a restricted and/or secured area, in the event of complete failure of both the primary and emergency sources of power. (SBI space is "mission critical" and thus will be on 100% emergency power. All electronics and computers will run through the UPS system. The UPS system will provide uninterruptible power until the generator starts and the UPS system also acts as a surge protector to provide smooth transitional power to the computers and other electronic equipment).

IV. SBI_{NET} TOWERS

- A. Locate towers on federally controlled property whenever possible. Design considerations using the ANSI/TIA-222-Rev G Standard, Class III: structures. Class

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

III structures specifically designed for essential communications or structures that represent a substantial hazard to human life and/or property. Examples of essential communications would be: civil or national defense; emergency, rescue, or disaster operations; military and navigation facilities. Loadings are increased for structures of this classification compared to Class II structures (15% for wind, 25% for ice and 50% for earthquake).

- B. *SBlnet* Tower structures and support modular sheds shall be hardened against small arms fire (UL 752) to minimum level III. (National Institute of Justice- A. Standard 0108.01).
- C. Harden support systems:
 - 1. Standby power sources, Electrical system conduits, Mechanical system conduits for air conditioning, heating, and venting systems, Roof-mounted equipment, filter banks, fuel systems, security systems and other openings must be protected from sabotage.
 - 2. All critical power, communications, and IDS lines should be well protected. Standby E. power sources must be protected from sabotage by facility hardening and IDS coverage.
- D. Access Control: Install access control device or system at entry point. Ensure that the access control device if keycard activated conforms to HSPD-12 compliancy. Examples such as mechanical push-button locks, electronic push button locks, digital touch pads with key override and proximity card readers may be utilized to augment the deadbolt lock.
- E. Closed Circuit Television: Install UL approved CCTV coverage to provide 360 degree visual surveillance of the tower area upon alarm activation at outer fence perimeter. Install closed circuit television coverage of the tower that “queues up” if an alarm activates at the site providing immediate visual observation of the situation, and digital recording at the monitoring center to review. Provide CCTV coverage at entry points (pedestrian/vehicular). Ensure no blind spots exist for the CCTV operator.
- F. Communications: Install alarm activated speaker (hailer) to immediately address threat on site upon alarm activations. Security systems transmission lines shall be encased in metal conduit and hardened against tampering. Intercom systems should have the capacity to accommodate all remote access points.
- G. COMSEC as per NSTISSI No. 4005 (1997) applies to Unattended 2. Telecommunication Facilities: Unattended telecommunications facilities must be protected by IDS or guarded in accordance with the requirements of paragraph # 32 of NSTISSI.
 - 1. Where IDS is employed and more than 15 minutes are required to (a) respond

- to an alarm, the COMSEC equipment in use should have remote zeroization capability.
2. In cryptography, (b) zeroisation (also spelled zeroization) is the practice of erasing sensitive parameters (especially keys) from a cryptographic module to prevent their disclosure if the equipment is captured.
 3. Personnel who visit unattended facilities should inspect for signs of (c) tampering, or attempted penetration (physical check once every 24 hrs.).
- H. Equipment: Install tamper/vandal resistant enclosures for equipment housing for cameras, lights, cabling, and support systems. Ensure camera enclosures are environmental proof to protect against weather elements associated with the specific facility geographical area. IDS devices shall be selected and installed to be fully functional under all environmental conditions for the specific location.
- I. Fence: Install a fence around the perimeter to delay unauthorized access. *SBN*et Towers are Class III critical communication sites and will require above and beyond the standard 12 foot impound lot fencing. *SBN*et Tower perimeter fencing will incorporate anti-ram and fence sensors into their design and construction due to the remote location of these critical assets and their critical mission.
1. *SBN*et Tower fence shall be minimum 12 foot impound lot fence as specified in [Appendix 7.3 - 12 foot impound lot fence](#).
 2. Restricted Areas. The following criteria are in addition to the standard fence installation requirements (a) listed above. Impoundment Lot Fence (Outside the Perimeter) will be 12 ft.(3.65m) high with a vehicle gate system and will have two outriggers installed at opposing 45-degree angles along the top of the fence to form a “V” or a “Y” configuration with dual coil (24”-30”) concertina/razor wire secured to the fence every 24”. The mesh will be a minimum 1 inches (25.4-mm) per side. The gate shall have electronic intrusion detection, access control system with audit capability and HSPD 12 FIPS 201 compliant.
 3. A reasonable approach to reinforce a standard chain link perimeter fence to resist a vehicle attack is both simple and aesthetic. Place a 3/4-inch (19.1-mm) diameter aircraft cable, Compliant with MIL-HDBK-1013/10 and conforming to MIL-W-88020, along the fence line, between the fence posts and the chain link fabric as per ([Appendix 7.3 II.6](#) and [7](#) and shown in Figure 10 and 12 foot impound lot cut sheet..
 4. [Digging under fence deterrent](#)
 - Fence will be buried 1’ below grade (Bottom 12” of fence material buried by 12” of soil composite grade).

- Rail pipe underneath grade to prevent peeling up
- J. Fence detection sensors are used, the best application is to use a dual zone to cover fence and buried in the ground leading to fence on the attack side. The fence having a strain-sensitive cable taut wire on the fence, to include the gate, and Microwave Fence Sensor (MFS) or Portal Coaxial Cable Sensor (PCCS) for detection with a Closed Circuit Television (CCTV).
- K. Gates will be provided with locking hardware conforming to RR-F-191/2. The locking system is designed to provide an equal level penetration resistance when a gate is closed and locked. Where locking hardware is not practicable, ½ inch (12.7 mm) case hardened chains meeting the requirements of RR-C-271 will be used with a padlock meeting the requirements of Federal Specification FF-P-2827A.
- L. Fence Signage:
 1. Install bilingual signage on all sides of the exterior fence line stating that the area is restricted, enforced by intrusion detection and only authorized personnel are admitted. Install appropriate (bilingual) signage. Fenced areas should have gate areas posted with signs 3 feet by 3 feet with lettering of contrasting color to the background and at least 1-inch high and ½ inch wide. At intervals of about 30-feet, signs bearing the following must be posted on fences:
 2. Perimeter security fences for restricted areas will be posted with signs. Signs will be posted on security fences at no less than 200-foot (60.9-m) intervals along the entire perimeter. Where a language other than English is prevalent, warning signs will be posted in both languages.

U.S. GOVERNMENT PROPERTY
NO TRESPASSING
VIOLATORS WILL BE PROSECUTED

- M. Clear Zones:
 1. Unless otherwise specified, locate the perimeter security fence at least 30 feet from enclosed structures (except guard shelters). Provide a clear zone not less than 30 feet wide immediately outside the fence. Keep this area devoid of buildings, parking areas, poles, guy line anchors, shrubs, trees, sign boards, and any other object that could conceal personnel. Grass is permissible, provided it is kept mowed. Provide a similar clear zone at least 30 feet wide immediately inside the fence. Ensure this area meets the requirements of the exterior clear zone, except for the installation of approved guard shelters and protective lighting poles
- N. Intrusion Detection System: Install UL approved Intrusion Detection System on inner perimeter fence line (microwave/ported coaxial), entry contacts (balanced magnetic switches/motion detection) of support systems structures, in ground (buried) sensors

[RETURN TO TOP](#)

within the dual fence clear zone, or wide area sensors that will detect in advance of exterior fence of intruder presence. All critical power, communications, and IDS lines should be well protected. Standby power sources must be protected from sabotage by facility hardening and IDS coverage.

- O. Security Lighting: Install perimeter protective security lighting to support threat detection and assessment function in the event intruders approach the exterior fence line. Install a safety beacon on the tower to alert low flying aircraft in the vicinity for safety reasons. The National Institute of Standards and Technology (NIST) standard requires critical areas to be illuminated 8 feet in height with 2-foot candle power.

P. Uninterrupted Power Source

- 1. All critical communications and monitoring equipment must have uninterrupted power supply (UPS) and should be connected to emergency power generators to maintain services during sustained power outages. Remote door release systems must have battery back up to allow control during emergencies and power failure. Emergency power systems must be adequate to sustain security lighting, CCTV, communications requirements, and other essential services required within a restricted and/or secured area, for a period of no less than 72 hours from the time of power failure. Emergency power systems will be tested quarterly to ensure the system will perform as needed and the test results will be recorded. Emergency power sources will start automatically. Battery powered lights and essential communications will be available at all times at key locations within a restricted and/or secured area, in the event of complete failure of both the primary and emergency sources of power. (SBI space is “mission critical” and thus will be on 100% emergency power. All electronics will run through the UPS system. The UPS system will provide uninterruptible power until the generator starts and the UPS system also acts as a surge protector to provide smooth transitional power to the electronic equipment).

Q. Special Security Feature:

- 1. The SBI communications shelter shall be bullet resistant withstanding 30/06 rifle fire at a distance of 15 feet per UL 752 standards. The shelter shall be vandal resistant and be constructed of steel reinforced concrete. The shelter structure shall provide a 2-hour fire rating as defined by the Uniform Building Code and meet Zone 4 seismic requirements. The shelter shall be designed for the explicit use of housing electronic equipment within a controlled atmosphere required for the proper conditions for transmitting and receiving equipment.
- 2. Fuel Storage Tank: Installed buried fuel storage tank or purchase GSA approved ballistic resistant above ground fuel storage tank to protect against small arms fire (UL 752) to minimum level III. (National Institute of Justice- A. Standard 0108.01). ensure continuity of the cable system.





APPENDIX 7.2: PERIMETER SECURITY BARRIERS

I. GENERAL

A. Anti-ram perimeter security barriers, also known as vehicle impact rated barriers, are designed to prevent the penetration of explosive-laden vehicles into the defended perimeter. Department of State (DoS)-rated physical barriers are grouped into several areas according to their function:

1. Active anti-ram barriers:

- (a) Retractable bollards
- (b) Deep foundation crash beam systems
- (c) Cable based systems
- (d) Drop arm/bar
- (e) Cantilever sliding gates
- (f) Interlocking steel beam gates
- (g) Wedge barriers

2. Passive anti-ram barriers:

- (a) Bollard
- (b) Planters
- (c) Cable based systems
- (d) Fences

3. Non-rated passive anti-ram barriers:

- (a) Trees and shrubs
- (b) Shallow bodies of water
- (c) Low berms
- (d) Shallow ditches
- (e) Unreinforced fences
- (f) High curbs

4. Although none of the non-rated passive vehicle barriers would stop a determined

[RETURN TO TOP](#)

aggressor, the act of driving through or over them would attract attention. They can also be placed with rated barriers such as bollards and planters for aesthetic reasons.

5. For further details see:

- (a) [DoS and DoD Barrier Anti-Ram Vehicle Barrier Certification](#)
- (b) [UFC Criteria for Security Engineering: Entry Control Facilities/Access Control Points](#)
- (c) [Chapter 7.3 Fencing](#)

B. Active anti-ram barriers fall into the perimeter tier of the DHS tiered defensive system concept. Active anti-ram barriers protect the vehicular access/egress points or Compound Access Controls (CACs), limiting perimeter vulnerability during the passage of vehicular traffic. Performance criteria for vehicle barrier systems are concerned with three areas:

- 1. Impact conditions and performance levels
- 2. Functional requirements and power systems
- 3. Control circuits

C. Active anti-ram barriers shall be selected from the list of Department of State (DoS) certified barriers. The Contractor shall also note that site adapted foundation designs require Security Management Division (SMD) approval.

II. ABBREVIATIONS

- BPA Blanket Purchase Agreement
- Cm Centimeter(s)
- DIA Diameter
- DC Direct Current
- DHS Department of Homeland Security
- DoS Department of State
- CBP Customs and Border Protection
- FBO Foreign Buildings Operations
- GSO General Services Officer
- Hz Hertz
- IPS Iron Pipe Size
- IR Infrared
- Km/h Kilometers per Hour
- kN Kilonewton(s)
- LBS Pounds

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- MAX Maximum
- mm Millimeter(s)
- Mpa Megapascal(s)
- NPT National Pipe Thread
- OC On Center
- OD Outside Diameter
- PLCS Places
- Psi Pounds per Square Inch
- PVC Polyvinyl Chloride
- SMD Security Management Division
- SQ Square
- TYP Typical
- V Volts

III. ACTIVE ANTI-RAM BARRIERS

A. Impact Conditions and Performance Levels

1. DoS Certification Program:

(a) The Department of State (DoS) has developed performance criteria and a testing procedure for Active Anti-Ram Vehicle Barrier systems: SD-STD-02.01, Revision A, March 2003, titled Specification for Vehicle Crash Test of Perimeter Barriers and Gates. This document specifies the testing procedure required for DoS certification of vehicle barriers. This program establishes a series of vehicle barrier classifications based on given impact conditions and performance levels. The rating of the barrier is determined when a 15,000 lb. (6810 kg) gross-weight vehicle impacts a barrier from a perpendicular direction. A K12 rating is achieved when the vehicle traveling at 50 mph is successfully arrested by the barrier. A K8 rating is achieved for a speed of 40 mph; and a K4 rating is achieved at 30 mph. In order to receive the highest DoS certification, the penetration of the vehicles cargo bed must not exceed 1 meter beyond the pre-impact inside edge of the barrier. Only vehicle barriers rated for the highest anti-ram level –K12/L3- may be used unless the designer can obtain CBP/ SMD permission to use a lower rated vehicle barrier.

2. For further details see:

- (a) [DoS and DoD Barrier Anti-Ram Vehicle Barrier Certification](#)
- (b) [UFC Criteria for Security Engineering: Entry Control Facilities/Access Control Points](#)

B. Impact Conditions

1. The standard categories differ only in the measured speed of the standardized 66.7 kN (15,000 lbs) test vehicle. The following designations are used to specify the impact conditions:

<u>Impact Conditions</u>	<u>Nominal Impact Speed</u>
K4	30 mph/48.4 km/h
K8	40 mph/64.5 km/h
K12	50 mph/ 81.0 km/h

C. Performance Levels

1. The vehicle barriers capability to arrest the crash vehicle is assessed according to three performance levels. A vehicle barrier that does not perform within these limits will not receive a rating and may be ineligible for procurement for DOS facilities. The following designations are used to rate a barriers performance:

<u>Performance Level</u>	<u>Crash Test Assessment</u>
L3.0	Vehicle and cargo are to be stopped although vehicle partial penetration and/or barrier deflection of up to 1 meter are permitted.
L2.0	Vehicle and cargo are to be stopped although vehicle partial penetration and/or barrier deflection of up to 6 meters are permitted.
L1.0	Vehicle is disabled and does not travel more than 15 meters after impact

D. Functional Requirements

1. Functional Requirements:
 - (a) The vehicle arrest system shall be provided with all of the functions and accessories included in the DOS Blanket Purchase Agreement (BPA) with the approved vendor. This includes, but is not limited to, a visible device such as a signal light (indicating the barriers status to an approaching driver) and emergency override.
2. Coordination and Surface Preparation:
 - (a) Early project coordination shall include selection of a proper barrier for the site, review of site conditions, provision of surface area preparation (including, but not limited to: special drainage/pumping, prevention of freezing/icing, prevention of corrosion, etc.), provision of power and

hydraulic lines, and provision of conduits and cable for barrier control points, etc.

IV. POWER SYSTEM AND CONTROL CIRCUITS

A. Power System and Control Circuits

1. Systems approved for use by CBP shall meet the following requirements:

- (a) **ELECTRIC MOTORS:** Voltage and phase must be compatible with the local power supply. Dual-rated 50 or 60 Hz motors are acceptable if warranted by the manufacturer for both conditions.
- (b) **CONTROL VOLTAGE:** The system should be no more than 24 volts, direct current.
- (c) **CONTROL SYSTEM:** The system must be designed in such a way that when power fails, the barriers automatically retain a status quo position; i.e., they will be neither fail secure nor fail safe. The control system must provide a manual operating capability for use in the event of power failure.
- (d) **DEPENDABILITY:** The system must provide maximum dependability and ease of maintenance. System design considerations should include, and their reliability will be assessed in light of, worst-known conditions; i.e., frequent power surges, brownouts and failures, absence of locally-available skilled labor, adverse climatic conditions, poor drainage, etc.
- (e) **CONTROL CIRCUITS:** The system must have two standard controls circuits: a slave or local control for the guard at the Perimeter Gate and a master or remote control for the Security Guard Booth. Both sets of controls will include status indicator lights for power and barrier position.

B. Local Control

1. The local guard control will have an emergency (fast operation) secure switch. The emergency switch for the local guard control will not be equipped with reset capability. The local guard control will include an annunciator, which will be triggered whenever the barrier remains in the non-secure position for a range of 0 to 60 seconds. The local control will not be provided with a reset switch for this feature.

C. Remote Control

1. A remote master control will be used at all posts. The remote master control will have an override switch and reset button for the local emergency override feature. The remote master control panel will have either an annunciator or a

[RETURN TO TOP](#)

signal light triggered by the local control annunciator. The security guard booth alarm, however, will include a silencer for the audible annunciator, if applicable. The annunciator will disarm automatically when the override switch is used. The remote master control will also have a reset switch for the local control annunciator.

D. Power and Hydraulic Lines

1. When power or hydraulic lines are not below ground, they will be protected through the use of rigid conduit. Manufacturers shall provide fail-safe lock options to the hydraulic reservoirs which will prevent the barrier from lowering in the event of hydraulic failure. The use of this fail-in-place is encouraged. For the most efficient operation, locate the pump/motor as close as possible to the barrier and with a minimum of turns and bends in the hydraulic lines themselves.

V. MAINTENANCE FOR ACTIVE ANTI-RAM VEHICLE BARRIERS

A. The philosophy for the maintenance of active vehicle barriers is as follows:

1. **Inspection/Maintenance Program:** The importance of adequate maintenance cannot be overemphasized. Malfunction of an active vehicle barrier may seriously compromise the security of the perimeter. An inspection/maintenance program must be established to ensure that active vehicle barriers will function as intended and as rapidly as the situation demands.
2. **Local Responsibility:** for the inspection/maintenance of installed active barrier systems must be established. Normally, the General Services Officer (GSO) will be responsible.
3. **System Documentation:** Provided locally at the time of system installation, must be reviewed to establish written inspection/maintenance guidance for use by local personnel. Some systems come with separate component manuals and maintenance data which must also be reviewed.

(a) The resulting guide should include as a minimum:

- Inspection/maintenance procedures (what to check, locations, what steps to follow, etc.).
- Special safety precautions.
- A listing of parts/components requiring inspection/maintenance together with frequency of the inspection/maintenance.
- Identification of specific maintenance materials or products (e.g., type or grade of oil and other fluids, size and types of filters, etc.).

- Identification of any special tool that must be available before inspection/maintenance can be performed.

VI. BOLLARDS AND PLANTERS

A. Bollards and planters fall into the perimeter tier of DHS/CBP's tiered defense system concept. Bollards and planters are designed to prevent the penetration of an explosive-laden vehicle into the compound. They are easily constructed and require low maintenance. They are effective in channeling vehicular traffic and reducing vehicular velocity.

B. Passive Perimeter Barriers

1. Passive anti-ram perimeter security barriers are designed to prevent the penetration of explosive-laden vehicles. Properly located and constructed bollards and planters are highly effective types of passive barriers. Where required, passive barriers shall be of a construction design approved by DHS/CBP/SMD to meet anti-ram standards K12 L3 (effectively arrest a 6810-kg (15000-lb.) gross weight vehicle traveling at a maximum of 80 kph perpendicular to the barrier) and shall raise a minimum of 915 mm (36 inches) above grade. This is intended to prevent a large-tired or high-axle vehicle such as a truck from rolling over the barrier.
2. Non-proprietary barriers such as bollards and planters can be effective supplements to existing substandard walls or fence lines in areas where it is not feasible to construct new walls or fences. Properly located and constructed, these barriers can reduce access size, provide traffic channelization and substantially reduce vehicular velocity.

C. Bollards

1. Steel bollards are an effective means to enhance security against vehicular bomb attacks and are easily constructed locally.
 - (a) Approved bollards are constructed of structural steel pipe composed of, or equal to, ASTM A-53, Grade B; or A-501, with a yield point of 250 MPa. The pipe should be a minimum of 2.1 m (83 inches) in overall length, have a minimum outside diameter of 200 mm (7.8 inches), and a wall thickness of 12 mm (0.42 inches). Each bollard is to be filled with concrete and topped with a grout wash. Spacing between bollards should be .90 m (35 inches) on center. They should be embedded to a depth of 1.2 m (47 inches) below grade in a continuous concrete footing.
 - **CONCRETE FOOTING:** Shall be installed with minimum 28 day strength of 20.5 MPa. The footing should be continuous for maximum resistance. The minimum width for the continuous footing is .60m and

[RETURN TO TOP](#)

the minimum depth is 1.20m.

- **STRUCTURAL STEEL CHANNEL:** The bollards should be reinforced with a structural steel channel of, or equal to, ASTM A-36. Use a 250 x 30 mm channel. The channel should be located on the attack side and attached to each bollard with a minimum of two 20-mm anchor bolts and nuts welded onto each channel after installation. The top flange of the channel should be 750 mm above grade.
- **CORROSION:** The portion of the bollard at grade is susceptible to corrosion from exposure to standing water. Additionally, it is difficult to achieve a good quality paint system in this location.
 - i. Therefore, measures must be taken to inhibit corrosion of the steel pipe. The most effective method is to apply a minimum 0.10mm thickness of Scotchcoat or X-Tru Coat along the entire length of the pipe. These coatings are extremely hard resin-based epoxies, and can last up to 20 years. An alternative is a rubber type shrink sleeve which is slipped over the pipe and heated with a low temperature flame to shrink the sleeve tightly around the bollard. The sleeve is an excellent insulator against electrolytic corrosion.
- **RATING:** Bollards described above are capable of stopping the perpendicular impact of a 6810 kg vehicle traveling at 80 kph with 915 mm (or less) of penetration.

D. Concrete planters

1. Planters serve as vehicular barricades, and are an attractive means of channeling traffic.
2. The planters should be constructed of reinforced concrete with a minimum 28 day strength of 20.5 MPa. The quality of construction is to be in accordance with American Concrete Institute (ACI) codes or the equivalent. All steel reinforcing bars are to be lapped a minimum of 300 mm where discontinuous or where splices occur.
 - (a) **DIMENSIONS:** In the plan view the individual units should be 2.75 m x 900 mm, with a support member located at each end and midway between the two ends. A variation of the 2.75-m planter is the continuous planter, which permits flexibility in length. The following specifications are consistent for both the 2.75-m planter and the continuous planter. The wall thickness at the attack side of the planter, at both ends and at the support member, should be 300 mm. The wall thickness at the non-attack side should be at least 150 mm.

- (b) HEIGHT: In the cross-sectional view of the planter, the outer wall should extend 965 mm above grade. The center support member should extend 815 mm above grade. The entire unit should be embedded 915 mm below grade. Thus, the overall height will be 1880 mm. If the footing depth below grade causes problems with utility lines, bridge the lines with U-shaped structural steel sleeves.
- (c) HAUNCH: Configured as an isosceles triangle with 150-mm legs, is situated at the intersection of the inside face of the attack side wall and the top of the concrete footing. The haunch is integrally poured with the rest of the planter. The legs of the haunch coincide with the intersecting concrete surfaces.
- (d) DRAINAGE: In order to provide adequate drainage of the planter, a 50-mm PVC drainage pipe is located on center, every 1200 mm. The outlet of the drain should be located just above grade to avoid below surface seepage and/or erosion.
- (e) REINFORCING BARS: Both faces of the planter on the attack side and the center support member should be reinforced with 16mm diameter bars at 200 mm on center each way. The haunch should feature the same size and spacing as the reinforcement above with the reinforcing bars positioned at a 45-degree angle.
- (f) FOOTING: The footing shall be continuous for individual planters. The top of the footing should be reinforced with 14-mm diameter bars at 200 mm on center each way. The bottom of the footing should be reinforced with 16-mm diameter bars at 150 mm on center each way. The faces of the planter on the non-attack side should be reinforced with 14mm diameter bars at 200 mm on center each way.
- (g) SPACING: The maximum spacing between individual planters is 915 mm.
- (h) RATING: These concrete planters described above are capable of stopping the perpendicular impact of a 6810-kg vehicle traveling at 80 kph with 915 mm or less of penetration.



APPENDIX 7.3: FENCING

I. FENCING

A. General

1. Requirements for security fencing generally fall into two categories:

- (a) Perimeter
- (b) Restricted Areas

2. Perimeter fencing:

(a) The entire site must be contained by an 8 ft. (2.43 m) high perimeter fence. The fabric height will be 7 ft. (2.13 m) and have twisted and barbed selvage at the top and bottom. There must be a minimum 1 ft. (.305 m) top guard, for a total fence height of no less than 8 feet (2.43 m). All perimeter chain link fencing will be fabricated with 9-gauge (3.9-mm) steel wire mesh material (type I, II, or IV as defined below, and before any coating) with mesh openings not larger than 2 (50.8 mm) per side. Provide Type I or Type II tension wire, Class 4 coating, in accordance with ASTM A 824. Provide 7-gauge coil spring tension wire for top and bottom wire. All fencing will be installed on the outside of the support posts. A clear zone will be established no less than 20 feet from any structure or object inside the fence and 10 feet from any structure or object outside the fence. The use of residential grade is not permitted. The impact of snow and blowing snow must be considered on the northern border in combination with the gate types. Based on a CBP/IA/SMD vulnerability assessment additional anti-ramming technology may be installed; see [Penetrations-Resistant Barriers, section II.A.6](#), below for detailed specifications.

(b) Top Guard/Outriggers

- Top guard will consist of 1 ft. (.305 m) outward slanting (45-degree angle). Provide barbed wire conforming to ASTM A 121 zinc-coated, Type Z, Class 3, or aluminum-coated, Type A, with 12.5-gauge wire with 14-gauge, round, 4 point barbs spaced no more than 5 inches (125 mm) apart.
- Steel outriggers will be installed to conform with RR-F-191/4 with their overhang facing outward (away from the protected site), except where the fence must be mounted directly on the property line (instead of at least 18 inches (457.2 mm) back), in which case outriggers can be modified (with exception approval by CBP/IA/SMD) to be vertical or angle into the site. At a minimum, the outriggers will provide an additional 12 inches (305 mm) to the fence height. The top guard fencing adjoining gates may range from a vertical height of 18 inches

[RETURN TO TOP](#)

(457.2 mm) to the normal 45-degree outward protection, but only for sufficient distance along the fence line to open the gates adequately. Outriggers will be permanently affixed to the fence posts with screws or by spot welding.

(c) See the [fencing cut sheets](#) for specific requirements.

3. Restricted Areas

(a) The following criteria are in addition to the standard fence installation requirements listed above.

- Impoundment Lot Fence (Outside the Perimeter)

Will be 12 ft.(3.6 m) high with a vehicle gate system and will have two outriggers installed at opposing 45-degree angles along the top of the fence to form a “V” or a “Y” configuration with dual coil (24”-30”) concertina/razor wire secured to the fence every 24”. The mesh will be a minimum 1 inches (25.4-mm) per side. The gate shall have an electronic intrusion detection and access control system with audit capability.

- Seizure Storage Fence

When the seizure storage facility is a stand alone structure, it must be protected by a security fencing system in compliance with the impound lot fence requirements.

- Visitor Parking Fence

When visitor parking and the employee parking are either next to each other or in close proximity to each other, provide a fence with fabric measuring 7 ft.(2.13-m) high fence with an additional 1 ft. (.305 m) outrigger, separating the two parking areas. When located directly adjacent to each other, two outriggers installed at opposing 45-degree angles along the top of the fence to form a “V” or a “Y” configuration with dual coil (24”-30”) concertina/razor wire secured to the fence every 24 in.along the common side.

- Employee Parking Fence

Provide an 8 ft. (2.43-m) high fence with a vehicle and pedestrian gate (see [Gates](#)) system with outrigger for a total height of 8 ft. (2.43-m).

- Inspection Lift Fence (Hard Secondary)

This fence (barrier) must restrict the viewing of the vehicle while in the lift area. As such, use more appropriate fencing material such as masonry or other more solid material. However, care must be given to also provide

[RETURN TO TOP](#)

adequate ventilation for this area. A wall system with decorative openings or screened grills should be considered. The fence does not need to extend to the underside of the canopy, but must extend high enough to restrict viewing or unauthorized entry. The gate must also restrict the viewing into this area.

- **Kennel Holding Cages and Runs**

Galvanized chain link at front, rear, and top of runs set at 6 ft. above finished floors (AFF). Outside fence needs a block wall or vinyl slats attached.

- **Lockable Gate**

Separate runs with masonry systems to 6 ft. AFF

- Emergency generator fence must meet perimeter fence requirements consider the use of privacy slats.
- Other internal fences must meet the perimeter fence requirements at a minimum.

B. Maintenance Considerations

Consider the following when designing chain link fencing:

- Fence components may require additional protective coatings in salt-laden and highly corrosive areas, e.g., plastic coating over galvanized steel fabric.
- Rapid growth of vegetation in fertile areas and rainy climates may justify paving the area under the fence and a portion or all of the clear zones.
- Consideration should be given for equipment, i.e., mowers, tractors, etc., required to maintain vegetation below 8 inches (203.2 mm) and to broadcast defoliant or sterilizing agents.
- Take particular attention in areas with harsh environments to determine if Type IV chain link fabric (which provides a plastic coating over zinc-coated steel) material is desirable. ASTM A 90, Standard Test Method for Weight of Coating on Zinc-Coated Galvanized Iron or Steel Articles, or ASTM A 428, Standard Test Method for Weight of Coating on Aluminum-Coated Iron or Steel Articles may be used to assure adequate protection for chain link fence components. Use ASTM standards where supplemental criteria are either required or desired.

C. Special Security Features

1. Clear Zones:

(a) A clear zone will be established no less than 20 ft. from any structure or object inside the fence and 10 ft. from any structure or object outside the fence. Maintain unobstructed areas or clear zones on both sides of, and between, physical barriers surrounding restricted and non-restricted areas. These areas must be cleared of all vegetation and man-made or natural obstructions that exceed 8 in.(203.2 mm) in height. All clear zones will be clear of visual obstructions such as vines, shrubs, tree limbs, electrical and telephone poles or junction boxes, steam pipes, fire hydrants, etc.

(b) Signage

- Perimeter security fences for restricted areas will be posted with signs. Signs will be posted on security fences at no less than 200 foot (60.9 m) intervals along the entire perimeter. Where a language other than English is prevalent, warning signs will be posted in both languages.

U.S. GOVERNMENT PROPERTY
NO TRESPASSING
VIOLATORS WILL BE PROSECUTED

(c) Drainage Culverts and Utility Openings

- Special protective measures must be designed for culverts, storm drains, sewers, air intakes, exhaust tunnels, and utility openings that:
 - i. Pass through cleared areas.
 - ii. Traverse under or through security fences.
 - iii. Have a cross-section area of 96 square inches (61,939 square mm) or greater, with the smallest dimension being more than 6 inches (152.4 mm). Such openings and barrier penetrations will be protected by securely fastened grills, locked manhole covers, or other equivalent means that prevent entry.
- Grills are fabricated for this purpose by cross-hatching 3/8 in.(9.5-mm) steel bars 9 in.(228.6 mm) on center. The bars will be welded at their intersections. Grills used for culverts will always be placed outside the secure area.
 - i. For steel pipe, the grill ends will be welded to the pipe as shown in [Figure 1](#).
 - ii. For concrete pipe, the grill ends will be welded to a steel rim that fits snugly over the concrete pipe.

- iii. The rim and grillwork will be fastened over the concrete pipe and bolted or pinned to the rim of the concrete pipe as shown in [Figure 2](#). As an alternative, the grill ends can be embedded in a concrete headwall that encapsulates the concrete pipe. See [Figure 7](#). Care must be taken during design to assure that bars and grills across culverts, sewers, storm drains, etc., are not susceptible to clogging. This must be considered early during the security fence planning phase.
- Culverts, storm drains, and sewers must be designed with a debris catcher to permit either rapid clearing or removal of grating for cleaning when required.
 - i. If the inlet is outside the fence line, the debris catcher and grating will be incorporated into the same structure.
 - ii. If the outlet is outside the fence line, the debris catcher will be on the inlet side inside the fence line and the grating on the outlet side. A solution is shown in [Figure 3](#) (note that the removable grate is locked in place as an added security measure).

Figure 1: Steel Culvert Grill

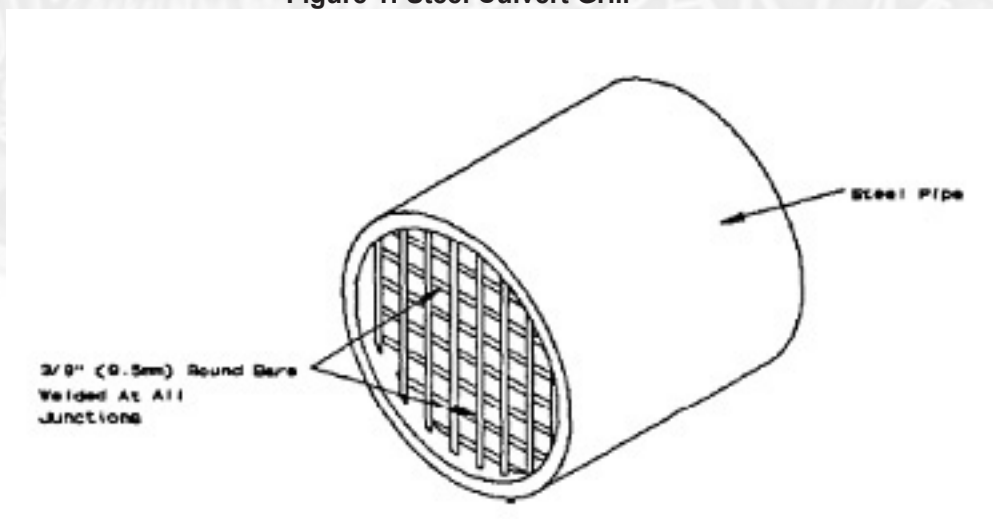


Figure 2: Concrete Culvert Grill

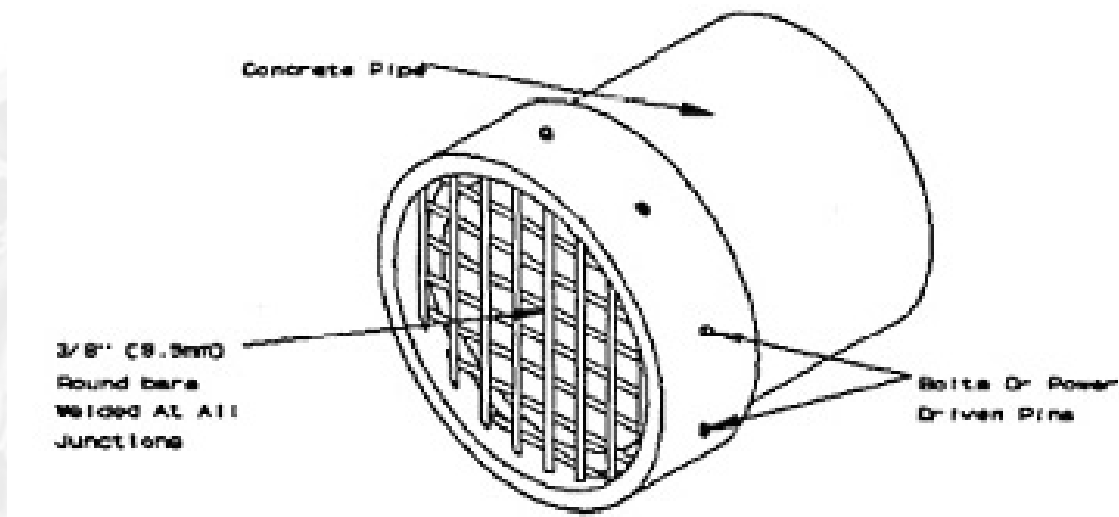
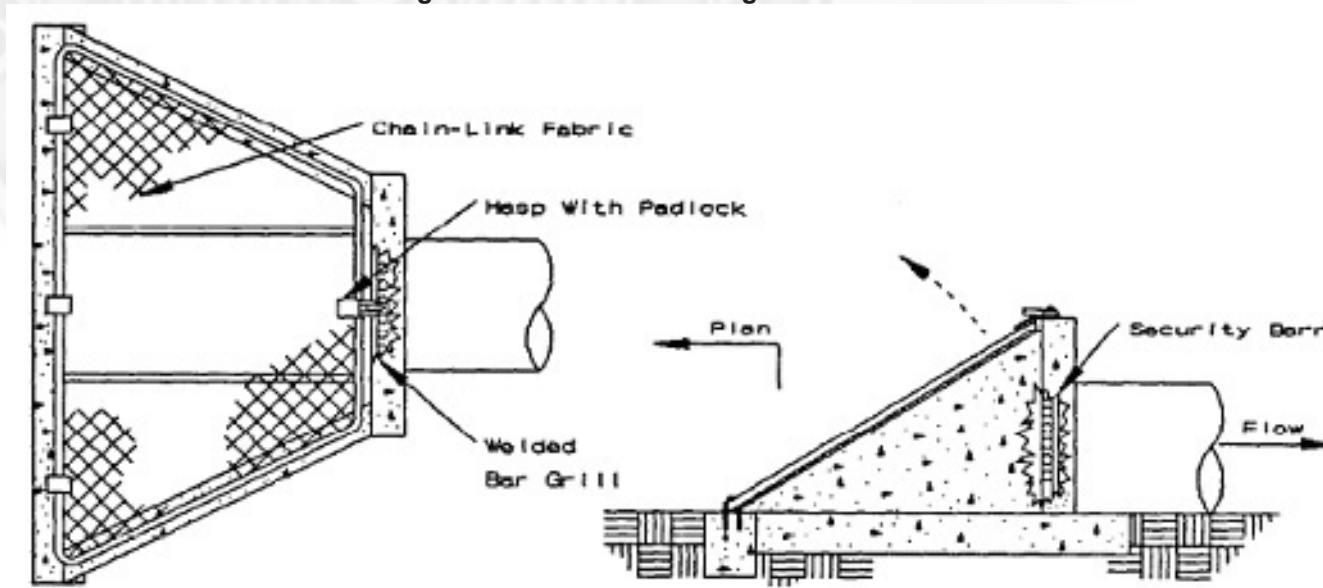


Figure 3: Removable Grating for Culverts



- Removable Grating for Culverts

As an alternative, drainage structures may be constructed of multiple pipes, each pipe having a diameter of 10 in.(254 mm) or less, joined to each other and to the drainage crossing. An economical solution to secure metal drainage structures is to weld short (approximately 6 in.(152.4 mm) long) multiple pipes, with diameters less than 10 in.(254 mm), in the “in-flow” end of the drainage culvert as shown in [Figure 4](#).

Figure 4: Large Culvert with Short Honeycomb Pipes

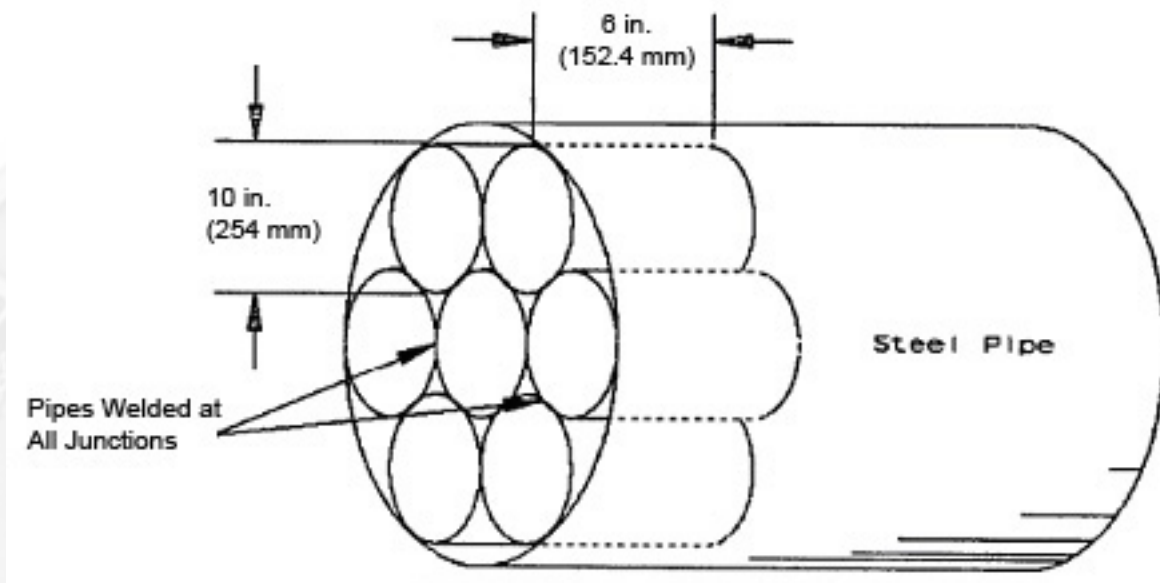


Figure 5: Swale Crossing with Ground Stakes

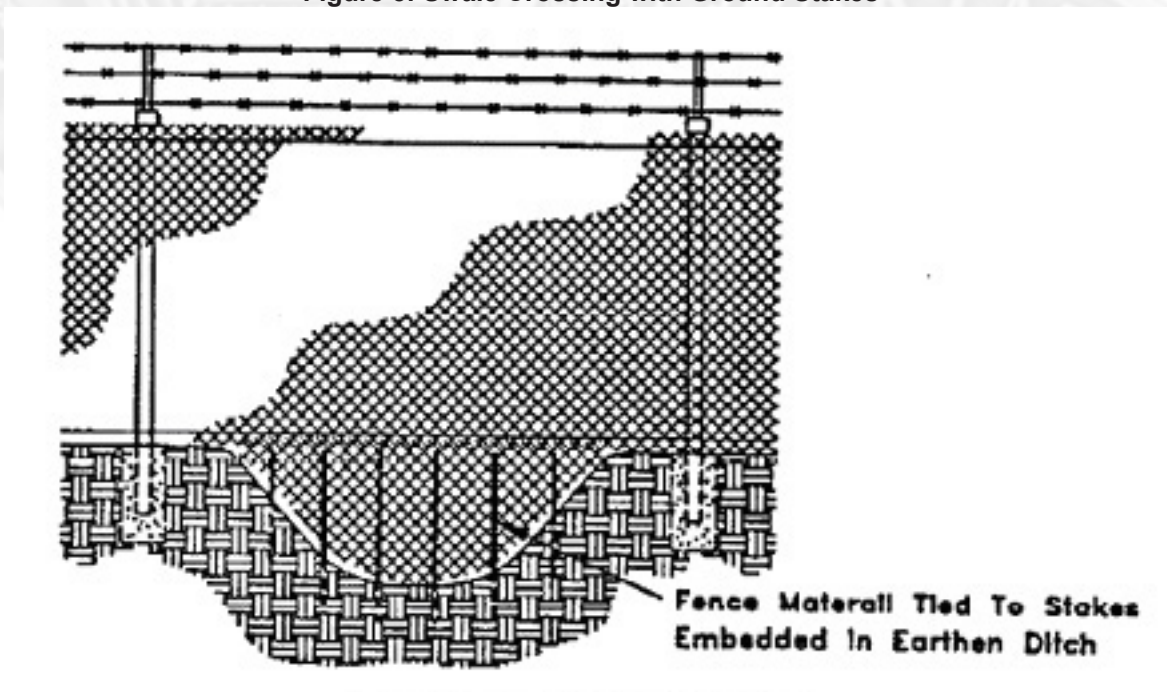


Figure 6: Swale Crossing Embedded in Concrete

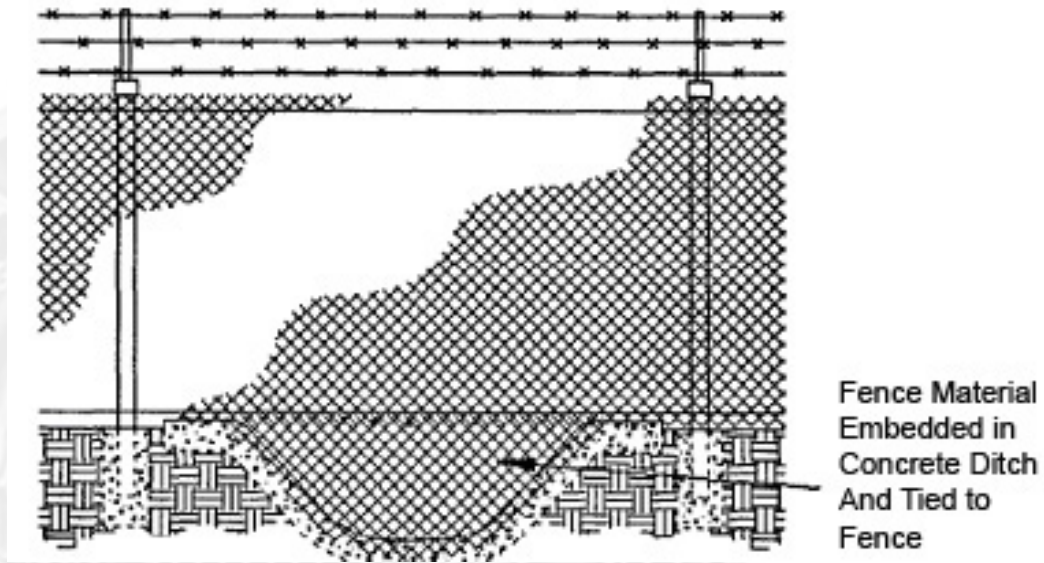


Figure 7: Bar Grill Embedded in Concrete

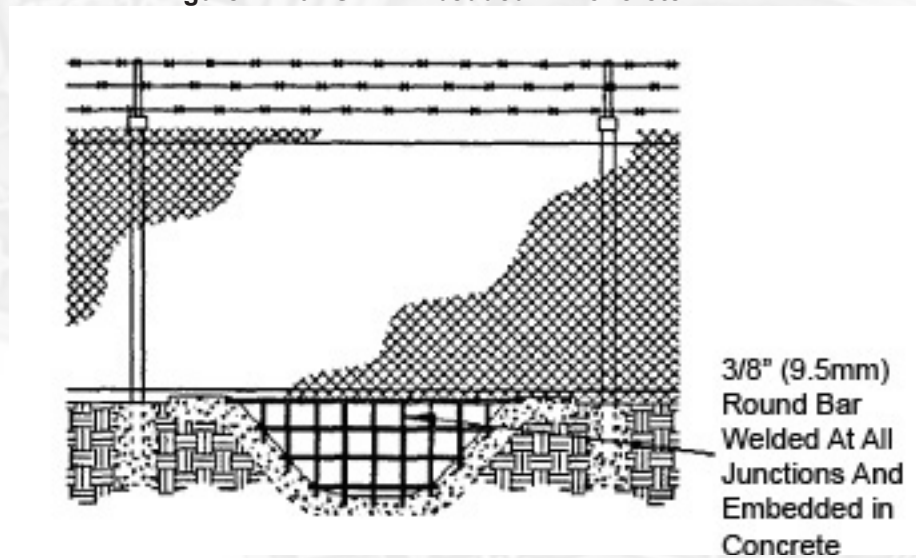
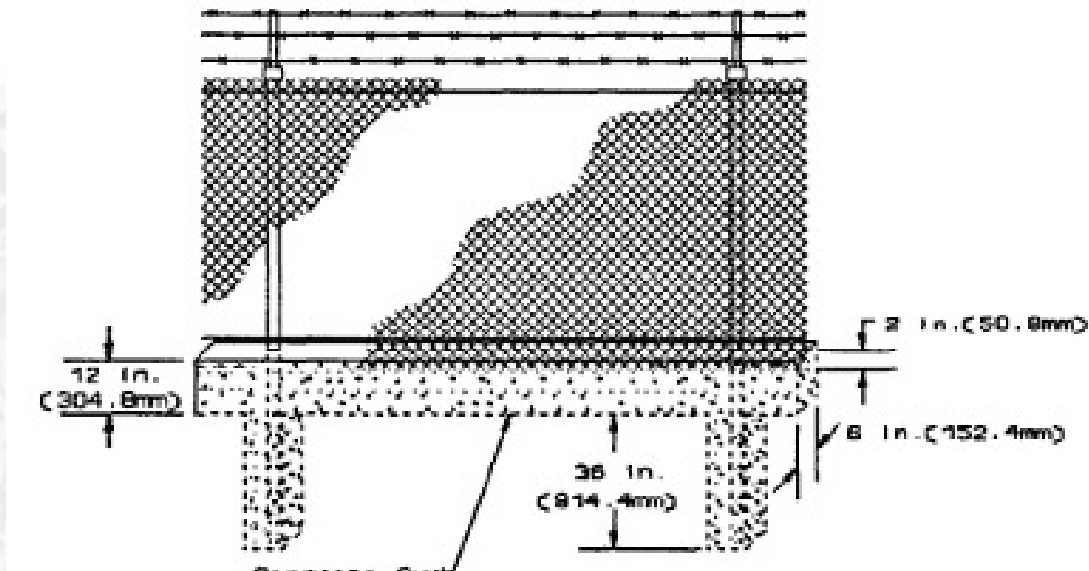


Figure 8: Chain link Fence Embedded in Concrete Sill



- Chain Link Fence Embedded in Concrete Sill (see [Figure 8](#)).
 - Special Requirements for Fences Equipped with Intrusion Detection Systems (IDS) Sensors:
 - IDS sensors are often placed on security fences and clear zones to detect aggressors attempting to gain access to an asset.
- Exterior sensors
 - Exterior sensors consist of four major types: beam, fence disturbance, seismic sensors, and video motion detectors. If exterior IDS sensors are to be included in the construction and installation of security fences coordination with CBP/IA/SMD is required.

D. Design

1. Posts and Bracing

- (a) Ensure all posts for security fencing meet the requirements of Federal Specification RR-F-191/3 for one of the following classes:
 - Class 1 - Steel pipe
 - Class 3 - Formed steel sections
 - Class 4 - Steel H-sections

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- Class 6 - Steel square sections

(b) Accomplish bracing with steel truss rods not less than 5/16-inch (7.9-millimeters (mm)) nominal diameter and a turnbuckle for tensioning, conforming to RR-F-191/4. Use the following ASTM Standards to supplement RR-F-191/3 and RRF-191/4:

- ASTM A 120, Specification for Pipe, Steel, Black and Hot-Dipped Zinc-Coated (Galvanized) Welded and Seamless, for Ordinary Uses.
- ASTM F 626, Standard Specification for Fence Fittings (particularly evaluation of corrosion resistance and material compatibility).
- ASTM F 669, Specification for Strength Requirements of Metal Posts and Rails for Industrial Chain link Fence.
- ASTM F 1083, Specification for Pipe, Steel, Hot-Dipped Zinc-Coated (Galvanized) Welded, for Fence Structures.

2. Chain Link Fence Fabric

(a) Ensure chain link fence fabric meets the requirements of RR-F-191/1 for one of the following:

- Type I - Zinc-coated steel.
- Type II - Aluminum-coated steel.
- Type IV - Polyvinyl Chloride (PVC) coated over zinc- or aluminum-coated steel.
- Perimeter fences will be fabricated with 9-gauge (3.9-mm) steel wire mesh material (before any coating) with mesh openings not larger than 2 inches (50.8 mm) per side.

Ensure that the fabric height is 7 feet (2.13 m) and has twisted and barbed selvage at the top and bottom.

(b) The designer may use the following ASTM Standards to supplement RR-F-191/1 for chain link fabric:

- ASTM A 116, Specification for Zinc-Coated (Galvanized) Steel Woven Wire Fence Fabric.
- ASTM A 392, Specification for Zinc-Coated Steel Chain link Fence Fabric.
- ASTM A 491, Specification for Aluminum-Coated Steel Chain link

[RETURN TO TOP](#)

Fence Fabric.

- ASTM A 817, Standard Specification for Metallic-Coated Steel Wire for Chain link Fence Fabric.
- ASTM F 668, Standard Specification for Poly Vinyl Chloride (PVC)-Coated Steel Chain link Fence Fabric.

E. Accessories:

Ensure accessories such as steel fittings and components used in the erection of chain link fences meet the requirements of RR-F-191/4. Use ASTM F 626 to supplement RR-F-191/4. Provide fittings electronically compatible with connecting fittings, components, and the fence fabric to inhibit corrosion.

II. INSTALLATION

A. Requirements

1. The design of security fencing, using the above specified components, will include the following provisions:

ASTM F567, Standard Practice for Installation of Chain link Fence, may be used as installation guidance to supplement RR-F-191/GEN.

2. Fence Placement:

Security fencing for restricted areas will consist of a single-line fence surrounding the restricted area. When specified by the CBP/IA/SMD, two single-line fences may be used to provide additional deterrence. The two fences shall be separated by a minimum of 30 ft. (9.1 m) and a maximum of not more than 150 ft. (45.7 m).

3. Posts, Top Rails, and Bracing:

- (a) Top rails will not be specified or allowed for fabrication of security fences. Required bracing for posts will be accomplished with diagonal truss rods and tubular horizontal or diagonal bracing.
- (b) All posts and structural supports will be located on the inner side of the fencing. Posts will be installed in concrete in accordance with ASTM F 567, as shown in [Figure 10](#). Posts must be vertical within plus or minus 2 degrees in two planes. Each gate, terminal, and end post will be braced with truss rods. Truss rods will be installed diagonally, from near ground level of a gate, terminal, or end post to the top of the adjacent line post, no higher than 6 in.(152.4 mm) down from the top of the fabric. There will be

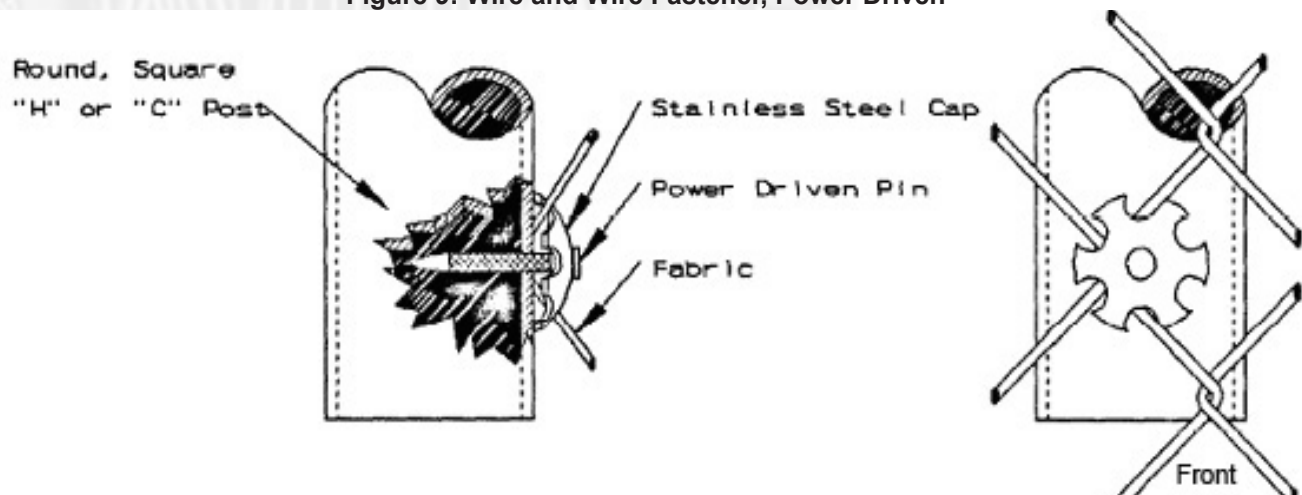
[RETURN TO TOP](#)

no more than a 50-degree angle between the truss rod and the ground.

4. Chain Link Fence Fabric Mounting:

Fence fabric will be mounted on steel posts. Tension wires will either be interwoven or clipped along the top and bottom row of fabric diamonds. The wire fabric will be secured to posts and tension wires as specified in RR-F-191/4. When a more secure manner of attaching the fabric to posts is desired, a power driven fabric and wire fastener, depicted in [Figure 9](#), may be used. If the ties or fasteners are coated or plated, the coating or plating must be electrically compatible with the fence fabric to inhibit corrosion. Where security fencing adjoins structures, the height of the fencing should be 12 ft. (3.7 m) high from the connection point with a building to a point 12'(3.7 m) away from the structure.

Figure 9: Wire and Wire Fastener, Power Driven



5. Anchoring/Fabric and Wire Fastener, Power Driven:

The bottom of the fabric will extend to within 2 inches (50.8 mm) of firm soil. In unstable or shifting soil such as sand, the fabric should either be buried to compensate for the shifting soil or a minimum of 2 inches (50.8 mm) of the bottom selvage of the fence anchored in concrete curbs, sills, hooked steel bars or similar types of anchoring devices extending below ground level as recommended by the soil engineer. (Frost levels should also be considered when placing curbs, sills, etc.) Even in unstable and shifting soil, the height of fabric and posts must be designed to assure that the top of the fence fabric will be maintained at 7 feet (2.1 m) above existing or anticipated ground level. This often may require that the fabric be 8 feet (2.4 m) or greater, so that sufficient material is buried below the surface or embedded in concrete sills.

[RETURN TO TOP](#)

6. Penetrations-Resistant Barriers:

Recent terrorist incidents involving the use of suicide-type crash entry forces the consideration of vehicle barriers capable of stopping large vehicles traveling at high speed. Crash tests of chain link fences, similar to the chain link fence required by this handbook, allowed full penetration with no personnel injuries of both a 1-1/2-ton (1360.7-kg) and 2-ton (1814.4-kg) vehicle traveling at 50 miles per hour (80.5 km per hour). An analysis of crash test data indicates that, unless enhanced by the addition of cables, fences offer little protection against penetration. Consequently, to meet a vehicle threat, fence reinforcement measures may be required to maintain security of a restricted area. Crash tests performed on a chain link fence reinforced with a 3/4-inch (19.1-mm) aircraft cable restricted penetration of a 2-ton (1814.4-kg) vehicle traveling at 50 mph (80.5 km/h) to 26 feet (7.9 m). When selecting barriers for penetration resistance, the designer should choose active or passive barriers based on their capacity to stop the threat vehicle at the maximum speed it could attain in its approach.

- Passive Barriers

Use passive barriers where unmovable barriers are needed, such as along a perimeter chain link fence.

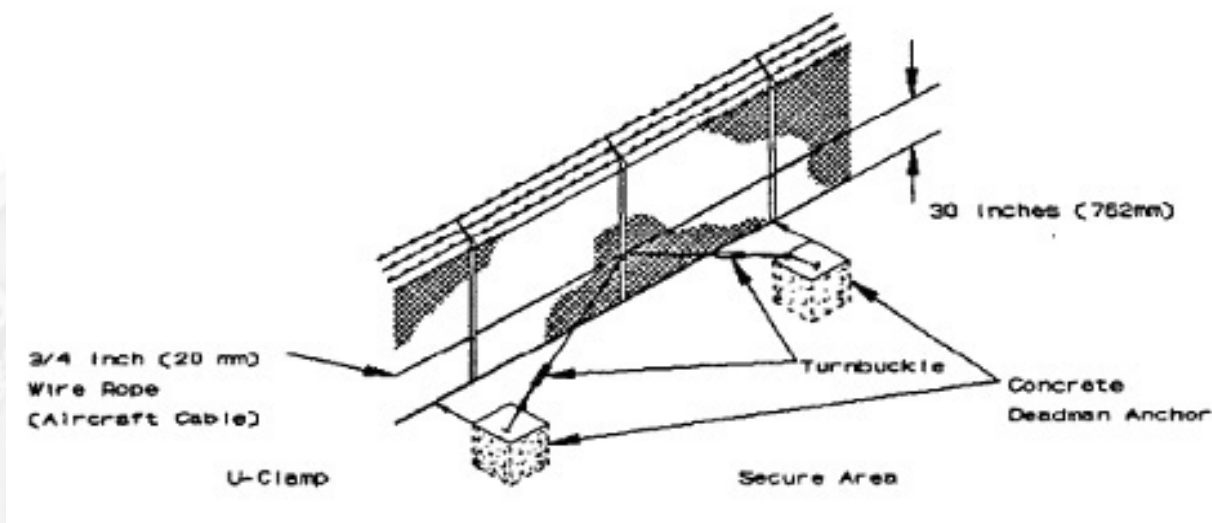
- Active Barriers

Use active barriers where vehicles must be allowed passage, but the capacity to stop them must also be maintained.

7. Reinforcement of Perimeter Chain link Fence:

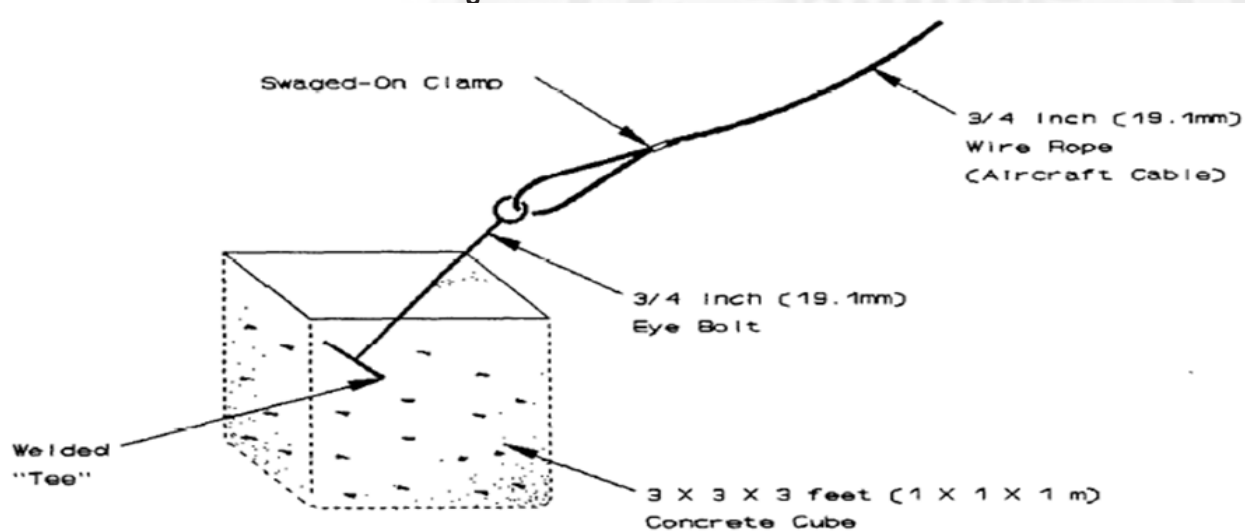
(a) A reasonable approach to reinforce a standard chain link perimeter fence to resist a vehicle attack is both simple and aesthetic. Place a 3/4-inch (19.1-mm) diameter aircraft cable, conforming to MIL-W-83420, along the fence line, between the fence posts and the chain link fabric as shown in [Figure 10](#).

Figure 10: Steel Cable-Reinforced Chain link Fence



(b) Fasten the cable with 1/2-inch (12.7-mm) U-clamps (SAE Grade 3 or better) at a height of approximately 30 inches (762 mm) from ground level. Terminate each cable end with either three wire rope clamps (MS16842) or a wire rope hydraulically swaged press fitting (MIL-P-80104). The cable end will be attached to one end of a 3/4-inch (19.1-mm) round turnbuckle (MS51561) with double eye ends which in turn will be attached to the deadman eyebolt (MIL-B-45908) by a 3/4-inch (19.1-mm) anchor shackle (SAE Grade 8 or ASTM A 490). The deadman anchor will be a concrete cube, Approximately 3-by-3-by-3 feet (1-by-1-by 1 m). Eyebolts captured in the deadman anchors will have either a welded “T” or “L” end embedded in the concrete as shown in [Figure 11](#).

Figure 11: Deadman Anchor



- (c) At a minimum, 2 feet (0.610 m) of the eyebolt and its welded extension will be captured within the concrete of the deadman. The shaft of the eyebolt will be either in-line with the attached cable or the eye of the eyebolt will be flush with the surface of the deadman.
- (d) Anchors shall be placed at a minimum of 200-foot (60.9-m) intervals and a maximum of 1,000-foot (304.8-m) intervals on the inside of the perimeter fence with the front edge of the deadman flush with the fence fabric.
- (e) The top of the deadman will be either flush or buried below the surface as long as the eye of the eyebolt is above ground level.
- (f) Cables must overlap as shown in [Figure 10](#) before terminating at a deadman so that no voids in the cable occur along the perimeter. If additional hardening is desired, a second cable should be placed about 5 inches (127 mm) above the first cable and attached as described above. It may be anchored to the same deadmen used by the first cable system.
- (g) When gates form a portion of the fence line being protected by a vehicle restraint cable system, then the gate cable system described in [Section III.E.2](#) must be interconnected to the fence cable system to ensure continuity of the cable system.
- (h) The vehicle restraint cable system should not be used along portions of the fence line that are otherwise protected by natural barriers, such as large boulders, trees, natural ravines, ditches, and other natural barriers.

III. GATES

A. General

1. Gates facilitate control of authorized traffic and its flow. They establish specific points of entrance and exit to an area defined by fences. They also function to limit or prohibit free flow of pedestrian or vehicular traffic, while establishing a traffic pattern for restricted areas. Gates, as a part of perimeter fences, must be as effective as their associated fence in order to provide an equivalent deterrent. Gates will normally require additional hardening features due to their location across entrance roads and the inherent vulnerability of their requirements.
2. The number of gates and perimeter entrances must be the minimum required for safe and efficient operation of the facility. Gates are protected by locks, intermittent guard patrols, fixed guard posts, contact alarms, CCTV, or a combination of these. Care must be afforded against the ability to crawl under gates and shall be adequately lighted. They shall be locked when not staffed and periodically inspected by a roving guard force. Utility openings in a fence that do not serve as gates should be locked, guarded, or otherwise protected. Top guard

[RETURN TO TOP](#)

is required and may be vertical where necessary.

B. Design

Materials used in fabricating and erecting chain link gates must be the same as the materials used for the associated chain link fence. As for security fences, aluminum pipe, poles, fabric, or accessories will not be used or specified for security gate components. Use American Society for Testing and Materials (ASTM) standards to supplement Federal specifications when further detail or criteria is desired.

C. Types of Gates

1. Federal Specification RR-F-191/2 is the basic criteria document for security fence gate design. It provides specifications for the following eight types of chain link fence gates:

- (a) Type I - Single Swing Gates.
- (b) Type II - Double Swing Gates.
- (c) Type III - Single Cantilever Sliding Gates, Wheel Sliding Gates.
- (d) Type IV - Double Cantilever Sliding Gates.
- (e) Type V - Single Overhead Sliding Gates.
- (f) Type VI - Double Overhead Sliding Gates.
- (g) Type VII - Vertical Lift Gates.
- (h) Type VIII - Special Gates.

2. The gate types listed above are the most common gate configurations used for perimeter fencing. These include single and double swing gates (Figures 12 and 13), single and double cantilevered gates ([Figures 14 and 15](#)), wheel-supported (V-groove) sliding gates ([Figure 16](#)), and single and double (bi-parting) overhead supported gates ([Figures 17 and 18](#)). While any of these may be used for pedestrian or vehicular traffic, generally single gates will be designed for pedestrian traffic and double gates for vehicular traffic.

Figure 12: Single Swing Gate

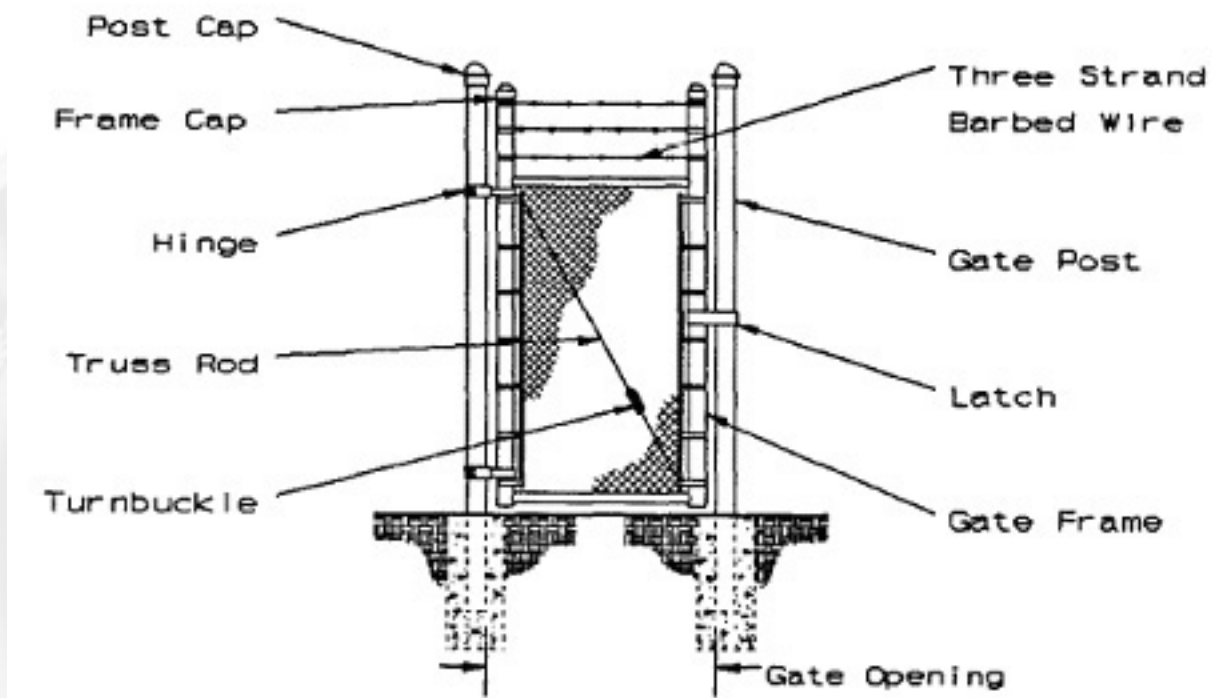


Figure 13: Double Swing Gate

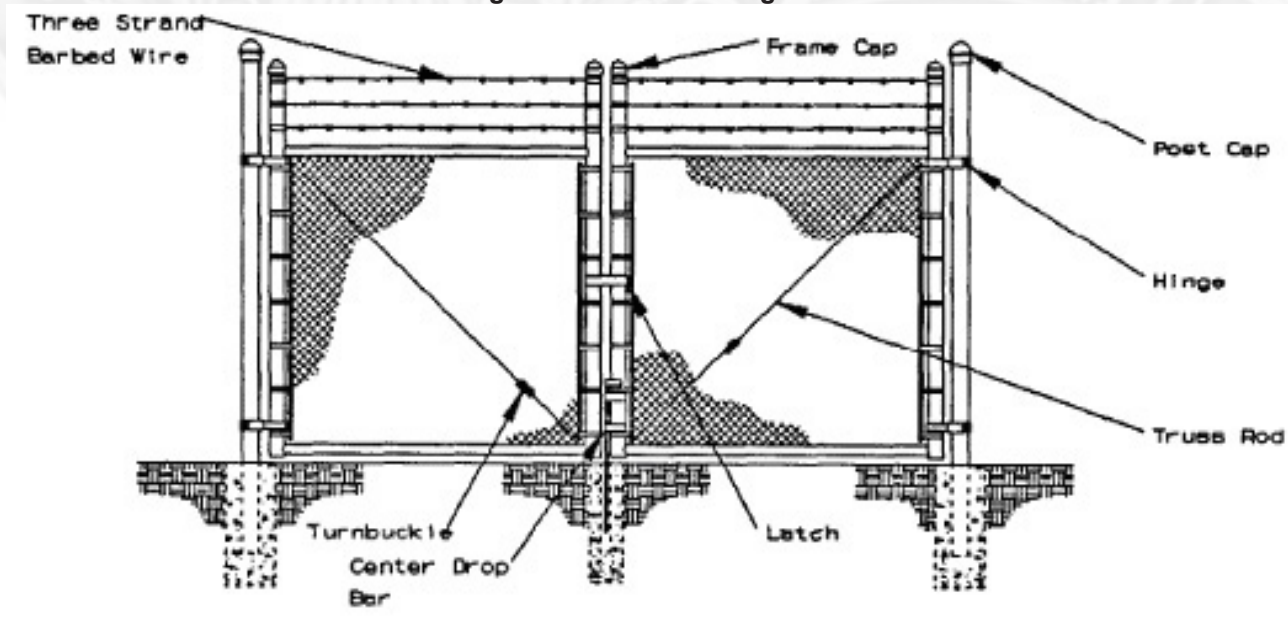


Figure 14: Single Cantilevered Gate

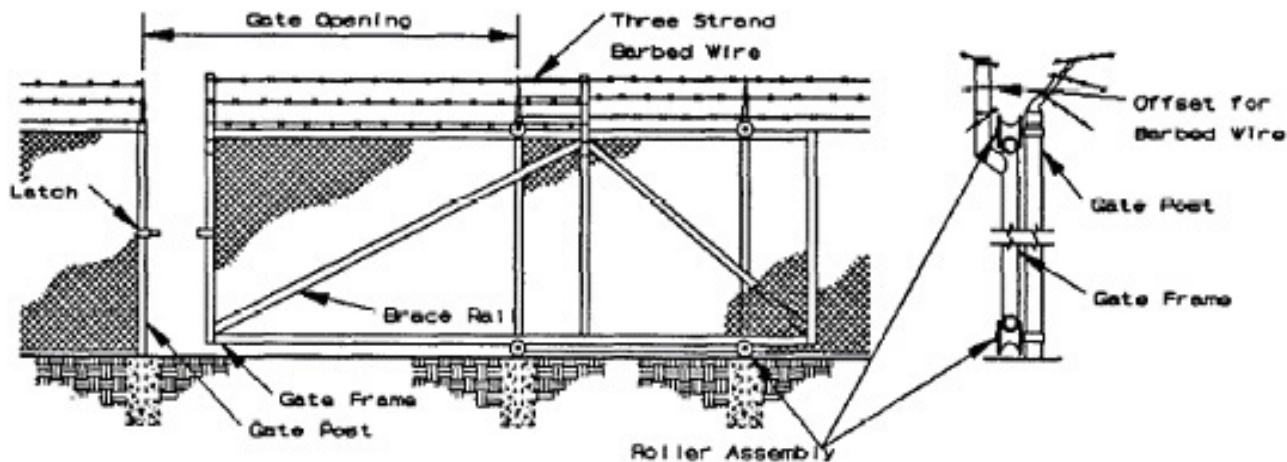


Figure 15: Double Cantilevered Gate

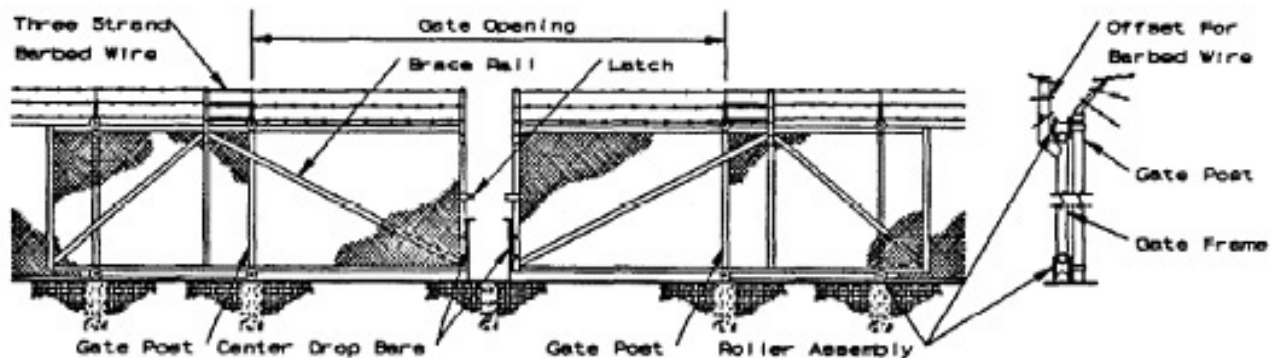


Figure 16: Single Wheel-Supported (V-Groove) Sliding Gate

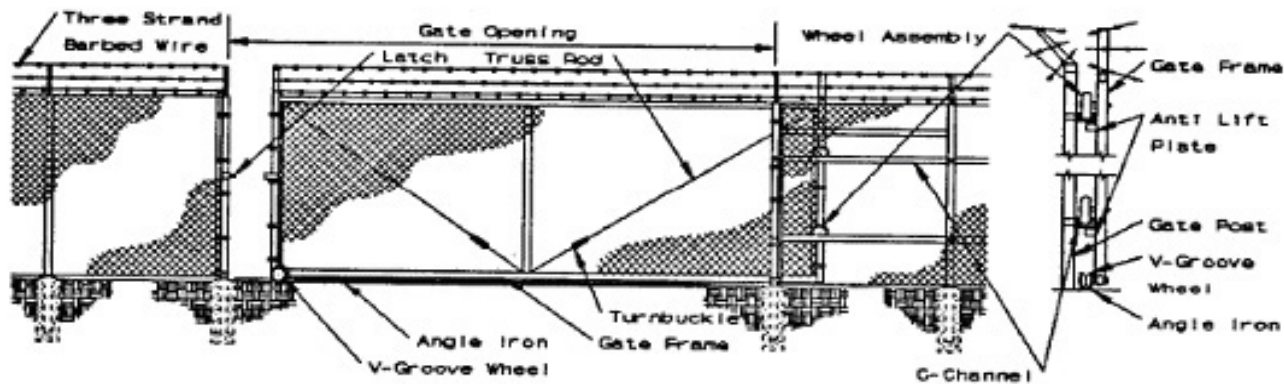


Figure 17: Single Overhead Supported Gate

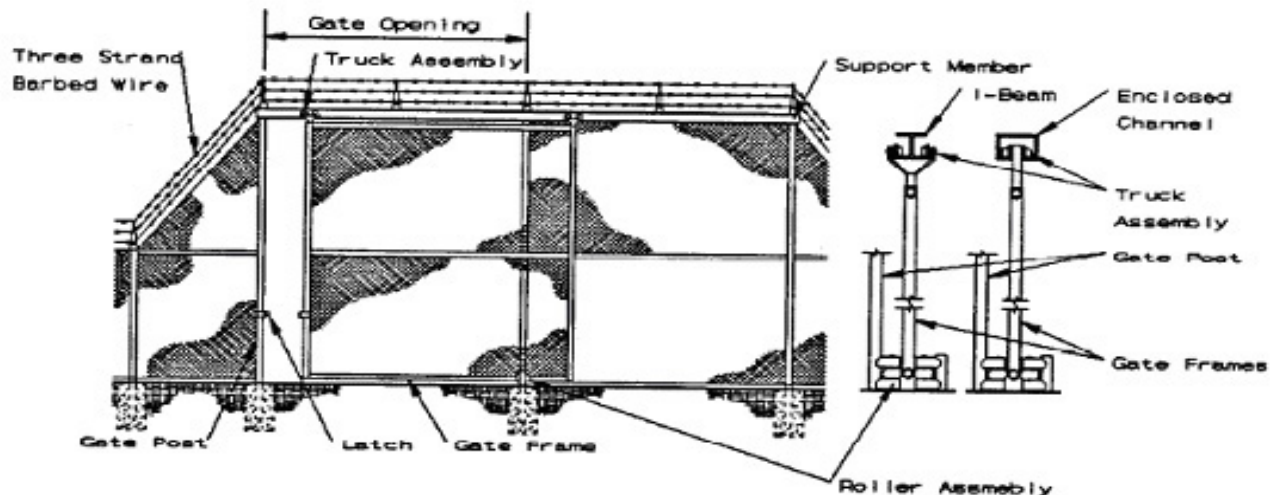
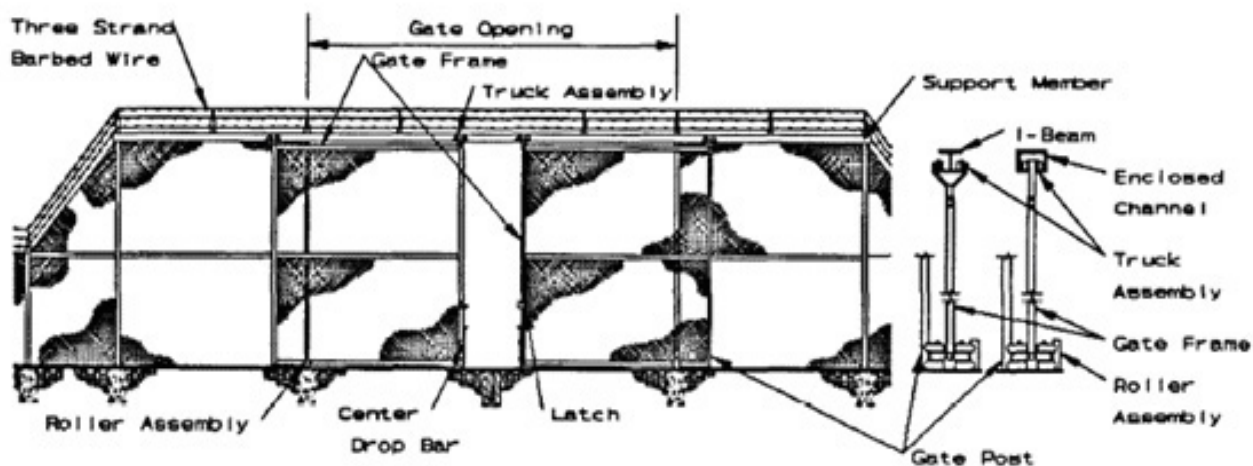
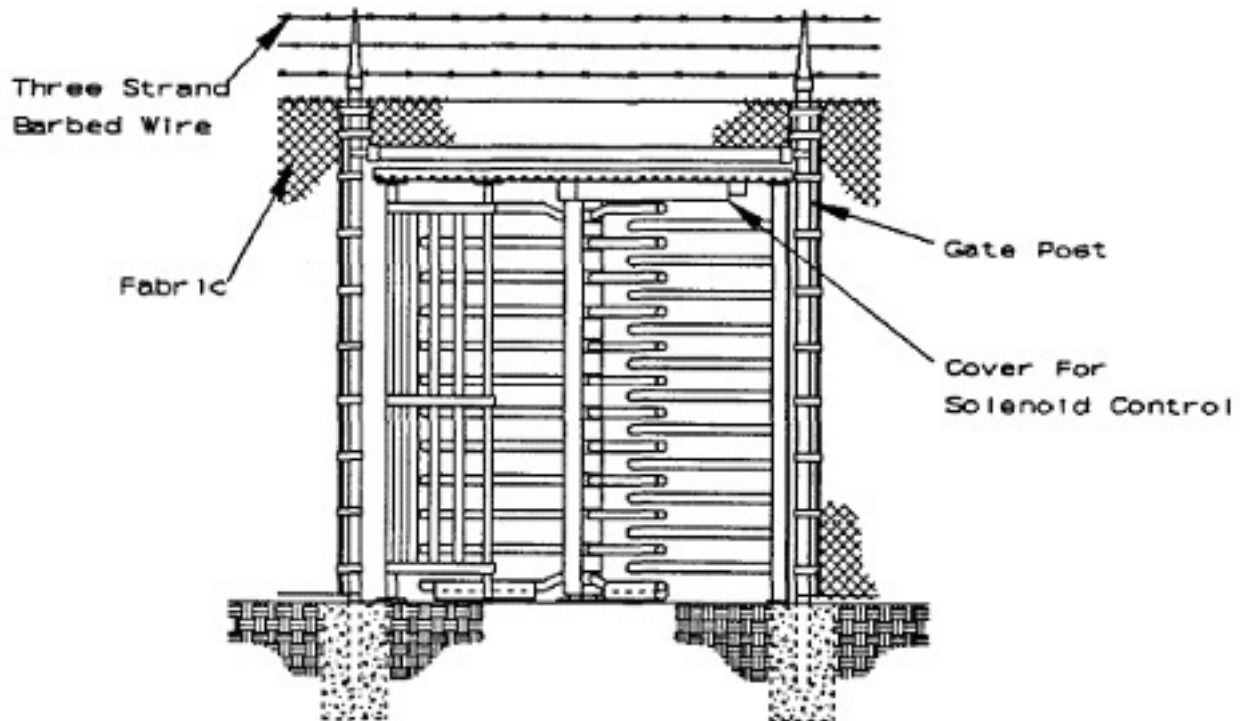


Figure 18: Double Overhead Supported (Biparting) Gate



3. The vertical lift gate (not shown), often referred to as a “guillotine” gate, is not desirable and should only be used under extremely unusual circumstances. Special gates, such as turnstile (rotational) gates ([Figure 19](#)), are designed either for specific purposes or to accommodate unusual circumstances.

Figure 19: Turnstile (Rotational) Gate



D. Gate Descriptions

1. Personnel Gates:

- (a) Where controlled access to a restricted area is required, turnstile gates are recommended for controlling pedestrian traffic, as shown in [Figure 19](#). Turnstile gates are also very helpful in relieving guard requirements for controlling personnel exiting a secured area since they can be set to revolve only in the exiting direction, thereby reducing the amount of guard supervision required.
- (b) Automated access control systems will use weather-proof readers with Dual Technology, Contact-less Smartcards, and Proximity or Long Range readers for vehicle gates. When automated access is desired, CBP/IA/SMD should be consulted for specific information concerning these access control systems. While turnstile gates provide security personnel with more positive access control and greater penetration resistance, swing gates are a second alternative when turnstile personnel gates are not practical. Swing type personnel gates may be more economical to procure and fabricate from a hardware aspect. However, both operational and guard personnel requirements should be considered to determine the most economical long-term cost for the facility.

[RETURN TO TOP](#)

2. Vehicle Gates:

Either wheel-supported or cantilever sliding gates are the best selection for vehicle security gates followed by overhead sliding gates. Swing gates are a third alternative and lastly, by far the least desirable, are overhead (“guillotine”) gates.

3. Sliding Gates:

Sliding gates, when open, store parallel to the adjacent fence line, unlike the large sweeping arc that swing gates require. When designing the roadbed at the gate opening, the surface should be kept as straight as possible, allowing for drainage by a slight incline to one side or the other of the entire roadbed. When an existing road surface is encountered that is not essentially flat, the designer should require asphalt or concrete fill to level the roadbed where the gate will be installed.

4. Cantilever Gates:

[Figures 14 and 15](#) Provide full support and suspension of the gate frame by four rollers secured to two posts inside the restricted area. Since the required length of a cantilever gate is 1-1/2 times the size of the opening, there must be a straight, and essentially level, fence line adjacent to the gate to accommodate this length when the gate is fully open. Cantilever gates can compensate for a somewhat crowned or unlevelled roadbed and do not require a “V”-bar guide rail or trough across the roadbed. Cantilever sliding gates are not recommended for openings exceeding 24 ft. (7.3 m), although two bi-parting sliding cantilever gates can be used for openings up to 48 ft. (14.6 m).

5. Wheel-Supported Gates:

[Figure 16](#), Single Wheel-Supported (V-Groove) Sliding Gate, requires either a guide rail (“V”-groove) or trough across the roadbed. With the “V”-groove design, the gate’s leading edge utilizes a wheel that has a deep groove cut into its outside circumference. This wheel travels on inverted angle iron that is secured across the roadbed on the ground. The rear of the gate travels with two wheels riding in “C” channels as shown in [Figure 16](#). The trough design utilizes a metal wheel with a convex diameter that rides down in a groove extending across the roadbed. While the trough provides a smoother surface for vehicular traffic, it is not recommended due to typical debris buildup in the groove causing the wheel to ride up out of the groove onto the roadbed surface. In both styles, the upper portion of the gate is supported laterally by additional vertical rollers. Since wheel-supported gates are not cantilevered, they only need to be somewhat longer than the actual size of the gate opening, requiring one-third less straight and level storage length along the

[RETURN TO TOP](#)

fence line than the cantilever gate. Wheel-supported gates essentially are not limited in the size of their opening except for the power requirements of the gate operator. A variation of the wheel-supported gate is one using dual pneumatic, hard rubber, or steel wheels to support the gate. These can be identified by their lack of roadbed guides. They should only be used as a last resort, and then only for manually opened sliding gates.

6. Overhead Gates:

Overhead gate design requires either an I-beam or an enclosed track, as shown in [Figures 17 and 18](#), suspended over the width of the opening and extending equidistant on one side or the other of the gate opening to store the gate when it is opened. Similar to wheel-supported and cantilever gates, the gate must store parallel to the adjacent fence line. The gate storage area must be in line with the gate opening and either be level or have a decreasing grade to accommodate the gate when it is fully open. The gate is suspended from the I-beam or enclosed track by a pair of rollers attached to posts extending upward from the leading and trailing edge of the gate. The overhead beam or track height must allow clearance for anticipated truck or rail traffic. The gate will be suspended above the ground from the overhead beam or track and supported laterally near the ground by vertical rollers. The enclosed track design incorporates the best of the overhead gate designs, and is well suited for automatic operators. The tracking system provides the convenience of a wheel-supported or cantilever-type installation, but with a much more efficient means to roll the gate. The amount of force to operate gates with these designs is significantly less than that of comparable gates. High-cycle demands, large opening sizes, or heavy gate construction may require strengthening the overhead I-beam design. Additional upright posts extending upward from the center of the gate will also allow the enclosed track to carry heavier loads.

7. Swing Gates:

Swing gates ([Figures 12 and 13](#)) should be designed so that they swing inward, toward the secured area. The disadvantage of the swing gate is the large arc of space required for operation. Swing gates can either be designed to swing 90 degrees inward and 90 degrees outward or swing 180 degrees inward only. An important consideration in selecting a single or double swing gate design is maintaining clearance along the bottom of the gate as it swings through its arc from the closed to the open position. If the grade is increasing inside of the gate, grading will be required to allow clearance. The required 2-inch (50.8-mm) maximum clearance between the bottom of the fence and the roadbed must be maintained when the gate is in the closed position. The swing gate design places considerable weight on the hinge post and its foundation. The longer the gate, the more load (movement arm) placed on the gate post. ASTM F 900 provides design detail for single swing gates up to 24 ft. (7.3 m).

[RETURN TO TOP](#)

Ideally, single swing gates should not exceed 14 ft. (4.3 m) and double swing gates should not exceed 28 ft. (8.5 m). Since the weight of the gate must be borne by the gate post, design of the gate post and its foundation is critical to assure proper support of the swing gate. An undersized or improperly installed gate post may shift and cause the gate to move out of plumb with the ground. This may cause the gate to drag on the ground or change elevation as the gate moves through its arc from the opened to closed position. The [fence cut sheets](#) at the end of this chapter provides recommended concrete foundation diameters for posts. At a minimum for swing gate posts, the concrete foundation should be 3 ft. (1 m) deep.

8. Vertical Lift Gates:

Vertical lift (“guillotine”) gates should only be used when the gate location is mandated, the site is so restricted, or the weather is so severe that a gate must be placed in such a location where the only way to open it is upward. Vertical lift gates should never be considered except as a last possible design choice. When a vertical lift gate is required, a counterweight with a continuous drive chain on each side (that pulls the gate both up and down) must be specified.

9. Hinges:

The weight, size, and frequency of use are important factors in the selection of gate hinges. Specific design guidance is not contained in the this specification or associated ASTMs. Gate hinges must have adequate strength to support the gate and have large bearing surfaces for clamping them into position. Commercial hinges manufactured to fit increasing diameters of gate posts also have increased mass and capability to support larger swing gates and generally have been found acceptable. The hinges must be secured to the gate post and the gate frame to assure they will not twist or turn under the weight and action of the gate. Welding is recommended. Gate hardware must conform to RR-F-191/2. ASTM F 900. Hinges must be made tamper-proof by the addition of welded security plates or by reversing the direction of the hinge pins (one up, the other down), thereby protecting the gate from being lifted off. Bolts and other hardware associated with gate hinges must be welded or peened (whenever possible on the inside) to prevent their removal by hand tools.

10. Reinforcement of Swing Gates:

The locking mechanism and the hinges on a security swing gate are the weakest components of the gate system. These areas can be reinforced by combining chain and wire rope (cable) to form a barrier across the opening. Once the chain and wire rope has been installed as shown in [Figure 22](#), the energy of a vehicle crash attempt is transferred from the gate through wire

[RETURN TO TOP](#)

rope links to the side gate posts, and further to the fence cable reinforcement system and deadman concrete anchors. The fence reinforcement cable is terminated with a swaged loop around the gate post to interconnect with the gate cable barrier system. With the wire ropes linked together at the fence posts as shown in [Figure 23](#) and chained together at their point of closure as shown in [Figure 24](#), in effect there is a continuous barrier across the opening. The system is simple, unobtrusive, and effective. When the chain is removed, gates can be operated normally without restriction.

Figure 20: Chain and Wire Rope Reinforced Gate

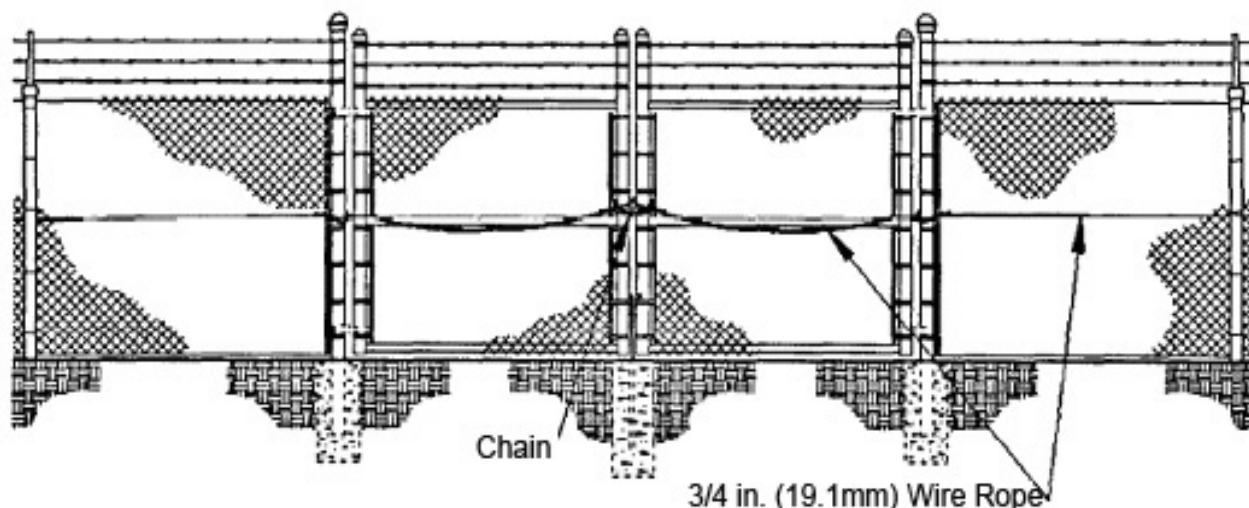


Figure 21: Wire Rope Interwoven at Gate Post

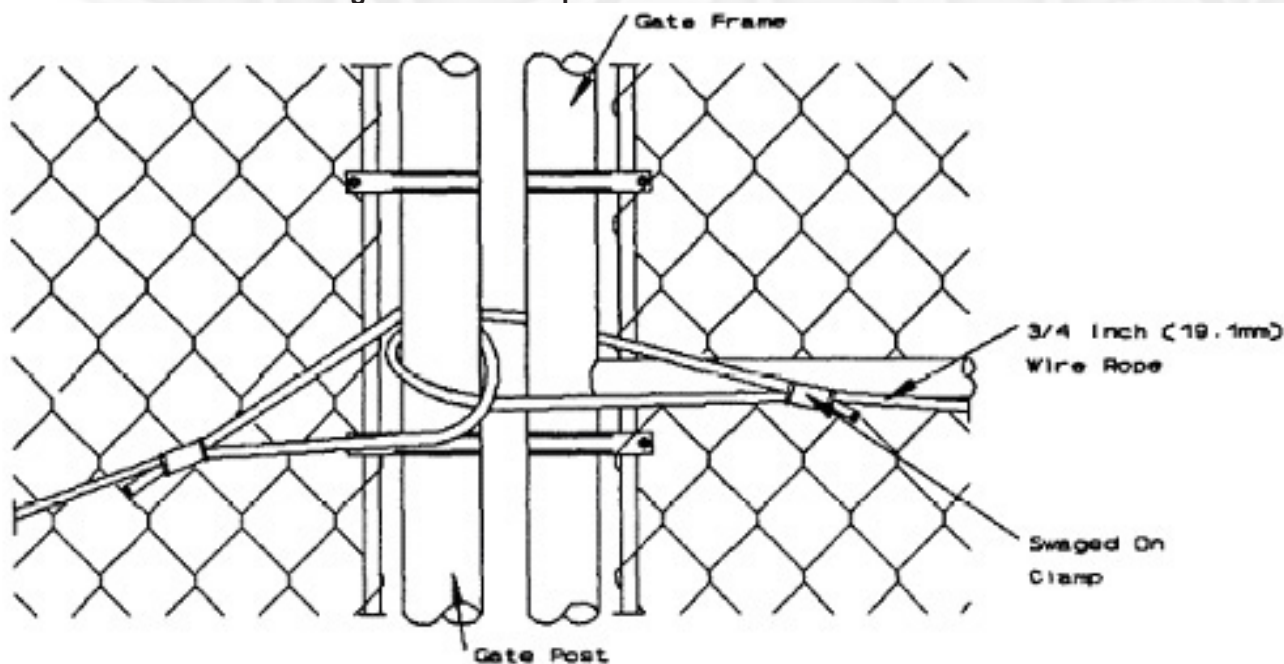
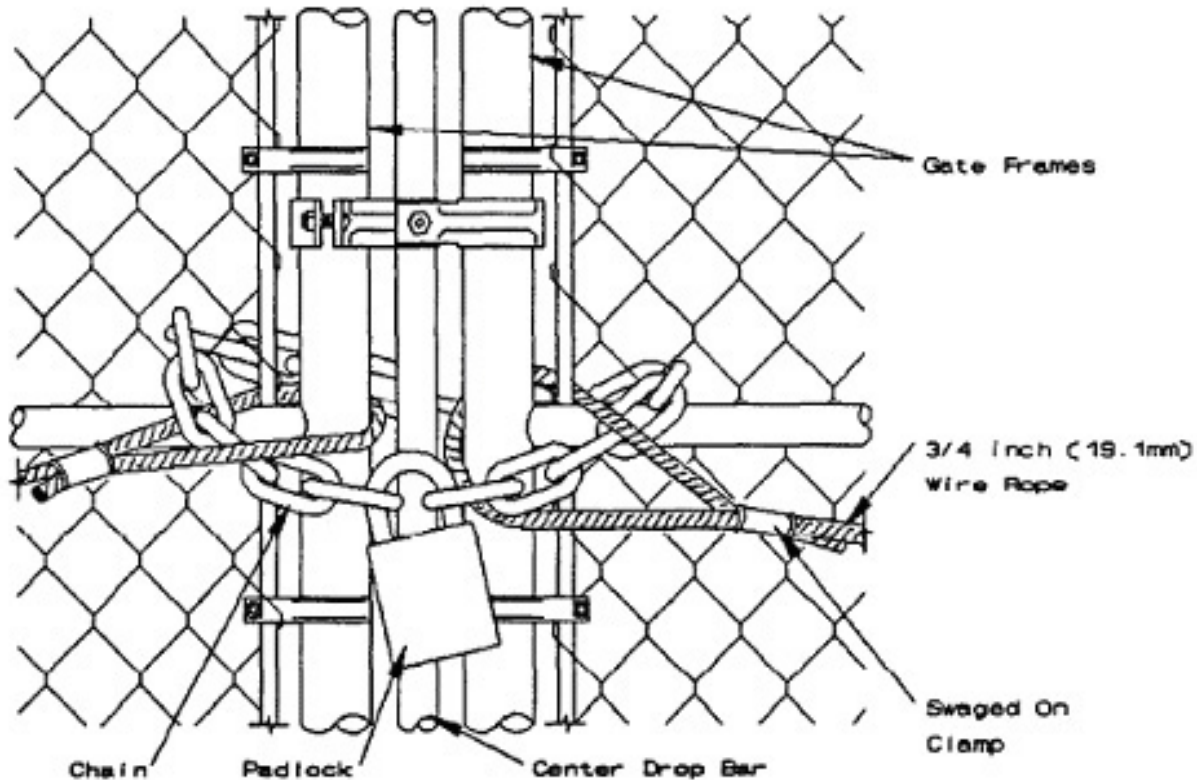


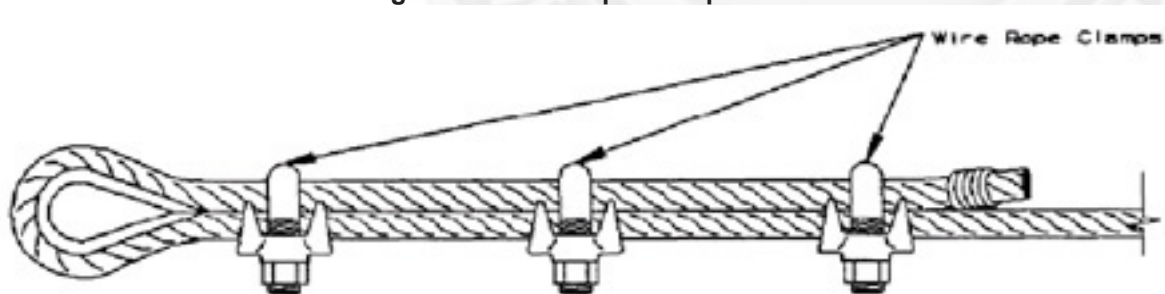
Figure 22: Chain and Wire Rope Locking System



E. Chain and Wire Rope Reinforced Gate

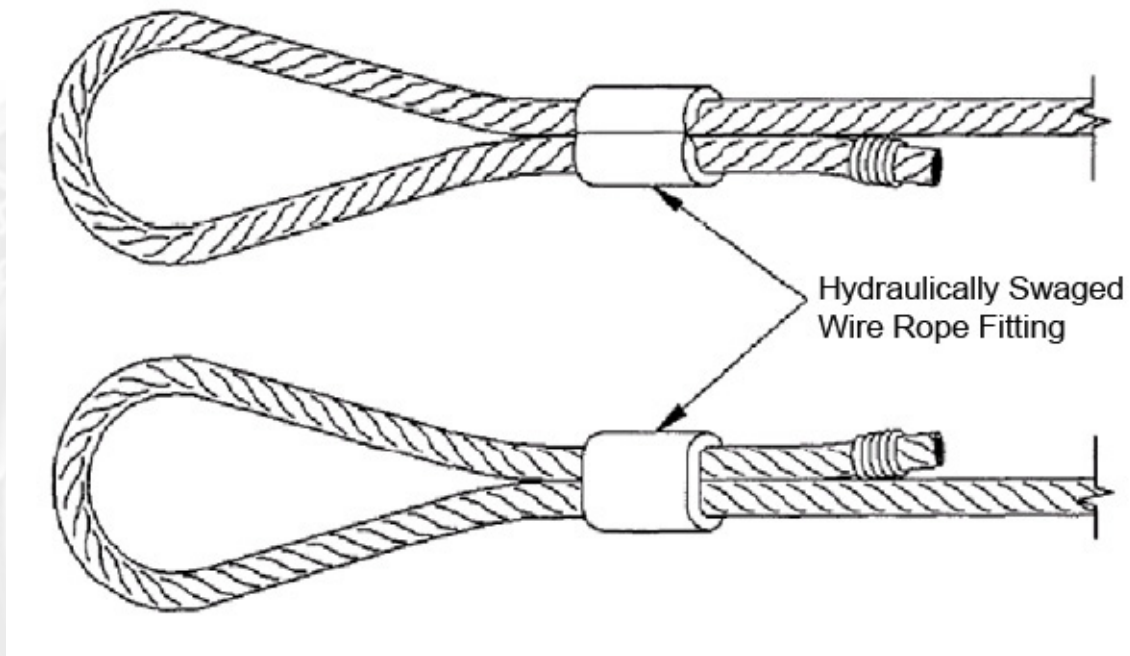
1. To construct the gate barrier system, a 3/4-inch (19.1-mm) diameter aircraft wire rope is looped around the gate post as shown in [Figure 21](#), around the gate frame upright, and through the fence cable loop. The wire rope is strung across the inside of the gate leaf and fastened around the vertical gate frame upright and fabric tension bar midway above the roadbed as shown in [Figure 20](#). Where gates have two leaves involved, a cable will be installed in the same manner on the second leaf. All cable ends are looped and terminated with either three wire rope clamps (MS16842) as shown in [Figure 23](#) or hydraulically swaged wire rope fittings (MIL-P-80104) as shown in [Figure 24](#).

Figure 23: Wire Rope Clamps

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Figure 24: Hydraulically Swaged Wire Rope Fitting



2. The critical component of the gate reinforcement system is the chain used to fasten the gates together. When the gates are closed, a 1/2-inch (12.7-mm) diameter welded steel alloy chain conforming to [RR-C-271](#) (Table 2, Type 1, Grade C, Class 1), is passed through each of the wire rope loops at the opening and around the two upright gate posts, then snugly fastened together with a Security Padlock as shown in [Figure 22](#). There are times when a gate reinforcement cable barrier system is desired but a cable reinforcement system for the adjoining fence is not necessary since terrain, natural barriers, structures, or other passive barrier features provide vehicle crash protection adjacent to the gate. In such cases, the gate cable system can be terminated directly on each side of the gate with deadman concrete anchors described for the vehicle restraint cable system above.

F. Reinforcement of Sliding and Vertical Lift Gates

1. While there is no “generic” or standard design method for hardening configurations of sliding and vertical lift gates, solutions for hardening various reinforcement materials used for swing gates above may be used effectively by the designer to reinforce either sliding or vertical lift gates. For example, a 3/4-inch (19.1-mm) wire rope (cable) (MIL-W-83420) could be attached along the length of a sliding gate as shown in [Figure 25](#) or a vertical lift gate as shown in [Figure 26](#). The cable ends are then looped securely around the gate frame uprights at each end as shown in [Figure 27](#). The end of the fence reinforcement cable system should be looped around the terminal posts on each side of the gate opening as shown for gate posts for swing gates in [Figure 22](#). A 1/2-inch

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

(12.7-mm) diameter welded steel alloy chain conforming to [RR-C-271](#) (Table 2, Type 1, Grade C, Class 1), can then be passed around the fence terminal post and the gate frame upright, passing through both the fence and gate cable loops as shown in Figures 29 and 30. Again, all cable ends are looped and terminated with either three wire rope clamps (MS16842) as shown in [Figure 25](#) or hydraulically swaged wire rope fittings (MIL-P-80104) as shown in [Figure 26](#). A security padlock is used to snugly fasten the chain together as shown in [Figures 29 and 30](#).

Figure 25: Cable Reinforcement for a Sliding Gate

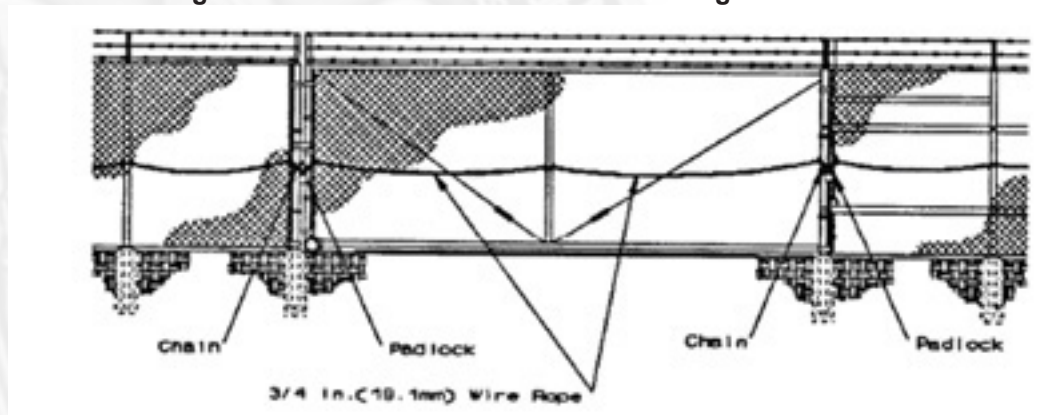


Figure 26: Cable Reinforcement of a Vertical Lift Gate

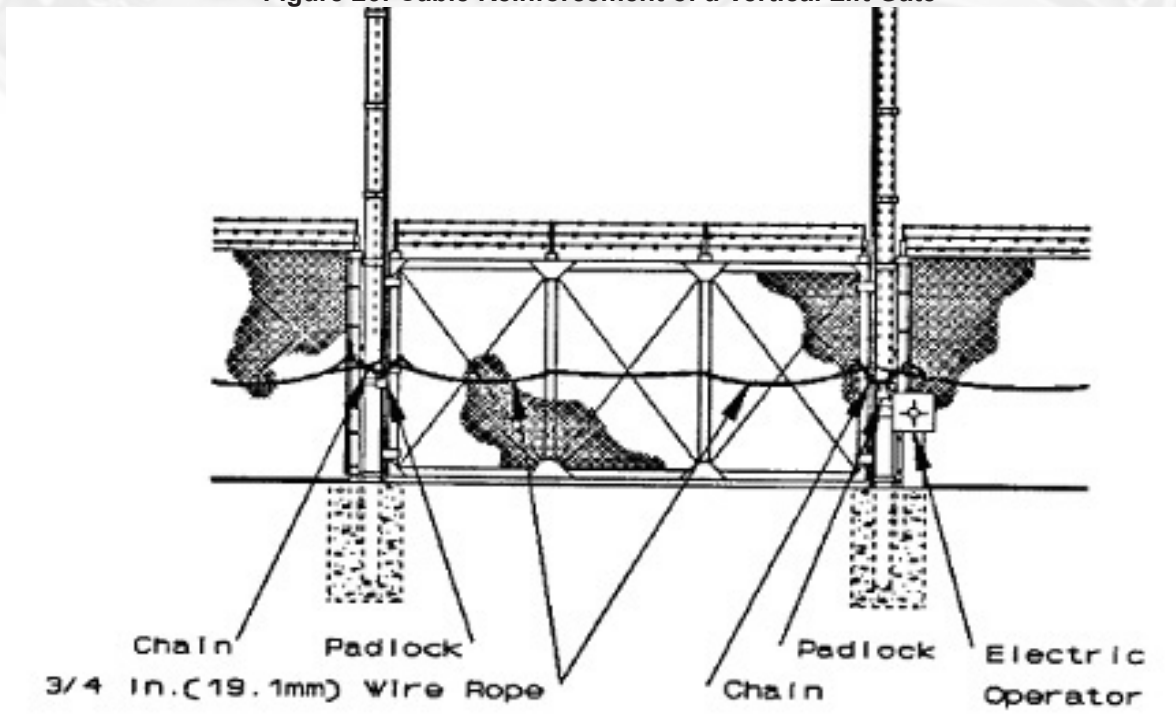


Figure 27: Chain and Wire Rope Reinforcing Sliding Gate

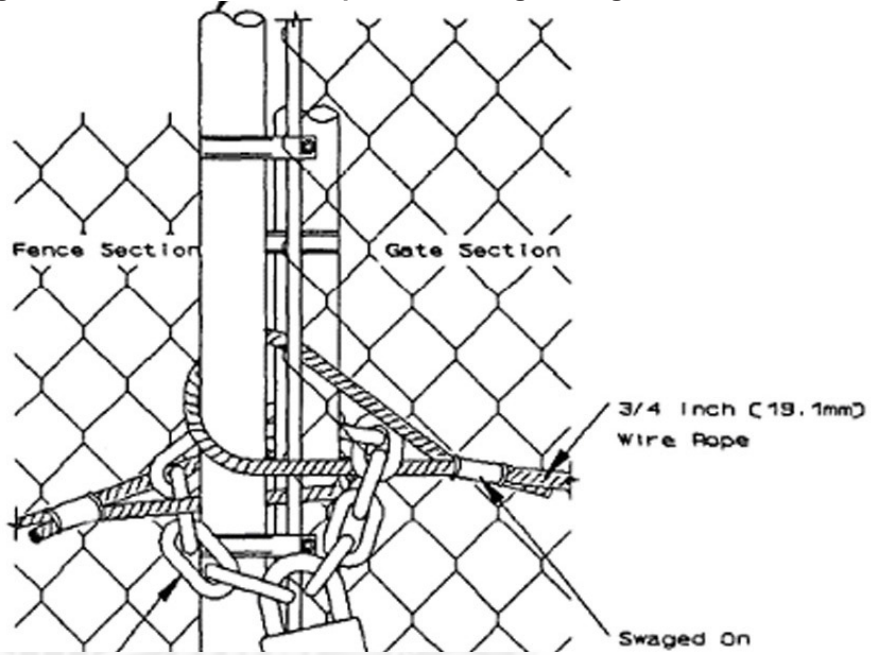


Figure 28: Chain and Wire Rope Reinforcing Sliding Gate

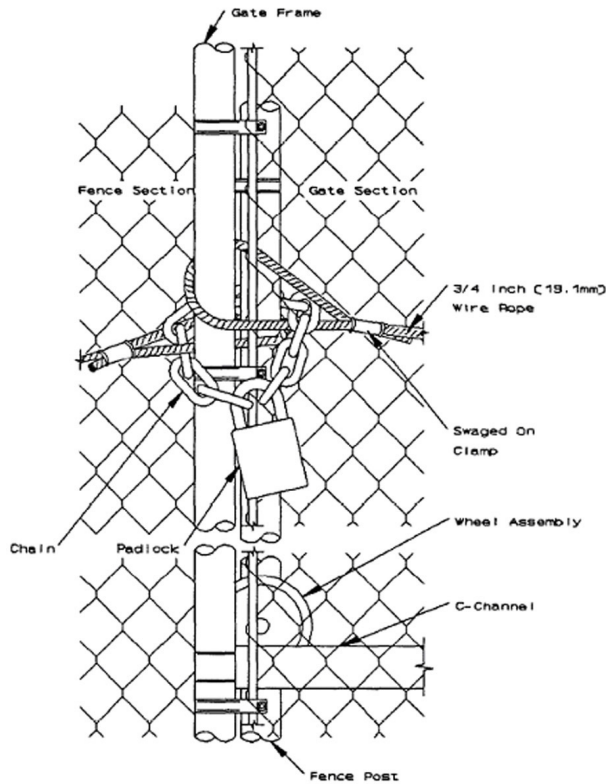


Figure 29: Chain and Wire Roping Reinforcing Vertical Lift Gate

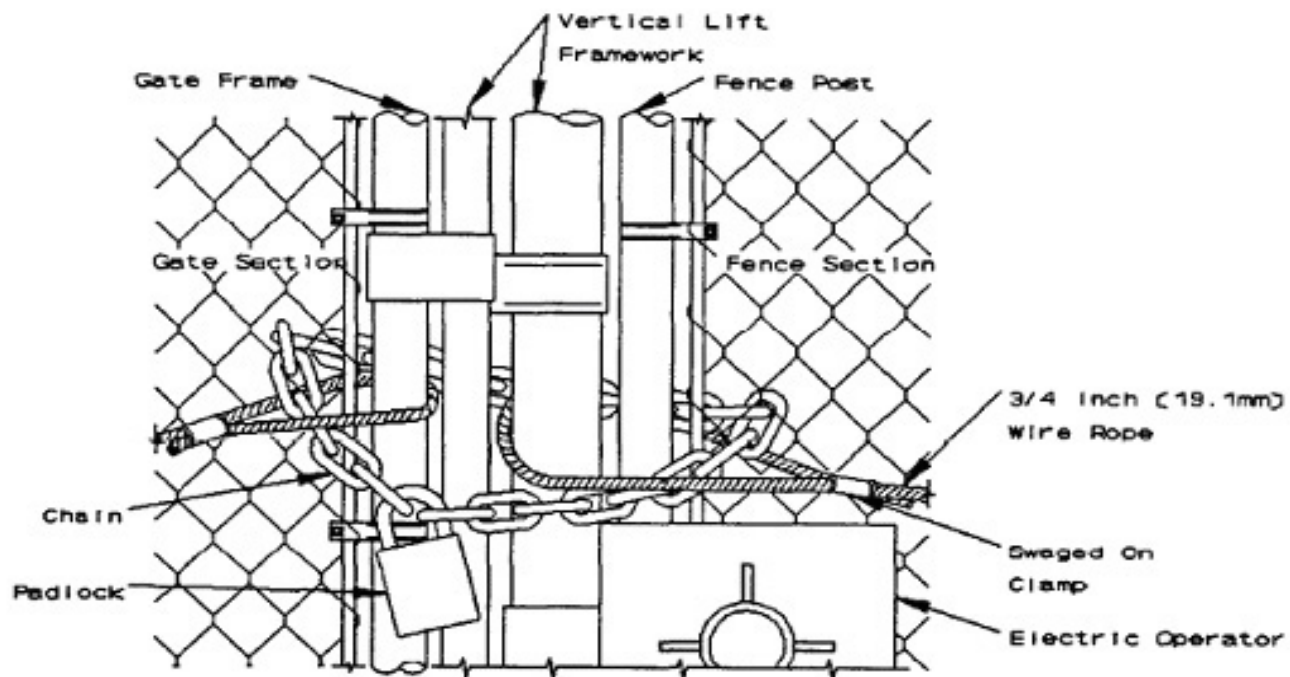
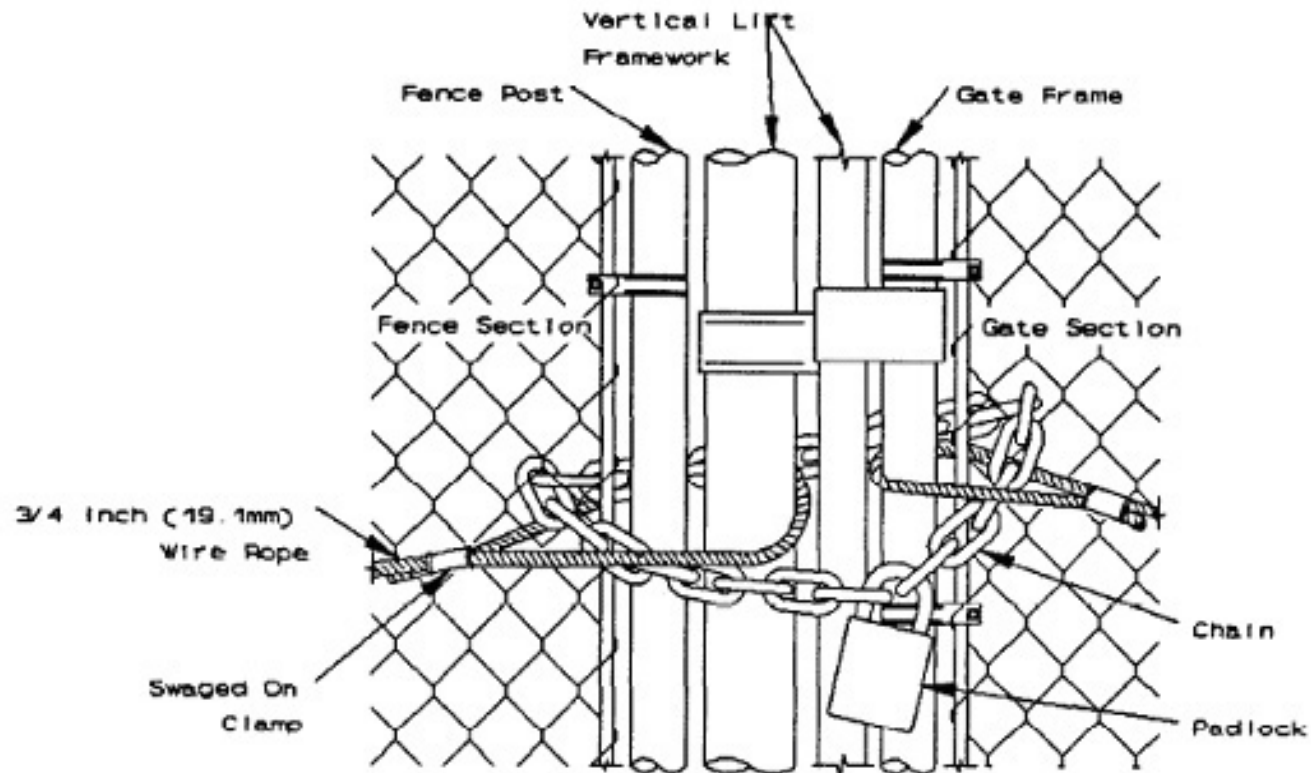


Figure 30: Chain and Wire Roping Reinforcing Vertical Lift Gate, cont'd



G. Locking System

1. Gates will be provided with locking hardware conforming to [RR-F-191/2](#). The locking system is designed to provide an equal level of penetration resistance when a gate is closed and locked. Where locking hardware is not practicable, 1/2-inch (12.7-mm) case hardened chains meeting the requirements of [RR-C-271](#) (Table 2, Type 1, Grade C, Class 1) will be used with a padlock meeting the requirements of Federal Specification FF-P-2927A. See [Appendix 7.6: Doors and Door Hardware](#) for more information. Vehicle entry sally-port(s), personnel swing gates, and turnstiles, each with its associated gate latching system(s), will be designed in accordance with the associated design guide. All pedestrian and vehicle gates incorporate an automatic electrical latching feature when closed. The remotely controlled gates are operated from a central location. An emergency override will be provided to allow both gates to be opened simultaneously for emergency vehicles.
2. Many power operators for sliding gates are designed to “lock-up” the gate motion by means of an internal friction brake system that engages when the operator is stopped. This type of locking device is not adequate to secure the gate when it is not manned by security personnel; therefore, one of the locking or latching methods discussed above must be provided.

H. Gate Power-Operators

1. As noted above, gate power-operators with automatic latching (locking) systems are required for vehicular gates and must be operated by the Command Center. With the requirements of access control becoming more sophisticated and involved, the use of power-operators for gates at other types of restricted areas is more compelling for active vehicular security gate operation. The designer should analyze the facility access control procedures and anticipated traffic flow through each proposed vehicular gate.
2. From this analysis, the potential effectiveness of a power-operator in improving access control operations for gates can be evaluated. When vertical lift gates are designed, gate power-operators are mandatory except in rare circumstances when the gate will seldom be used and manual operation of the gate is reasonable.
3. Gate power-operator controls must be located so they cannot be reached or tampered with from outside the security fence. Most gates will require site-specific operating accessories, warning devices, or safety systems in addition to the actual operator. Gate power-operators shall be connected to emergency power and must work manually in case of power failure. The designer should coordinate the design of gate power-operators with CBP/IA/SMD.

I. Gate Power-Operator Design

1. A manufacturer's design (using similar components), the standard features provided, and optional accessories available are what primarily separate one manufacturer's products from another. Some manufacturers provide a full line of power-operators for gates in all horsepower, voltages, and phases, while others limit selection to one or two models which may provide inadequate horsepower and improper voltages for the gate being designed. Gate power-operator capabilities are of particular concern when cantilever gates are installed, particularly when the grade increases from side to side of the opening.

J. Sliding Gate Power-Operators

1. Power-operators for sliding gates are generally associated in three groups based upon their method of operation:
 - (a) Electromechanical Chain Driven - An electric motor drives a series of reduction and worm gears, chains, and sprockets which in turn drive a chain attached to the gate thereby operating the gate.
 - (b) Electromechanical Rack and Pinion - An electric motor, through gear reduction, operates a rack and pinion gear arrangement attached to the gate thereby operating the gate.
 - (c) Hydraulic Compression Rail - An electric motor operates a hydraulic pump which in turn drives two hydraulic motors. The drive wheel mounted on each motor is compressed and runs on opposing sides of a rail (leg of angle iron), with the other angle iron leg attached to the gate to operate the gate.

K. Swing Gate Power-Operators

1. Power-operators for swing gates can generally be placed in two groups based upon their method of operation:
 - (a) Hydraulic Piston - A hydraulic piston is attached between the gate leaf and an offset post. The piston is extended and contracted to operate the gate.
 - (b) Electromechanical Swing Arm - An electric motor, through gear reduction, operates a primary arm that travels in an arc parallel to the ground. A second arm is attached between the gate leaf and the primary arm thereby operating the gate. While an independent life-cycle cost analysis for swing gate power-operators has not been made, preliminary analysis indicates that the hydraulic piston type of swing gate power-operator has a greater degree of reliability, particularly in areas of measurable snowfall. Greater reliability generally relates to lower maintenance cost. With the acquisition

cost of swing gate power-operators being comparable, the hydraulic piston type of swing gate power-operator is recommended for swing-gates.

L. Gate Power-Operator Peripherals

1. The means of activating gate power-operators can be as simple as push buttons to open, close, and stop the gate or can be a very complex electronic automated system. The requirements of controlling the motion, direction, braking, and locking of the gate and gate power-operator are increasingly more demanding. Manufacturers can provide many additional features as standard equipment such as “pause to reverse” and “maximum run time.” (“Pause to reverse” delays the gate from immediately reversing from an open cycle to a close cycle, thereby avoiding the shock load on the gate power-operator’s mechanics; “Maximum run time” prevents the gate power-operator from continuing to run after a preset time if the gate is obstructed.)
2. Access control must be a primary consideration for the designer when designing gate systems. Access control may be as simple as having a guard physically open a gate to allow access, or as complex as a system that logs the activity of individuals and the time of their access to specified areas by use of a designated code number. Features, devices, and electronic equipment to automate or expedite access control should be considered during the design of power-operated gates. A number of issues must be addressed before an access control system design can be considered complete. These include pedestrian traffic, reversing devices to keep gates from closing on vehicles, traffic flow, number of open and close cycles, and type of vehicular traffic. The designer needs to analyze the operational site security plan and review the details of his on-site inspection. Next, he should discuss access requirements for the restricted area(s) consult with CBP/IA/SMD to determine the degree of access control required. Electronic access control has a very broad spectrum of devices, technology, and capabilities. CBP/IA/SMD should be consulted for specific information concerning electronic access control systems. Additionally, technical guidance may be obtained from CBP/IA/SMD at CBP.Security@dhs.gov.

- For more information, see [Chapter 11, Access to Facilities](#).

M. Select Peripheral Equipment

The following must be taken into account when selecting peripheral equipment to activate gate power-operators:

- (a) Who will be authorized to activate the power-operators and where are they located? (Guard in Access Control Point, remote radio control, key switch, push button, or card reader?)
- (b) How will access control personnel communicate with personnel desiring

entrance and exit from the restricted area? (Directly, intercom, telephone?)

- (c) How will the gate be closed after the vehicle has gained entry? (Guard personnel, automatic timer, infrared (IR) beam?)
- (d) How will the gate be opened and closed to permit vehicle exit? (Guard personnel, IR beam, button or keypad, remote radio control, roll-across sensor, card reader?)

N. Study Terrain

Conduct a thorough study of the terrain in the general vicinity of a proposed gate to determine the most suitable gate type and design for that specific location. Review the site survey and access control plan during the gate selection process. Basically, there is little security difference between gate types. While there are a number of factors to consider in selecting the proper gate for a perimeter fence, the designer will find that terrain and operational aspects are the driving forces in gate selection.

O. Protection for Overhead-Supported and Vertical-Lift Gates

For overhead-supported and vertical-lift gates, the designer needs to provide additional protection for the upright posts, protruding above the nominal fence height that can be used as an advantage by an intruder.

P. Impound Lot (Outside) Fence

Basic Requirements

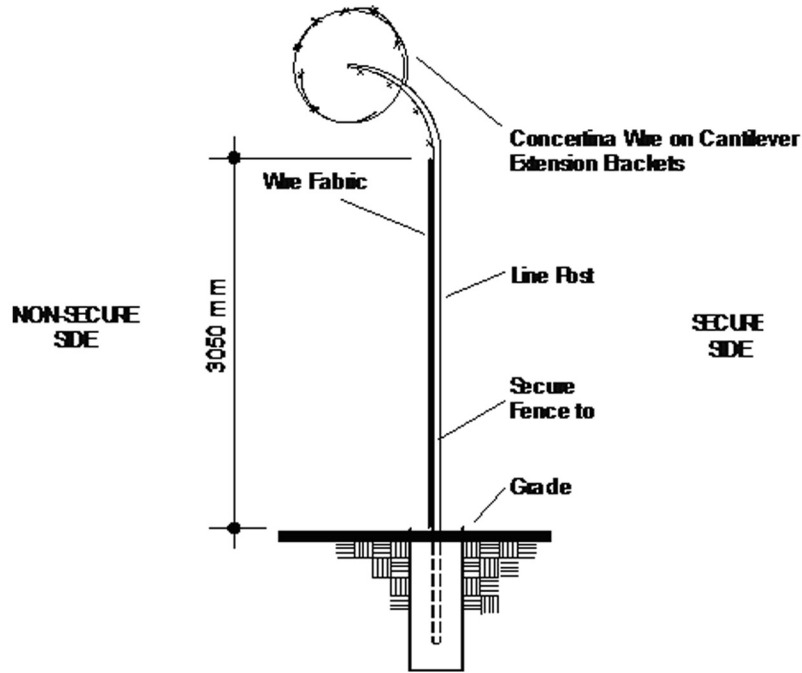
A fenced impoundment lot is required for the storage of seized vehicles and other large items such as boats, trailers and recreational vehicles. Parking space for oversized vehicles must be provided in the impoundment lot. It should be located as far away from the border or public occupied areas as possible, yet still be observable from the regularly staffed areas. Security cameras and additional lighting must be provided.

Q. Paving

The impoundment lot should be paved, through 100-mm (4-inch) thick crushed rock or gravel surface may be considered depending on climate conditions. It must be surrounded by a 3000 mm (10 foot) high fence, with an outward sloping cantilever top and crowned with 3 strands of barbed wire. The fence must be continuously secured to grade. A storage building may be required for storage of large non-vehicle items. The entrance must be well lit and must have an intrusion detection system.

R. Minimum lighting level shall be 32–54 lx (3 - 5 FC).

Figure 31: Perimeter Fence with Concertina Wire



Minimum Requirements for an 8-Ft. Perimeter Fence Cut Sheet	
Component	Perimeter, Employee parking, Securing equipment within the perimeter
Specification	Federal Specifications RR-F-191/GEN
Gauge/Material	9-Gauge (3.9-mm) or heavier Steel Wire Mesh (Before any coating)
Mesh	Minimum 2 inches (50.8-mm) per side
Fabric	Fabric height is 7 feet (2.13-m) and has twisted and barbed selvage at the top and bottom
Coating	Zinc coated, aluminum coated, or polyvinyl chloride (PVC) over zinc or aluminum coated
Tension Wires	Provide Type I or Type II tension wire, Class 4 coating, in accordance with ASTM A 824. Provide 7-gauge coil spring wire for top and bottom wire
Line Posts and Bracing	Steel pipe formed sections, H-Sections, square sections (See Federal Specs RR-F-191/GEN). Accomplish bracing with steel truss rods not less than 5/16-inch (7.9-mm) nominal diameter and a turnbuckle for tensioning, conforming to RR-F-191/GEN
Outriggers	Steel outriggers and barbed wire will be installed to conform to RR-F-191/4 with their overhang facing outward (away from the protected site). As a minimum, the outriggers will provide an additional 12 inches (304.8 mm) to the fence height
Barbed Wire	Provide barbed wire conforming to ASTM A 121 zinc-coated, Type Z, Class 3, or aluminum-coated, Type A, with 12.5-gauge wire with 14-gauge, round, 4-point barbs spaced no more than 125 mm (5 inches) apart
Height of Fence with Outriggers	8 Feet (2.44-m)
Pole Reinforcement	Buried, encased in concrete
Concrete Footing	Build to your local building code. Terminal post footings should be 12 inches (300 mm) wide and 36 inches (1 m) deep. Line post footings should be 10 inches (250 mm) wide and 36 inches (1 m) deep

Minimum Requirements for a 10 Ft. Impound Lot Fence Cut Sheet	
Component	Impound Lots within the perimeter
Specification	Federal Specifications RR-F-191/GEN
Gauge/Material	9-Gauge (3.9-mm) or heavier Steel Wire Mesh (Before any coating)
Mesh	Minimum 2 inches (50.8-mm) per side
Fabric	Fabric height is 9 feet (2.73-m) and has twisted and barbed selvage at the top and bottom
Coating	Zinc coated, aluminum coated, or polyvinyl chloride (PVC) over zinc or aluminum coated
Tension Wires	Provide Type I or Type II tension wire, Class 4 coating, in accordance with ASTM A 824. Provide 7-gauge coil spring wire for top and bottom wire
Line Posts and Bracing	Steel pipe formed sections, H-Sections, square sections (See Federal Specs RR-F-191/3). Accomplish bracing with steel truss rods not less than 5/16-inch (7.9-mm) nominal diameter and a turnbuckle for tensioning, conforming to RR-F-191/4
Outriggers	Steel outriggers and barbed wire will be installed to conform to RR-F-191/4 with double V of two 45-degree arms for six strands of wire, one set for each post where barbed wire is indicated. As a minimum, the outriggers will provide an additional 12 inches (304.8 mm) to the fence height
Barbed Wire	Provide barbed wire conforming to ASTM A 121 zinc-coated, Type Z, Class 3, or aluminum-coated, Type A, with 12.5-gauge wire with 14-gauge, round, 4-point barbs spaced no more than 5 inches (125 mm) apart
Height of fence with Outriggers	10 Feet (3.66-m)
Pole Reinforcement	Buried, encased in concrete
Concrete Footing	Build to your local building code. Terminal post footings should be 12 inches (300 mm) wide and 36 inches (1 m) deep. Line post footings should be 10 inches (250 mm) wide and 36 inches (1 m) deep

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

Minimum Requirements for a 12 Ft. Impound Lot (Outside) Fence Cut Sheet	
Component	Impound Lots and remote sites outside the perimeter
Specification _____	Federal Specifications RR-F-191/GEN
Gauge/Material	9-Gauge (3.9-mm) or heavier Steel Wire Mesh (Before any coating)
Mesh	Minimum 1 inches (25.4-mm) per side
Fabric	Fabric height is 11 feet (3.35-m) and has twisted and barbed selvage at the top and bottom
Coating	Zinc coated, aluminum coated, or polyvinyl chloride (PVC) over zinc or aluminum coated
Tension Wires	Provide Type I or Type II tension wire, Class 4 coating, in accordance with ASTM A 824 . Provide 7-gauge coil spring wire for top and bottom wire
Line Posts and Bracing	Steel pipe formed sections, H-Sections, square sections (See Federal Specs RR-F-191/3). Accomplish bracing with steel truss rods not less than 5/16-inch (7.9-millimeters (mm)) nominal diameter and a turnbuckle for tensioning, conforming to RR-F-191/4
Outriggers	Steel outriggers and barbed wire will be installed to conform to RR-F-191/4 with double V of two 45-degree arms for six strands of wire, one set for each post where barbed wire is indicated. As a minimum, the outriggers will provide an additional 12 inches (304.8 mm) to the fence height
Barbed Wire	Provide barbed wire conforming to ASTM A 121 zinc-coated, Type Z, Class 3, or aluminum-coated, Type A, with 12.5-gauge wire with 14-gauge, round, 4-point barbs spaced no more than 125 mm 5 inches apart
Height of fence with Outriggers	12 Feet (3.66-m)
Pole Reinforcement	Buried, encased in concrete
Concrete Footing	Build to your local building code. Terminal post footings should be 12 inches (300 mm) wide and 36 inches (1 m) deep. Line post footings should be 10 inches (250 mm) wide and 36 inches (1 m) deep

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.



APPENDIX 7.5: PROTECTIVE LIGHTING

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

[Return to Table of Contents](#)

I. GENERAL

A. Physical Security Definitions

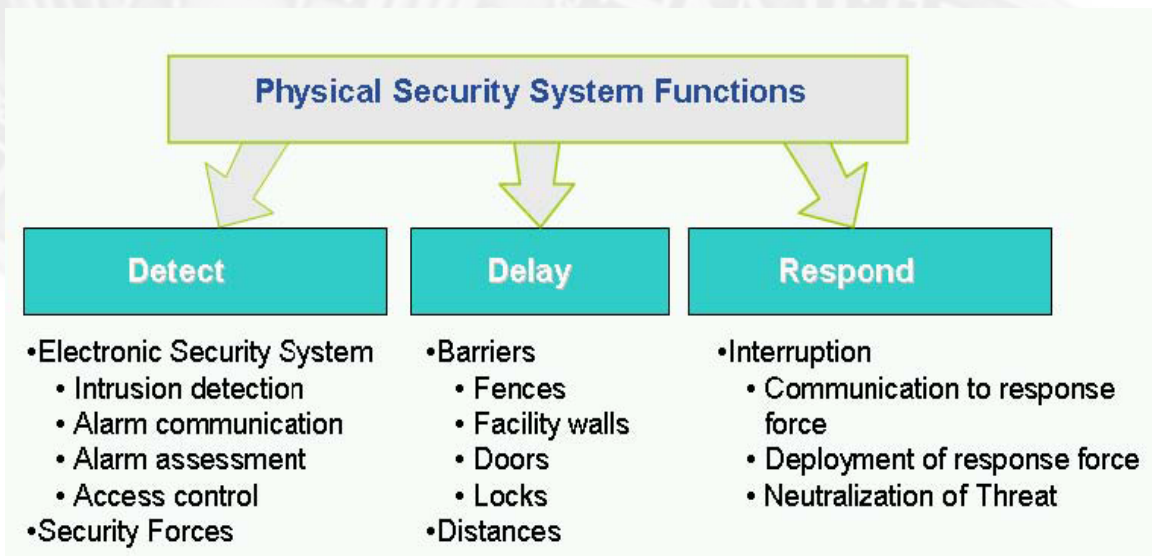
1. Physical Security:

(a) That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

2. Physical Security System:

(a) A system comprised of people, equipment, and operational procedures that control access to critical facilities or assets. Security lighting is one of the elements that comprise the equipment component of a physical security system. [Figure 1](#) diagrams some of the components of a physical security system.

Figure 1: Physical Security System Functions



3. Security lighting provides illumination during periods of darkness or in areas of low visibility to aid in the detection, assessment, and interdiction of aggressors by security forces. Security lighting is sometimes referred to as protective lighting. It enhances the Deter, Detect, Assess, and Respond functions of a physical security system.

B. Security Lighting Objectives

1. Security lighting is one of many components of an in-depth physical security

[RETURN TO TOP](#)

system. While the level of protection may vary, the lighting must supplement and facilitate all other measures taken to ensure the security of an asset.

2. These measures may include security forces at an entry control point, patrols along a perimeter fence, or closed circuit television (CCTV) cameras. In all cases, the lighting enhances visibility for either an individual or device and facilitates their performance.
3. In the simplest form, security lighting provides a clear view of an area for security personnel while reducing concealment opportunities for aggressors. A physical security system must be able to detect a threat, assess the threat, and then neutralize the threat.

C. Deterrent Value

1. Security lighting at a site may deter lesser threats and aggressors. While a security lighting system will not deter sophisticated criminals or terrorists, it may influence unsophisticated criminals or vandals from taking their planned actions. The mere presence of light will increase the probability of detection or capture and may influence these types of aggressors to look for an easier target.
2. Similarly, the effective use of lighting can enhance the perception of security, which is important to the personnel who work within a secure area. This can be accomplished through the definition of requirements. Defining the requirements of a physical security system and its components involves an interdisciplinary planning team. The team considers all interests relating to a project to determine how security fits into the total project design. Developing the planning team will be based on local considerations, but in general, the following functions should be represented: facility user, antiterrorism officer, operations, security, logistics, engineering, life safety, and others as required. That team will use the process in UFC 4-020-01 to identify the design criteria, which includes the assets to be protected, the threats to those assets (the Design Basis Threat), and the levels of protection to be provided for the assets against the identified threats. In addition to those criteria elements, the team must also identify user constraints such as appearance, operational considerations, manpower requirements or limitations, energy conservation, and operational costs.
3. In some areas where fence lines and water boundaries cannot be patrolled, the use of effective lighting can be critical.

D. Security Lighting Design

1. The security lighting system must aid in the detection of aggressors and assist personnel in the assessment and response to potential threats. The type of site lighting system provided depends on the installation environment and intended use.

[RETURN TO TOP](#)

E. Lighting Systems

1. There are three types of systems used for security lighting:

(a) Continuous Lighting

- The most common security lighting system is a series of fixed lights arranged to illuminate a given area continuously.

(b) Standby

- With this system, the luminaires are either automatically or manually turned on at times when suspicious activity is detected by security personnel or an intrusion detection system. A standby system creates the impression of activity and may offer a deterrent value while also achieving energy conservation. Consider electrode-less fluorescent (induction) lamp systems in lieu of light sources that require re-strike.

(c) Moveable

- Moveable lighting (stationary or portable) consists of manually operated searchlights that may be lighted during hours of darkness or as needed. This system is normally used to supplement continuous or standby lighting. This system will not be discussed in these criteria.

2. Each lighting type may be designed with a particular strategy or technique.

F. Controlled Lighting

1. Controlled lighting is best used when it is necessary to limit the width of the lighted strip outside the perimeter due to adjoining property. Care should be taken to minimize or eliminate silhouetting or illuminating security personnel on patrol. Use full cutoff or fully shielded luminaires mounted in the horizontal plane. [Figures 2 - 4](#) show different configurations of controlled lighting.

Figure 2: Example of controlled lighting with luminaire located outside the perimeter fence. This illuminates and draws attention to the aggressor, but not the security personnel.

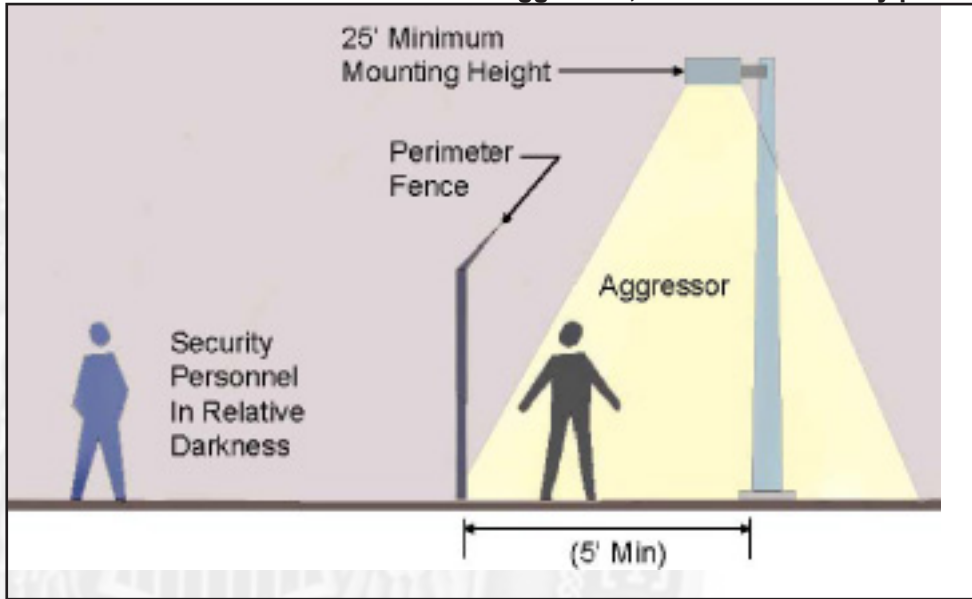


Figure 3: Example of controlled lighting located inside and adjacent to perimeter fence. The luminaire location must not provide a means for access over the fence.

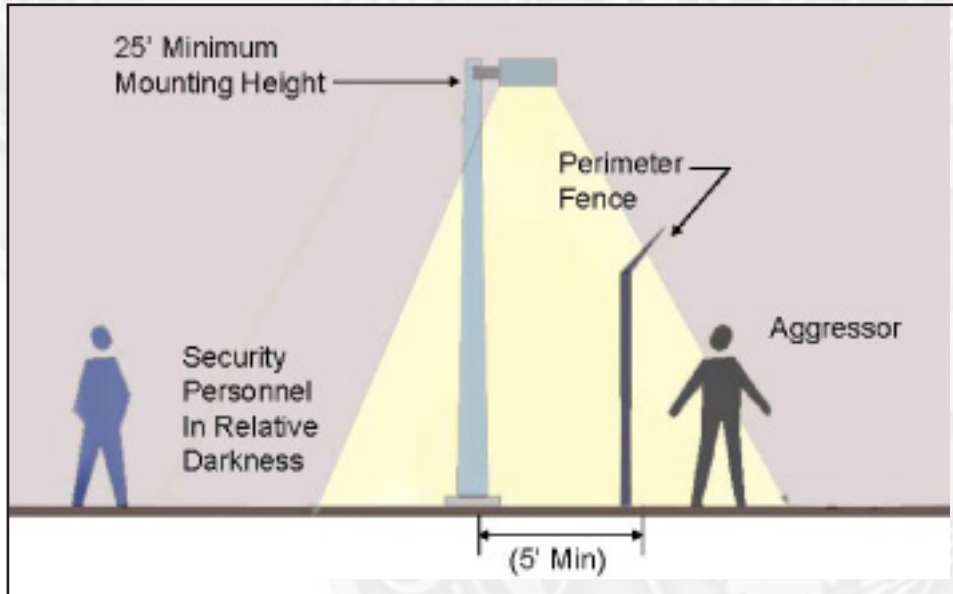
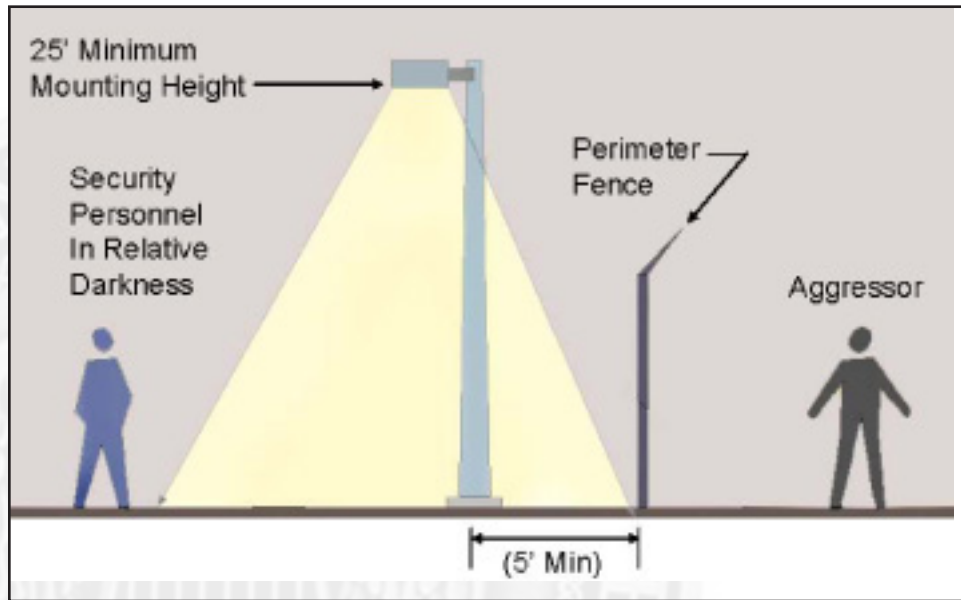


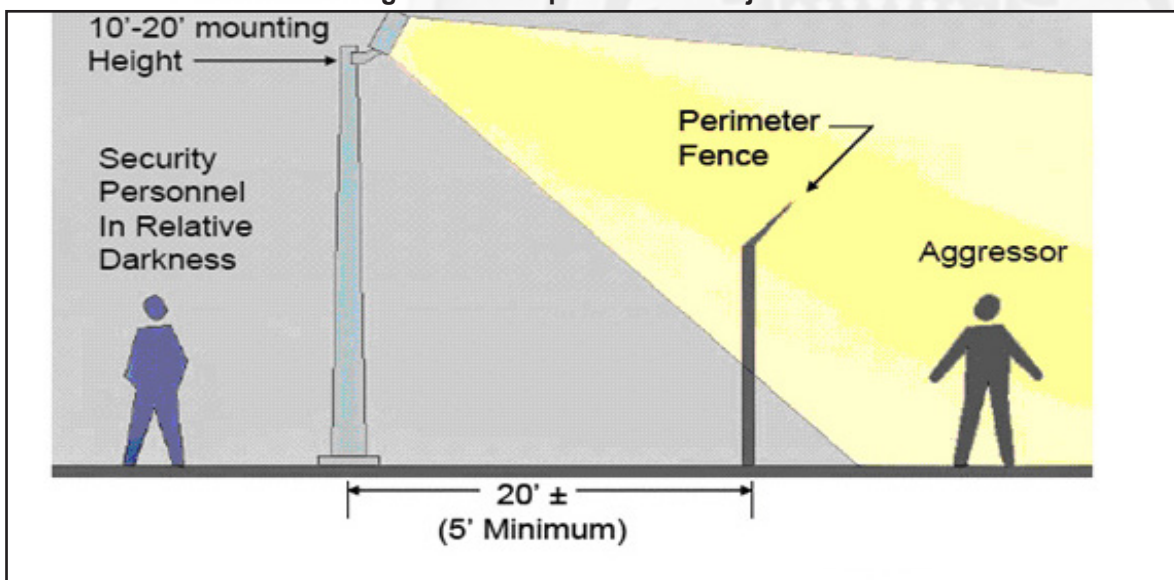
Figure 4: Example of Controlled Lighting



G. Glare Projection.

1. One technique for glare projection lighting is to place lights slightly inside a security perimeter and directed outward. This method is useful when the glare of lights directed across surrounding territory will neither annoy nor interfere with adjacent operations. It is a deterrent to potential intruders because it makes it difficult to see inside the area being protected. It also protects security personnel by keeping them in comparative darkness and enabling them to observe intruders at a considerable distance beyond the perimeter.

Figure 5: Example of Glare Projection



H. Conditions for Visibility

1. When designing a security lighting system, consider the viewer of the scene. Conditions for adequate visibility may differ widely depending on how a particular scene will be surveyed. The human eye sees quite differently from the lens of a security camera. A camera may not require visible light at all or be hampered by the addition of visible light. In many applications, the lighting will be for guards, patrols, or other security personnel. The human eye responds to light to provide two types of vision: off-axis and on-axis.
2. Off-axis detection refers to peripheral vision. This type of vision is very sensitive to movement as well as glare. Its poor visual acuity does not allow off-axis vision to distinguish details or recognize objects or people. Under low light levels, off-axis vision is enhanced by white light. White light sources include metal halide, fluorescent, and induction.
3. On-axis focus refers to viewing objects immediately within the field of view (or straight ahead). The visual acuity is much higher for on-axis vision and it is not as sensitive to glare. This type of vision allows for the identification of objects and people.

I. Integration With Other Security Measures

1. When possible, consider integrating the lighting equipment with other architectural or landscape features. For example, some manufacturers offer hardened light poles which offer the strength of a bollard at the base while providing a mounting location for the luminaire.

J. Security Lighting Criteria

1. Acceptable ranges of illuminance, luminance, and uniformity should be provided for security tasks. Illuminance values appropriate for security personnel may range from an average of 1 lux (0.1 fc) for large open areas to an average of 100 lux (10 fc) in area of ID checks for entry control points. If guards must perform any written task (such as inside a guardhouse), the illuminance on the task plane may reach an average 300 lux (30fc). However, this value should not be exceeded and should also be limited to the task plane only. Illuminance values in excess of this may inhibit the individual's ability to adapt to lower lighted areas outside. See [Table 1](#) for more detail.

K. Color Rendition Index

1. For individuals, the color rendition index is vital to the threat identification objective of security lighting and should be a minimum of 80. Guards must be able to accurately describe and report the threat. White light sources such as metal halide, induction, and fluorescent all render color much better than the

[RETURN TO TOP](#)

yellow light of sources such as high pressure sodium.

L. Color Temperature

1. Color temperature is the color appearance of the lamp. A lower color temperature refers to a warmer colored lamp while a higher temperature designates a cooler color. While individuals typically prefer warmer colors, cooler colors may be considered in security applications to improve visual acuity and help to maintain alertness. A minimum color temperature of 3500 K should be specified.

M. Level of Protection (LOP)

1. Level of Protection (LOP) defines the degree to which the asset is protected from the threat. Various facilities may require various levels of protection. The levels of protection are established using UFC 4-020-01, and should be provided as part of the design criteria. The LOP of any area determines the amount and type of security lighting necessary.
2. Low Level of Protection (LLOP)
 - (a) Low Level of Protection (LLOP) requires illumination at building entries and exits. The luminaires should be low brightness and well shielded so that it does not become a glare source in the much darker surroundings.
3. Medium Level of Protection (MLOP)
 - (a) Medium Level of Protection (MLOP) requires LLOP criteria and illumination of the building exterior. Full cutoff or fully *shielded* luminaires mounted on the building wall can illuminate the exterior of the building without adding light to the surrounding area or cause light trespass to neighboring properties.
4. High Level of Protection (HLOP)
 - (a) High Level of Protection (HLOP) requires MLOP criteria and illumination of the area around the facility. This lighting may still be accomplished with wall mounted lighting on the building. By using a different luminaire distribution, light can be directed to the surrounding area rather than just at the building. For larger areas, poles may be necessary to light further from the building. With full-cutoff luminaires, a perimeter width of 2-3 times the mounting height can be illuminated.
5. Very High Level of Protection (VHLOP)
 - (a) Very High Level of Protection (VHLOP) requires HLOP criteria and lighting of the perimeter fence. In some circumstances, glare projection strategies may be employed to limit visibility into a secure area.

[RETURN TO TOP](#)

N. Design Coordination

1. Architectural:

- (a) Coordinate luminaire locations with building entries, building surfaces, and mounting locations. Building-mounted luminaires can provide surface brightness and eliminate the cost of a pole.

2. Site:

- (a) Coordinate locations of luminaires with gates, fences, standoff requirements, trees and shrubs. Avoid locations which will result in shadows that could be used by aggressors for hiding.

3. Electronic Security Systems:

- (a) Investigate ways that the lighting system may be integrated with the alarm system. Are some lights automatically turned on when a zone goes into alarm? How might the lighting change once an alarm has been initiated? Design the lighting system so that luminaires are not in the field of view of the camera. Verify the camera illumination requirements and limitations for proper function and display.

4. Operational:

- (a) Determine how a facility will be secured. Coordinate security lighting strategies, lighting controls, and timers with planned patrol routes, schedules and operational procedures.

II. SECURITY LIGHTING APPLICATIONS

- A. General strategies or providing good visibility in an energy efficient manner include controlling glare, providing good lighting uniformity, and addressing other issues such as surface brightness and controls. The following specific strategies pertain to security lighting.

1. General Area Security Lighting

- (a) Luminaires located along the fence perimeter provide uniform horizontal and vertical illuminance. Use adjacent building facades or other structures to mount area lighting. This can add brightness to the surrounding environment and reduce the amount of equipment needed.

2. Building Security Lighting

- (a) Entrances and Exits

- Increasing the light level at the building entrance directs visitors and other personnel to the appropriate building entry. It also serves as exit lighting to guide individuals out of a building for life safety in case of an emergency. The security lighting at these locations should protect against forced-entry and provide enough light for threat assessment. Building entrances and exits must be lighted for all levels of protection. Use concealed, fully shielded or low brightness sources to limit glare while still increasing brightness.

(b) Building Exterior

- Lighting of the building frequently includes some area lighting as well. By using full cutoff or fully shielded, wall mounted luminaires; both the building and the adjacent area can be illuminated. Mounting luminaires at the top of the facade and aiming the light down will increase the facade brightness and also reduce light trespass and light pollution.

3. Perimeter Lighting

- (a) Illumination of a restricted area perimeter includes the exterior and interior clear zones adjacent to the fence, or in some applications, the area between multiple fences. Provide poles, power circuits, and transformers within the protected area. Coordinate pole locations with the user to ensure that the applicable egress requirements and patrol routes of the clear zone are not violated. The distance of poles from the fence will not be less than 10 feet. Perimeter lighting can be either continuous or standby, controlled or glare projection depending on the application.

4. Controlled Lighting

- (a) Illumination levels for controlled lighting shall be adequate to detect a moving aggressor, either visually or by use of CCTV. Provide full cutoff or fully shielded luminaires mounted in the horizontal plane to minimize glare. Glare may hinder security personnel visibility and interfere with authorized activities or activities outside the installation.

5. Glare Projection

- (a) Glare Projection shall provide glare projection only to illuminate flat areas which are free of obstructions for a minimum of 100 feet outside the fence. Glare projection should only be utilized in isolated or expeditionary locations in high threat environments. When designing for glare lighting, the designer must check for light pollution ordinances of the local jurisdiction.

III. ENTRY CONTROL FACILITIES

A. Entry Control Facility Criteria

1. Refer to [UFC 4-022-01 for Entry Control Facility Criteria](#). Entry Control Facilities are separated into several zones. The lighting design for each zone is described in the following paragraphs.

2. Approach Zone

(a) While the approach zone can vary significantly between locations, it should be illuminated to lead motorists safely to the access zone. Full cutoff or fully shielded luminaires mounted in the horizontal plane should be used to minimize glare. To reduce adaptation issues for the motorist, gradually increase (transitional lighting) lighting levels as the motorist approaches the access zone. To reduce glare for security personnel, provide signage to instruct motorists to turn off headlights as they approach the access zone.

3. Access Zone

(a) Lighting in the access zone provides the highest light levels in the entry control facility. The lighting system must provide for identification and inspection. For most of the access zone, full cutoff or fully shielded luminaires will provide adequate lighting for most of these visual tasks. However, vertical illuminance on motorists' faces can be improved with the use of low brightness (less than 3500 lumen lamp output). Luminaires mounted to the side and behind security personnel will improve identification tasks.

(b) Response Zone

- From the access point, roadway lighting should gradually return to lower light levels (transitional lighting) while still providing adequate uniformity.

(c) Cutoff and Shielded Luminaires

- Provide full cutoff or fully shielded luminaires mounted in the horizontal plane to minimize glare for motorists and security personnel in the response zone. In addition, provide signage to instruct motorists to turn headlights back on after leaving the access zone.

(d) Pedestrian Access Control Point (ACP)

- Pedestrian zones must provide light for both pedestrians and security personnel. Pedestrians must have a clear view of gates and

[RETURN TO TOP](#)

card access readers and security personnel must be able to see pedestrians approaching the ACP. Provide full cutoff or fully shielded luminaires mounted in the horizontal plane to minimize glare.

(e) Guard Station

- Inside the guard station, task lighting must be provided for reviewing identifications, paper work, and possibly computer tasks. However, the interior light levels must be kept at a lower ambient light level than the exterior. Otherwise, the security personnel will have reduced visibility and those approaching the shack will have a clear view of the interior. The location and shielding of interior lighting must minimize the chance of veiling reflections on the glass which may limit visibility to the outside. All luminaires must be dimmable to adjust inside lighting levels. Colored light should not be used for task lighting when color is to be distinguished.

(f) Over Watch Position

- These locations must maintain an unobstructed view through the access and response zones. Additionally, inside the over watch itself, lighting must be kept to extremely low levels or eliminated entirely to prevent the lighting of the security personnel. All luminaires must be dimmable to adjust lighting levels. While red colored light has been used in such applications to maintain the eye's dark adaptation, colored light should not be used for task lighting when color is to be distinguished in the task.

B. CCTV camera

1. Vehicle Inspection

- (a) In areas where a security personnel must identify visitors, check credentials, and read shipping manifests, lighting must not interfere with the operations while vehicles approach, stop for inspection, and proceeds. Having to continually adapt to different illuminance and brightness levels could lead to eyestrain and reduced performance by security personnel. Additional task lighting should come from behind the guard and light the person to identify or the vehicle to inspect.
- (b) Cameras respond to a luminous environment differently than the human eye. The field of view of a camera refers to the extent of the scene that can be viewed at one time. Some devices may use motorized swivels to pan across a scene and increase the viewing area. Cameras adjust the view based on the brightest point in this field. If it must adjust for a hot spot, areas under low illuminance levels may not be visible at all. Uniform

[RETURN TO TOP](#)

illuminance and fully shielded/full cutoff luminaires are vital to limit hot spots and improve CCTV system performance. Any luminaire that falls within the camera's field of view at any time must be shielded. If a light source can be seen directly by the camera, the glare and high contrast will limit the visibility of the entire scene. Therefore, the source of illumination is best located above the level of the camera.

2. Color Rendition Index

- (a) For color cameras, the color rendering index of the sources lighting the area should be above 80. While color rendering is less important for monochrome systems, high pressure sodium lamps should still be avoided as their limited spectral distribution may render a fuzzy image.

3. Uniform Vertical Illuminance

- (a) CCTV cameras typically record objects and people in elevation. Therefore, the security lighting system must provide adequate and uniform vertical illuminance. As in many security lighting applications, the amount of vertical illuminance is far more important than horizontal. Vertical illuminance should average 0.2 to 0.5 foot-candles at 5 feet above the ground. Furthermore, it should have a very uniform coverage of 4:1 average to minimum. Color cameras may require higher light levels than monochrome cameras. Review camera manufacturer recommendations and coordinate with the security system designer when designing the lighting system.

4. Infrared (IR) Cameras

- (a) IR cameras utilize IR sources to illuminate the field of view. Light in the IR spectrum is not visible to the human eye. IR cameras then pick up the reflections of these wavelengths from objects in the area.

5. Thermal Imaging

- (a) Devices using thermal technology do not require any light source to operate. They create images based on the heat differences between humans, vehicles, the ground, and foliage. Unlike other camera technologies, thermal imagery is not affected by glare from headlights or light sources. While this technology can indicate the presence of people and objects in complete darkness, it does not provide the detailed images obtainable from visible light or IR cameras.

6. Waterfronts

- (a) These areas are typically a combination of the entry control facilities, area,

[RETURN TO TOP](#)

and perimeter lighting. However, approach zones are often very short and additional control points are located at the entry to each pier. Full cutoff area and structure lighting will limit both direct and reflected glare near waterfronts for all of these areas.

- (b) Be aware of environmental issues, such as impact of lighting on indigenous wildlife, when planning exterior lighting near waterfronts.
- (c) For example: when lighting facilities near sea turtle nesting areas, the exterior lighting must be fully shielded and limited to reduce its impact on turtle hatchlings, especially during hatching seasons. These seasons typically fall between May and October although they may vary by particular region. Hatchling turtles orient themselves with visual cues including skylight reflected from the ocean. Each year, electrical exterior lighting disorients thousands of sea turtles and draws them away from the ocean – their best chance of survival. While researchers do not have exact casualty figures, many states, including Florida maintain aggressive lighting ordinances to limit exterior light during the nesting season.

7. Airfields

- (a) Exterior lighting must meet all Federal Aviation Administration (FAA) and airfield operational regulations. These regulations may restrict the height of poles located near an airfield. Coordinate security lighting with installation's airfield safety officer. Use full cutoff or fully shielded luminaires to reduce glare which may affect airfield operations.

8. Specific Lighting Criteria

- (a) The specific lighting criteria and design issues may vary with application. For this reason, see the appropriate security lighting application in [Chapter 7, Exterior Protection, Table 1](#) summarizes the minimum horizontal and vertical illuminance levels for typical facility applications. It is important to note however that over lighting can cause just as many visibility problems as under lighting. In typical applications, the maximum light levels should not be more than double the recommended average value.

9. Electrical Requirements

- (a) Backup power is not required for all security lighting systems. The assessment of risk and asset value will determine this need. For critical security lighting systems, several different types of systems are available for providing backup power in the event of a power outage. All offer various advantages and disadvantages. They vary in amount of time that they can provide power, amount of downtime between a power outage and backup power, and cost. The back-up power system must also

[RETURN TO TOP](#)

consider the re-strike time of some light sources. Metal halide and high pressure sodium lamps both require a certain amount of time to cool-down before they can be re-ignited. This time may reach up to fifteen minutes. While these sources can still be used, an intermittent light source may be required.

10. Backup Generators

- (a) Generators are commonly used to provide backup power but have some downtime between the outage and when the generator restores power. Minimum downtime can be as low as ten seconds. While this is one of the least expensive solutions, operations must be able to sustain the short period of darkness. Frequently, small battery packs power a few luminaires during this downtime until the generator can restore power.

11. Uninterruptible Power Supply

- (a) An Uninterruptible Power Supply (UPS) is a battery source that provides instantaneous power in case of a power loss. UPS systems have a high initial cost and are expensive to maintain. Therefore, only provide a UPS for security lighting systems associated with the protection of critical assets or operations when continuous, full brightness lighting is required.

12. Flywheels

- (a) Flywheels provide instantaneous power in the case of power loss in the form of the kinetic energy in a constantly rotating wheel. This energy can be harnessed immediately in the event of a power outage and used to power critical lighting. These devices vary widely in price and capacity.

13. Integral Batteries

- (a) Individual battery packs are available for some luminaires. In the event of a power outage, these packs can power the lighting for times ranging from five minutes to two hours, depending on the battery capacity. For fluorescent or induction sources, the battery will power the ballast directly although the lamp may not provide full light output.

14. Partial Back-up Systems

- (a) Light sources requiring a re-strike can be specified with a partial back-up system such as quartz re-strike. In this case, the luminaire contains a primary lamp, such as metal halide, and then a smaller quartz lamp. In the event of a power outage, the metal halide source will require a cool down time before it can be re-ignited. During this period the quartz lamp uses generator-supplied power to light the area. The lighting level will not be as

[RETURN TO TOP](#)

high, but interim lighting will be provided. When the primary source returns to full brightness, the quartz lamp is extinguished. A separate, complete back-up lighting system does not provide an economical or effective design solution. Consider electrode less fluorescent (induction) lamp or LED systems in lieu of light sources that require re-strike.

15. Circuiting Techniques

- (a) Circuiting luminaires onto separate circuits in the same space will not provide backup power but will limit vulnerabilities during a fault. If the lighting system is divided onto two circuits, the loss of one will not affect half of the lighting system. Multiple systems should be installed, except where their use is clearly impracticable. The over current devices, transformer, and wiring should be within the restricted area. Locate circuits underground to minimize the possibility of sabotage or vandalism. Equipment and design should provide for simplicity and economy in system maintenance. To minimize security degradation during faults, feeders may be 3-phase, 4-wire with single pole over current devices at the service equipment. Consecutive luminaires will be connected to alternate phases of 3-phase feeders.

C. Controls

1. On/Off control will be automatic, manual, or manual/automatic as appropriate.

(a) Automatic

- Perimeter and area lighting On/Off control will be automatic and will be activated during periods of darkness or at other times when visibility is reduced or by electronic security systems. In expeditionary environments, automatic on-off control must be capable of being deactivated which may require either manual/automatic or manual on-off control depending upon the site.

(b) Manual

- Wherever manual On/Off control is appropriate, on-off controls will be accessible to and operable only by authorized personnel. Systems which are designed to remain off until needed, will have on-off control at the surveillance location and will meet instant-on requirements. Electrode-less fluorescent (induction) or LED would be the appropriate luminaire choice for this type of application.

(c) Manual/Automatic

- In some applications, motion sensors can be used to turn on lights

[RETURN TO TOP](#)

FOR OFFICIAL USE ONLY

BACK

[Return to Table of Contents](#)

when someone approaches. This alerts patrols or other personnel that activity is taking place in a particular area and should be assessed. Such control strategies will reduce energy consumption and may also startle and deter unsophisticated criminals.

**Table 1: Minimum Lighting Criteria for Unaided Guard Visual Assessment.
TABLE 1: CBP SECURITY LIGHTING**

Application			Illuminated Width Feet (m)		Average Illuminance (All Lighted Areas)		Uniformity
Type	Lighting	Area	Inside	Outside	Locations to Light	Foot-candles (lux) ^a	(Max : Min)
Perimeter	Glare	Isolated	25 (7.6)	150 (46)	Outer lighted edge	0.2 (2) ^b	20:1
	Controlled	Semi-isolated	10 (3.0)	70 (21)	At fence Outer lighted edge	0.4 (4) 0.2 (2)	20:1
	Controlled	Non-isolated	20-30 (6.1-9.1)	30-40 (9.1-12)	At fence Outer lighted edge	0.4 (4) 0.4 (4)	10:1
Inner Area	Area	General	All	-	Entire Area	0.2-0.5	10:1
Building Lighting	Controlled	LLOP	-	-	Building Entry and Exits	0.1-0.3 (1-3)	20:1
	Controlled	MLOP	-	-	Same as LLOP and exterior walls.	0.2-0.5 (2-5)	15:1
	Controlled	HLOP	-	-	Same as MLOP and perimeter area.	0.5-1.0 (5-10)	10:1
	Controlled	VHLOP	-	-	Same as HLOP and lighting of perimeter fence.	0.5-1.0 (5-10)	10:1
Entry Control Facility	Controlled	Pedestrian	25 (7.6)	25 (7.6)	Entry	2 (20)	10:1
		Vehicular (Approach and Response Zones)	50 (15)	50 (15)	Pavement and sidewalk	1 (10)	10:1
		ID Verification	All	-	Guard station	20 (200)	10:1
Parking or Storage Areas	Area	Outside	All	-	Entire Area	2 (20)	10:1
	Area	Covered	All	-	Entire Area	5 (50)	10:1

a Horizontal plane at ground level unless otherwise noted. b Vertical plane, 3 feet (0.9 m) above grade. c Use higher value for more sensitive areas.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.





APPENDIX 7.6: DOORS AND DOOR HARDWARE

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

I. EXTERIOR/PERIMETER DOORS

- A. The number of doors to a facility should be limited to an absolute minimum. In cases where more than one door exists, only one of these should be provided with outside-mounted locks and entry hardware. All others should, if possible, present blank, flush surfaces to the outside to reduce their vulnerability to attack.
- B. Perimeter doors must be constructed of 12-gauge steel clad, hollow core metal, 1³/₄-inches thick. Solid core wood doors are not authorized for use on the perimeter of a facility. Door frames must be constructed of hollow metal that is equal in strength to that of the door.
- C. All exterior perimeter doors must be equipped with deadbolt locks equipped with UL 437 cylinder. The deadbolts must have at least a 1-inch throw. Coordination must be made with the local fire marshal before construction to determine compliance with building code(s) associated with National Fire Protection Association 101 (NFPA 101).
- D. Double doors must have one door secured with Flush Mount Bolts ([Door Hardware H](#)) at the top and the bottom. Astragals ([Door Hardware A](#)) must be used to inhibit access to latches from the attack side of the door.
- E. A Balanced Magnetic Alarm Switch ([Door Hardware G](#)) must be installed on each perimeter door to detect the opening/closing of the door. The application of this type of door alarm is utilized due to its application of two magnetic poles rather than one on standard alarm systems. This reduces the risk of the alarm switch being compromised. For more information on Intrusion Detection Systems, see [Appendix 8.9, IDS](#).
- F. All perimeter doors must have a commercial grade automatic door closer installed ([Door Hardware K](#)).
- G. To prevent access to the latch/deadbolt, all perimeter doors will have anti-pry strips installed. Refer to [Figure 3](#) for minimum design specifications and illustrations.
- H. Perimeter door hinge pins that are located on the outside of the facility must be non-removable ([Door Hardware J](#)). Additionally, a dowel-pin and socket system should be utilized. Refer to [Figure 2](#) and [Figure 4](#) for minimum design specifications and sample illustrations.
- I. All door hardware (e.g., hinges, lock hardware) must be secured to the door frame with stainless steel screws that are at least 3 inches long.

1. Building Entrances

(a) Material:

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- Doors must be constructed of 12-gauge steel clad hollow core metal, 1³/₄-inches thick, and hung in hollow metal frames. Wood Doors will not be used on the perimeter of a facility.
- Other than in a secure reception area, there will be no windows.

(b) Hardware:

- Install [Lockset D](#) or [H](#) (as applicable).
- Install [Cylinder A](#).
- Install [Door Hardware F.1](#), if door is equipped with a card reader/ keypad.
- Install [Door Hardware E](#).
- Install [Door Hardware G](#).
- Install [Door Hardware L](#), if door swings outward.
- Install [Door Hardware J](#), if door swings outward.
- Install [Door Hardware K](#).

J. Perimeter door designated as an emergency exit

1. Perimeter exits that provide emergency egress must generate a local audible/ visual alarm at the door, if it is breached. An alarm must also annunciate in the Control Room. Depressing a door activation bar for more than two seconds will initiate an alarm and activate the associated CCTV camera.
2. A High-Security Emergency Exit device with deadbolt should be installed. It is distinguishable from other exit devices in the following ways: (1) it is labeled for both fire and emergency and (2) it has no means of locking the deadbolt or latch in a retracted position.
3. Emergency exits should be equipped with special locking devices approved by the National Fire Prevention Association (NFPA), that provide opening delays of 5-15 seconds. The installation of breakable devices or niches over door activation bars can often deter misuse. In consultation with local code officials, design a system that assures safety and also satisfies CBP requirements.
4. Emergency exits will be equipped with non-removable hinges with a set screw in the barrel that is only accessible when the door is swung open.

(a) Material:

- Doors must be constructed of 12-gauge steel clad hollow core metal, 1³/₄-inches thick, and hung in hollow metal frames.

(b) Hardware:

- Install [Lockset H.](#)
- Install [Door Hardware E.](#)
- Install [Door Hardware G.](#)
- Install [Door Hardware L.](#), if door swings outward.
- Install [Door Hardware J.](#), if door swings outward.
- Install [Door Hardware K.](#)

K. Overhead Coiling Doors:

1. Overhead doors will be the roll-up, flush-fitting type with a balanced magnetic switch attached to the bottom of the door.
2. The doors are to be factory-fitted with a slide-bolt that can be extended through each of the metal slide rails. Each slide-bolt will be fitted to the door within 6 inches of the floor and designed to accommodate the use of a high security padlock.
3. The doors will be fitted with the appropriate electric motor system supplied by the manufacturer. The motor system shall have a manual override feature in the event the motor fails. Chains used to operate the door manually shall be of such a length that the door can be easily operated from the floor. An eyebolt will be affixed into the concrete in the area of the chain to allow the use of a high security padlock as an additional security feature. The electric control buttons and the manual override feature will be located so that they cannot be reached by cutting a hole through the door.

(a) Material:

- Doors must be metal, dual-slat, manufactured with 12-, 14-, or 16-gauge exterior slats and 18-, 20-, 22-, or 24-gauge interior slats with insulated centers.

(b) Hardware:

- Install [Door Hardware G.](#)
- Install High Security Padlock

II. INTERIOR DOORS

A. Counter-Terrorism Response Suite (CTR), Rover Coordination Center (RCC),
CBP Coordination Center (CCC)

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset D](#) or [H](#).
- (b) Install [Cylinder A](#), keyed individually under a CBP master.
- (c) Install [Door Hardware F.1](#).
- (d) Install [Door Hardware G](#).
- (e) Install [Door Hardware L](#), if door swings outward.
- (f) Install [Door Hardware J](#), if door swings outward.
- (g) Install [Door Hardware K](#).
- (h) Provide access control/card reader.

B. Secondary Exam Podium and Baggage Belts Area (Port of Entry only)

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset D](#).
- (b) Install [Cylinder A](#), keyed individually under a CBP master.
- (c) Install [Door Hardware F.1](#).
- (d) Install [Door Hardware J](#), if door swings outward.
- (e) Install [Door Hardware K](#).

[RETURN TO TOP](#)

C. CBP/APHIS Veterinary Services (VS) Bird Quarantine and Bird Holding Facilities
(Port of Entry only)

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset D](#).
- (b) Install [Cylinder A](#), keyed individually under a CBP master.
- (c) Install [Door Hardware B](#).
- (d) Install [Door Hardware D](#).
- (e) Install [Door Hardware E](#).
- (f) Install [Door Hardware J](#), if door swings outward.
- (g) Install [Door Hardware K](#).
- (h) Install door seal around frame.

D. Interview Rooms

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames. The upper half of the door must be equipped with a tempered-glass view window. The door must swing 180-degrees in the direction of egress.

2. Hardware:

- (a) Install [Lockset B](#).
- (b) Install [Cylinder A](#), key interview rooms alike.
- (c) Install [Door Hardware B](#).
- (d) Install [Door Hardware D](#).
- (e) Install [Door Hardware E](#).

E. Violator Waiting Area (Port of Entry only)

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames. The door should have a 180-degree swing in direction of egress. (The doors must swing out from the room so individuals can not barricade themselves in when the officer steps out.)

2. Hardware:

- (a) Install [Lockset E2](#).
- (b) Install [Cylinder A](#), keyed individually under a CBP master.
- (c) Install [Door Hardware B](#).
- (d) Install [Door Hardware D](#).
- (e) Install [Door Hardware E](#).
- (f) Install [Door Hardware J](#).
- (g) Install door-pull on ingress side and a push plate on egress side of door.

F. Violator Processing Area (Port of Entry only)

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset D](#).
- (b) Install [Cylinder A](#), keyed individually under a CBP master.
- (c) Install [Door Hardware D](#).
- (d) Install [Door Hardware F1](#).
- (e) Install [Door Hardware K](#).
- (f) Provide access control/card reader.

G. Search Room

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾ inches thick, and hung in hollow metal frames. The doors must swing in the direction of egress.

2. Hardware:

- (a) Install [Lockset E2](#).
- (b) Install [Cylinder A](#), key search rooms alike.
- (c) Install [Door Hardware B](#).
- (d) Install [Door Hardware D](#).
- (e) Install [Door Hardware E](#).
- (f) Install [Door Hardware J](#).
- (g) Install door-pull on ingress side and a push plate on egress side of door.

H. Hold Room

1. Material:

- (a) Doors must be constructed of 2-inch thick, detention-grade, 12-gauge steel that swings in the direction of egress. The door frames must be 12-gauge steel and grouted into the surrounding wall. The door must be equipped with security glass or a barred window, 12-inches x 12-inches and installed at the standard height for convenient visual checks. Security glass and bars must be of appropriately sturdy construction to prevent escape. Do not install a door closer on hold room doors.

2. Hardware:

- (a) Detention –type hardware is required, as indicated below. Finish of visible parts must match finish of other building hardware.
- (b) Hinges: 4 1/2” X 4 1/2”, minimum 3 per door, heavy duty ball bearing type with tamper-resistant screws and non-removable pins.
- (c) Locks: Locks shall be detention dead bolt, heavy duty, mortised (MOGUL Key on One Side) mechanical with ADA compliant lever handles; except where suicide resistance is warranted, a substitute cone-shape handle may be used. Locks with interchangeable cores are acceptable (obtain

[RETURN TO TOP](#)

approval from COTR and Using Agency). It must deadlock in both locked and unlocked positions.

- (d) Door Pull: Raised pull on outside of door. Pushplate not required on inside face.
- (e) Door Stops/Wall Bumpers: Dome type 13/8" high or as required to meet applicable conditions.
- (f) Door Closers: No closers or self-closing hinges on hold rooms. Closers are required on doors to a secure perimeter.
- (g) Additional information about specifications for Electro-Mechanical Locks can be found in the following UL Listings: UL1034 listed as Burglary-Resistant Mechanisms, and UL10B listed as Fire Door Accessories.

I. Fraudulent Document Analysis Room (Port of Entry only); Alien Baggage Storage; and Joint Automated Booking System/Identification Room:

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset D](#).
- (b) Install [Cylinder A](#), keyed individually under a CBP master.
- (c) Install [Door Hardware B](#).
- (d) Install [Door Hardware D](#).
- (e) Install [Door Hardware E](#).
- (f) Install [Door Hardware J](#), if door swings outward.
- (g) Install [Door Hardware K](#).

J. Alien Documentation, Identification & Telecommunications Room (ADIT) (Port of Entry only)

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset D](#).
- (b) Install [Cylinder A](#), keyed individually NOT under a CBP master.
- (c) Install [Door Hardware B](#).
- (d) Install [Door Hardware D](#).
- (e) Install [Door Hardware E](#).
- (f) Install [Door Hardware J](#), if door swings outward.
- (g) Install [Door Hardware K](#).

K. Seizure Processing Area (Port of Entry only)

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Tamperproof with high security deadlock and no master key. Provide card reader/keypad to track users, but not as a substitute for a deadlock. The card reader shall be integrated to the locking mechanism. One shouldn't work without the other. Appropriately authorized card and key should be necessary for access. The door must be fitted with a UL-437 approved high security locking cylinder deadbolt lock (or equivalent). The keying must be different from all other keys and must be keyed off a master key.

L. General Storage/File Room

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, 40-42" wide and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset D](#).
- (b) Install [Cylinder A](#), keyed individually under a CBP master.
- (c) Install [Door Hardware D](#).

(d) Install [Door Hardware J](#), if door swings outward.

(e) Install [Door Hardware K](#).

M. Secure Storage Room

1. Material:

(a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾ inches thick, 40-42" wide and hung in hollow metal frames.

(b) Hinges and frame should be appropriate for door. Door may require shoring.

2. Hardware:

(a) [Install Lockset D](#).

(b) Install [Cylinder A](#), keyed individually, NOT under a CBP master.

(c) Install [Door Hardware B](#).

(d) Install [Door Hardware D](#).

(e) Install [Door Hardware J](#), if door swings outward.

(f) Install [Door Hardware K](#).

N. Temporary Seized Property Storage Vault (Evidence Storage)

1. Material:

(a) Doors must be constructed of 12-gauge steel clad hollow core metal, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

(a) Install [Lockset D](#).

(b) Install [Cylinder A](#), keyed individually under a CBP master.

(c) Install [Lockset G](#).

(d) Install [Door Hardware J](#).

(e) Provide Access Control/Card Reader

NOTE: A card reader/keypad will be utilized to augment the deadbolt lock. During non-working hours, the

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

deadbolt lock will be engaged.

O. CBP Chief Officer's Office (OIC); Supervisor's Office; Secondary Supervisor's Office

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾ inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset B](#).
- (b) Install [Cylinder A](#), keyed individually under a CBP master.
- (c) Install [Door Hardware B](#).
- (d) Install [Door Hardware D](#).
- (e) Install [Door Hardware E](#).

P. Anti-Terrorism Contraband Enforcement Team (AT-CET) Office; Passenger Analysis Unit (PAU)/Intelligence Office

(a) Material:

- Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾ inches thick, and hung in hollow metal frames.

(b) Hardware:

- Install [Lockset D](#).
- Install [Cylinder A](#), keyed individually under a CBP master.
- Install [Door Hardware B](#).
- Install [Door Hardware D](#).
- Install [Door Hardware E](#).
- Install [Door Hardware K](#).

Q. Weapons and Ammunition Storage

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

1³/₄-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset J](#) (recommended)
- (b) Install [Lockset G](#).
- (c) Install [Cylinder A](#), keyed individually NOT under a CBP master.
- (d) Install [Lockset D](#).
- (e) Installation of one of the following types of Door Hardware may be recommended: [F](#), [J](#), [K](#), [B](#), or [E](#)
- (f) An access control device or system will be utilized to track users. A card reader/keypad will be utilized to augment the deadbolt lock. During non-working hours, the deadbolt lock will be engaged.

R. General Office

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1³/₄-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) When entered from processing area, floor, or non-sterile side of terminal:
 - Install [Lockset D](#).
 - Install [Cylinder A](#), keyed individually under a CBP master.
 - Install [Door Hardware B](#) or [D](#).
 - Install [Door Hardware J](#), if door swings outward.
 - Install [Door Hardware K](#).
 - Provide access control/card reader.
- (b) When entered from a secure corridor:
 - Install [Lockset B](#).
 - Install [Cylinder A](#), keyed individually under a CBP master.

- Install [Door Hardware D](#).
- Install [Door Hardware K](#).

S. Cashier's Office

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1³/₄-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset D](#).
- (b) Install [Cylinder A](#), keyed individually NOT under a CBP master.
- (c) Install [Door Hardware B](#) or D.
- (d) Install [Door Hardware J](#), if door swings outward.
- (e) Install [Door Hardware K](#).
- (f) Provide access control/card reader.

T. Break Room; Male & Female Staff Toilets/Showers/Locker Rooms; Document/Copy/Shredder/Fax Room;

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1³/₄-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset B](#).
- (b) Install [Cylinder A](#), keyed like toilet rooms and physical training room under a CBP master.
- (c) Install [Door Hardware D](#).
- (d) Install [Door Hardware K](#).

U. Conference/Muster/Training Room

1. Material:

(a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset A](#).
- (b) Install [Cylinder A](#), keyed individually under a CBP master.
- (c) Install [Door Hardware B](#).
- (d) Install [Door Hardware D](#).
- (e) Install [Door Hardware E](#).
- (f) Install [Door Hardware K](#).

V. Canine Unit Office with General Storage

1. Material:

(a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset D](#).
- (b) Install [Cylinder A](#), keyed individually under a CBP master.
- (c) Install [Door Hardware B](#).
- (d) Install [Door Hardware D](#).
- (e) Install [Door Hardware E](#).
- (f) Provide access control/card reader.

W. CBP Agricultural Laboratory & Disposal Room

1. Material:

(a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) [Door Hardware K](#)

X. Emergency Generator Room

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

- Install [Lockset D](#).
- Install [Cylinder A](#), keyed individually under a CBP master.
- Install [Door Hardware C](#).
- Install [Door Hardware D](#).
- Install [Door Hardware J](#), if door swings outward.
- Install [Door Hardware K](#).

Y. Local Area Network/Telephone Communications Room; Communications Room (Radio)

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset D](#).
- (b) Install [Cylinder A](#), keyed individually NOT under a CBP master.
- (c) Install [Door Hardware D](#).
- (d) Install [Door Hardware J](#), if door swings outward.
- (e) Install [Door Hardware K](#).
- (f) An access control device or system will be utilized to track users. A card reader/keypad will be utilized to augment the deadbolt lock. During non-working hours, the deadbolt lock will be engaged.

Z. Mechanical Room

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames. Provide double doors, as required.

2. Hardware:

- (a) Install [Lockset D](#).
- (b) Install [Cylinder A](#), keyed individually under a CBP master.
- (c) Install [Door Hardware C](#).
- (d) Install [Door Hardware D](#).
- (e) Install [Door Hardware J](#), if door swings outward.
- (f) Install [Door Hardware K](#).

AA. Electrical Closet

1. Material:

- (a) Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1¾-inches thick, and hung in hollow metal frames.

2. Hardware:

- (a) Install [Lockset D](#).
- (b) Install [Cylinder A](#), keyed individually under a CBP master.
- (c) Install [Door Hardware D](#).
- (d) Install [Door Hardware J](#), if door swings outward.
- (e) Install [Door Hardware K](#).

III. VAULT DOORS

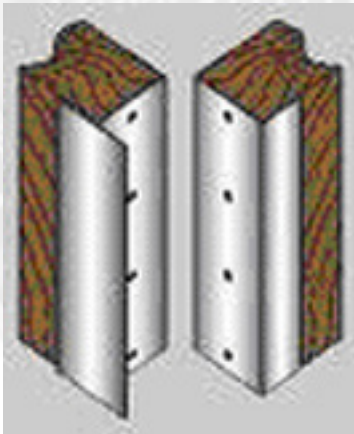
- A. Armory vault doors and security vault doors are both manufactured according to Federal Specification [AA-D-600](#) Door, Vault, and Security. The difference between the two doors is that armory vault doors, used to protect AA&E, are fitted with UL Standard 768, Group 1, mechanical combination locks. Security vault doors, used to protect classified information, are fitted with locks meeting Federal Specification [FF-L-2740 \(with Amendment 1\)](#), Locks, Combination. The armory vault door label (silver with red letters) states that it is a “GSA Approved Armory Vault Door.” The security vault door label reads “GSA Approved Security Vault Door” (label also silver with red

letters).

- B. At present, there are numerous GSA approved Class 5 security vault doors being used for the protection of weapons. We strongly recommend that locks be changed out to the UL Standard 768, Group 1, mechanical combination lock, when and if a failure occurs with an X-07, X-08 or X-09 lock. When that change is made it must be noted on the [Optional Form 89](#) (Maintenance Record for Security Containers/Vault Doors). It should also be noted on the front of the armory door that is not authorized for the protection of classified information.
- C. For further information on vault doors refer to [Chapter 8.7](#) and Federal Qualified Products List [QPL-AA-D-600-8](#).

IV. DOOR HARDWARE DESCRIPTIONS

Door Hardware A: Astragal

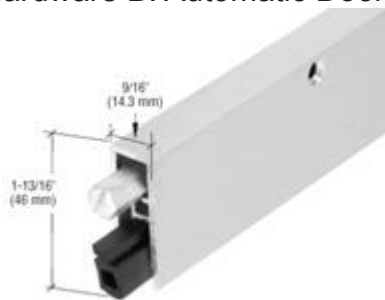


Hardware A1

A metal molding attached to the face of the active leaf of a pair of doors and overlapping the inactive leaf. See Figure A1.

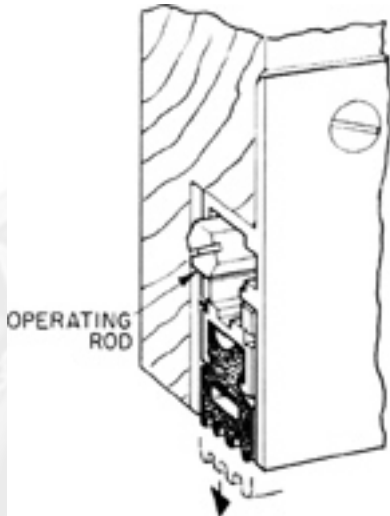
(CBP Policy: Astragals must be installed on all double doors leading into CBP space)

Door Hardware B: Automatic Door Bottom



Hardware B1

A movable plunger, in the form of a horizontal bar (B1) at the bottom of a door, which drops automatically when the door is closed; when closed, a horizontal protruding operating rod (B2) strikes the door jamb, thereby actuating the plunger, sealing the threshold (B3) and reducing noise transmission. This device is also known as an automatic threshold closer



Hardware B2

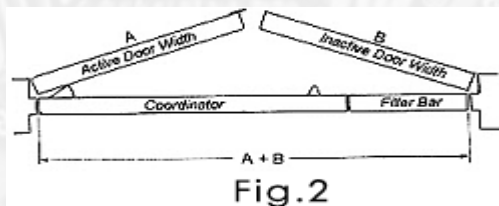


Hardware B3

Door Hardware C: Door Coordinator



Hardware C1



Hardware C2

A door coordinator is used on double doors when the inactive door needs to close earlier than the active door. This prevents the active door from closing before the inactive door thus preventing an unsecured situation.

Door Hardware D: Door Stop

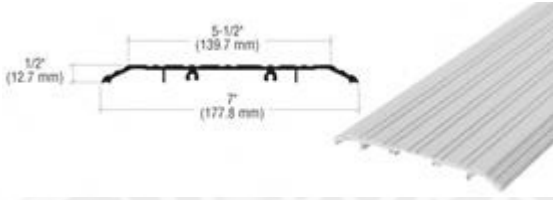


Hardware D

A rubber-tipped projection attached to a wall or floor to protect it from the impact of an opening door.

Door Hardware E: Door Threshold (Saddle)

A horizontal piece of metal that forms the bottom of a doorway and provides a visual and mechanical transition between the bottom of the door and the floor.



Hardware E1



Hardware E2

Door Hardware F: Electric Strike



Hardware F

A strike used with a lock and designed to be actuated by a remotely controlled electromagnet to permit the door to be opened without retracting the latch.

(CBP Policy: All electric door strikes must be 24 Volts AC and be centrally powered from a Communications closet.)

Hes-1006

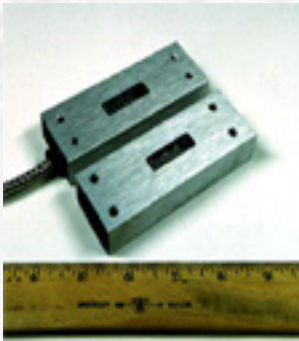
Door Hardware F-1: Electric Strike for Deadbolt Lock Doors

An electric strike must be utilized that can accommodate a mortise lock having up to a 3/4 inch throw latch bolt with a 1-inch deadbolt where the strike does not release the deadbolt. The strike must be tamper resistant, will be of heavy duty stainless steel construction, and must have a horizontally adjustable keeper or other horizontal adjustment to allow for door and frame misalignment. The strike must be Fail Secure.

Door Hardware F-2: Electric Strike for Non-Deadbolt Lock Doors

An electric strike must be utilized that can accommodate a non-deadbolt lock, e.g., bored lock, mortise lock, or mortise exit device having up to a 3/4-inch throw latch bolt. The strike must be tamper resistant, be of heavy duty stainless steel construction, and have a horizontally adjustable keeper to allow for door and frame misalignment. The strike must be Fail Secure.

Door Hardware G: Balanced Magnetic Alarm Switch (BMS)



Hardware G

A two-part sensor that generates an alarm condition when a change in the magnetic field between the parts is detected. A BMS is usually mounted on a door and door frame to detect opening of the door. The application of this type of door alarm is utilized due to its application of two magnetic poles rather than one on standard alarm systems. This reduces the risk of alarm switch compromise.

The BMS must meet UL 637 (Level II) requirements.

(CBP Policy: A BMS must be installed on each perimeter door to detect the opening/closing of the door.)

Door Hardware H: Flush Bolt



Hardware H1



Hardware H2

A bolt that is mortised into the edge of a door that will lock either or both the top and bottom of the door

Door Hardware I: Latch Protector

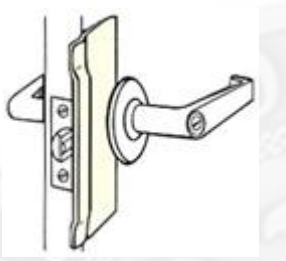


Figure I1

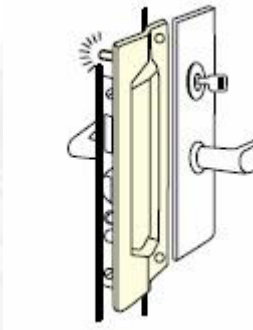


Figure I2



Figure I3

A device fastened to the door or frame that prevents access to the latch/deadbolt and cannot be pried or forced back.

(CBP Policy: Latch Protectors must be installed on all out swinging doors)

Door Hardware J: Non-Removable Hinges (NRPs)



Hardware J

A hinge equipped with a set screw in the barrel that is only accessible when the door is swung open. Must be installed to door frame with stainless steel screws at least 3 inches long.

(CBP Policy: NRP Hinges must be installed on all perimeter and out swinging doors)

Door Hardware K: Pneumatic Door Closer - Commercial Grade

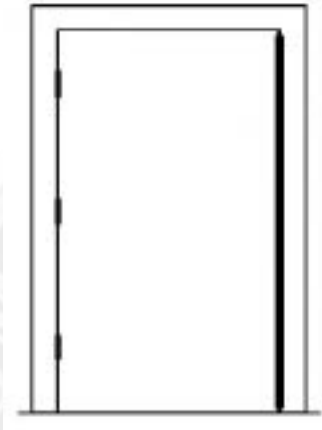


Hardware K

A device that automatically controls the closing or positioning of a door.

(CBP Policy: Automatic Door Closers must be installed on all perimeter doors and card reader doors.)

Door Hardware L: Anti-Pry Strip



Hardware L

A strip of 7-gauge steel, a minimum of 1¾-inches-wide that is installed on the outside of the door on the lock side. Used to prevent the door from being pried open.

(CBP Policy: All perimeter doors are required to have anti-pry strips installed.)

Cylinder A: UL 437 Compliant



Cylinder A

All CBP lock cylinders must be of a high security, pick resistant design with angled key cuts, rotating tumblers, keyway side biting, and a slider mechanism. The cylinders must be Underwriters Laboratories (UL) listed under UL437 and certified under American National Standards Institute (ANSI)/Builder's Hardware Manufacturer's Association (BHMA) certification A156.30, Levels MIAM and ANSI/BHMA A156.5, Grade 1.

All cylinders must incorporate three locking elements: a slider mechanism, a sidebar mechanism with tumbler rotation, and a pin tumbler elevation. All cylinders must be constructed of solid brass with hardened steel inserts. The lock tumblers must combine a dual-axis action with one axis utilized for pin tumbler rotation and the other axis utilized for positioning key cuts. Randomly selected tumbler pins must incorporate a hardened steel insert. The cylinders must be capable of being immediately re-keyed to a new combination or a new system.

Interchangeable cores should be used to facilitate this process. A suitable number of spare cores should be maintained to facilitate lock changes in the event of a lost or stolen master key.

The manufacturer must have the capability of establishing a key system with a minimum of six angle cuts in six possible pin positions with the capability of two distinct positions of

[RETURN TO TOP](#)

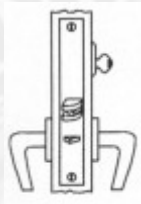
WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

cut per pin chamber, if required by the parameters of the system. The manufacturer must have the capability of producing a keying system in either of two distinct and different keying specifications and pinning specifications. The system must be capable of incorporating a key, with each being capable of more than one bitting per position to expand master keying and key changes. The key must also incorporate the capacity to include twelve possible side bittings along the key blade located on two different planes or surfaces of the key. The system must also have the capability to provide a single master key with over 1 million (1,000,000) usable, non-interchangeable change keys in a single keyway. The key thickness must be no less than one hundred, twenty-five thousandths (.125") and must be made from a nickel silver alloy. Each key must be custom coined for tracking and identification purposes.

The locking system must be deemed proprietary information shared only among authorized U.S. Customs and Border Protection (CBP) entities and the manufacturer. Security Specialists assigned to the Office of Internal Affairs, Security Management Division (IA/SMD) and employees serving as Collateral Security Liaison's for IA/SMD, will have the authority to request additional pinning materials and duplicate keys.

V. LOCKSETS

Lockset A: Commercial Grade 1 - Mortise Lever Lockset - Classroom Function

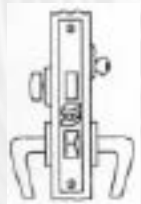


Lockset A

- For Doors 1 3/4" Minimum (1 1/4" armor front)
 - For Doors 1 3/8" Minimum (1" armor front)
- Latch Bolt By Key outside and lever either side unless outside lever is locked by key outside
Auxiliary latch deadlocks latch bolt
(CBP Policy: This lock is not permitted on perimeter doors or doors equipped with a card reader and electric strike.)

Lockset B: Commercial Grade 1 - Mortise Lever Lockset with Thumb Turn

Entrance Function



Lockset B

- For Doors 1 3/4" Minimum (1 1/4" armor front)
 - For Doors 1 3/8" Minimum (1" armor front)
- Latch Bolt By Key Outside and lever either side unless outside lever is locked by toggle action stop
Deadbolt by key outside and turn piece inside
Turning inside lever retracts latch and deadbolt simultaneously
Outside lever remains locked.

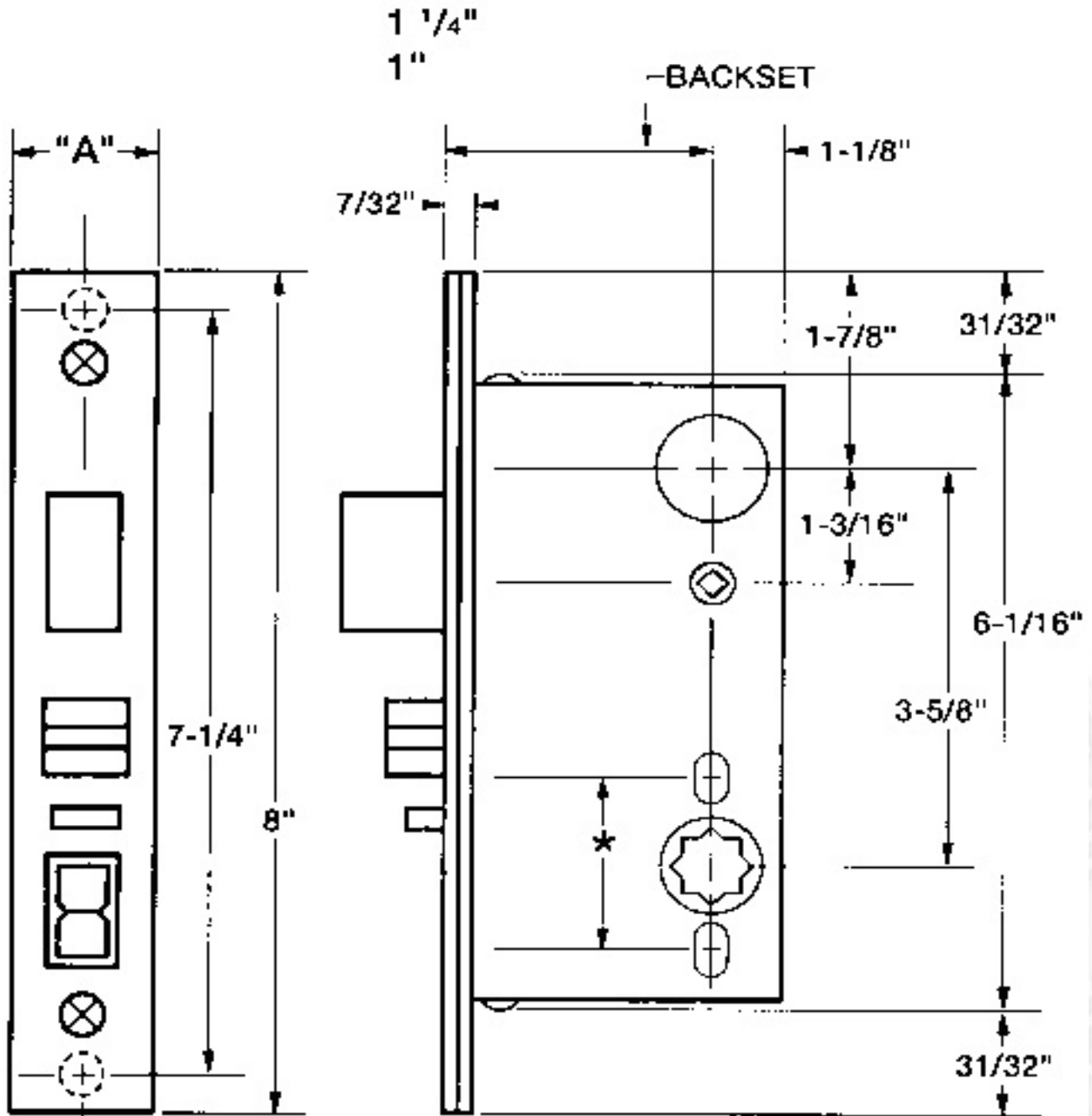
(CBP Policy: This lock is not permitted on perimeter doors or doors equipped with a card reader and electric strike.)

Mortise Lockset: Details



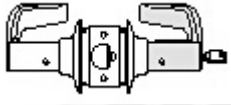
[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.



* TO ACCOMMODATE THRU BOLTING
1 1/2" - 1 11/16" CENTER TO CENTER

Lockset C: Commercial Grade 1 - Cylindrical Lever Lockset - Storeroom Function



Lockset C1

A lockset where the outside lever is always fixed, (i.e., locked) and the inside lever is always unlocked. Entrance is permitted by key only.

Lockset D: Commercial Grade 1 – Mortise High Security Lever Lockset with Deadbolt - Storeroom Function



Lockset D1



Lockset D2

A lockset where the latch bolt has a minimum 3/4-inch throw that is retracted by a key outside or by a lever inside and the outside lever is always fixed (i.e., locked). The deadbolt must have a 1-inch minimum throw which can only be thrown or retracted by a key outside or a thumb turn inside. By turning the inside lever, it simultaneously retracts both the deadbolt and latch bolt. Auxiliary latch deadlocks latch the bolt when the door is closed

FOR PERIMETER DOORS TRANSFORMATION INSTRUCTIONS (BELOW) MUST BE STRICTLY OBSERVED FOR LOCKSET D.

DO NOT INSTALL THUMBTURN UNIT ON INSIDE OF LOCKSET D SO THAT THE Deadbolt CAN ONLY BE THROWN OR RETRACTED BY THE KEY OUTSIDE.

Lockset E: Commercial Grade 1 - Mortise High Security Institutional Deadbolt Lever Lock (i.e., Double Cylinder Lock)



Lockset E1

Lockset E2



A lock where a deadbolt is installed on both sides of the door and must have a minimum 1-inch throw that is retracted by a key outside or inside

[RETURN TO TOP](#)

Lockset F: Commercial Grade 1 - Deadbolt/Dead Latch



Lockset F

A lockset where the outside handle is stationary. The hook shaped deadbolt is thrown or retracted by a 360-degree turn of the key. Turning the key 120-degrees further retracts the latch bolt.

Lockset G: CDX-09 High Security Electromechanical Lock

A self-powered, tamper resistant lock where the bolt is retracted by dialing a combination. The lock has audit trail capability and a limited view LCD display with indicator arrows.



CDX-09

5340-01-498-2759 CDX-09 Combination Deadbolt Lock For Pedestrian Doors With A Non-Drill Resistant Mounting Plate.

5340-01-498-2760 CDX-09 Combination Deadbolt Lock For Pedestrian Doors With a Drill-Resistant Mounting Plate.

CDX-09 must meet FF-L-2890.

Lockset H: High Security Exit Device with Deadbolt



Lockset H

An exit device which may legally be installed on a fire door. It is distinguishable from other exit devices for the following reasons: (1) it is labeled for both fire and panic and (2) it has no means of locking the deadbolt and latch in a retracted position.

(CBP policy: This device must be installed on all CBP doors designated as perimeter emergency exits. The device must accept a large format interchangeable core (LFIC) for key override purpose.)

Lockset I: Panic Exit Device



Lockset "I"

An exit device which may legally be installed on a fire door. It is distinguishable from other exit devices for the following reasons: (1) it is labeled for both fire and panic and (2) it has no means of locking the latch in a retracted position.

(CBP policy: This device must be installed on all CBP doors designated as interior emergency exits.)

Audible alarm requires key reset.

Lockset J: UL Group 1, Mechanical Combination Lock



Lockset J

A mechanical combination lock able to withstand 20 man-hours of expert manipulation as well as other specifications listed in UL 768.

VI. ADDITIONAL INFORMATION

Figure 1: Perimeter Door Hinge Side Protection – Medium-Severity Threat

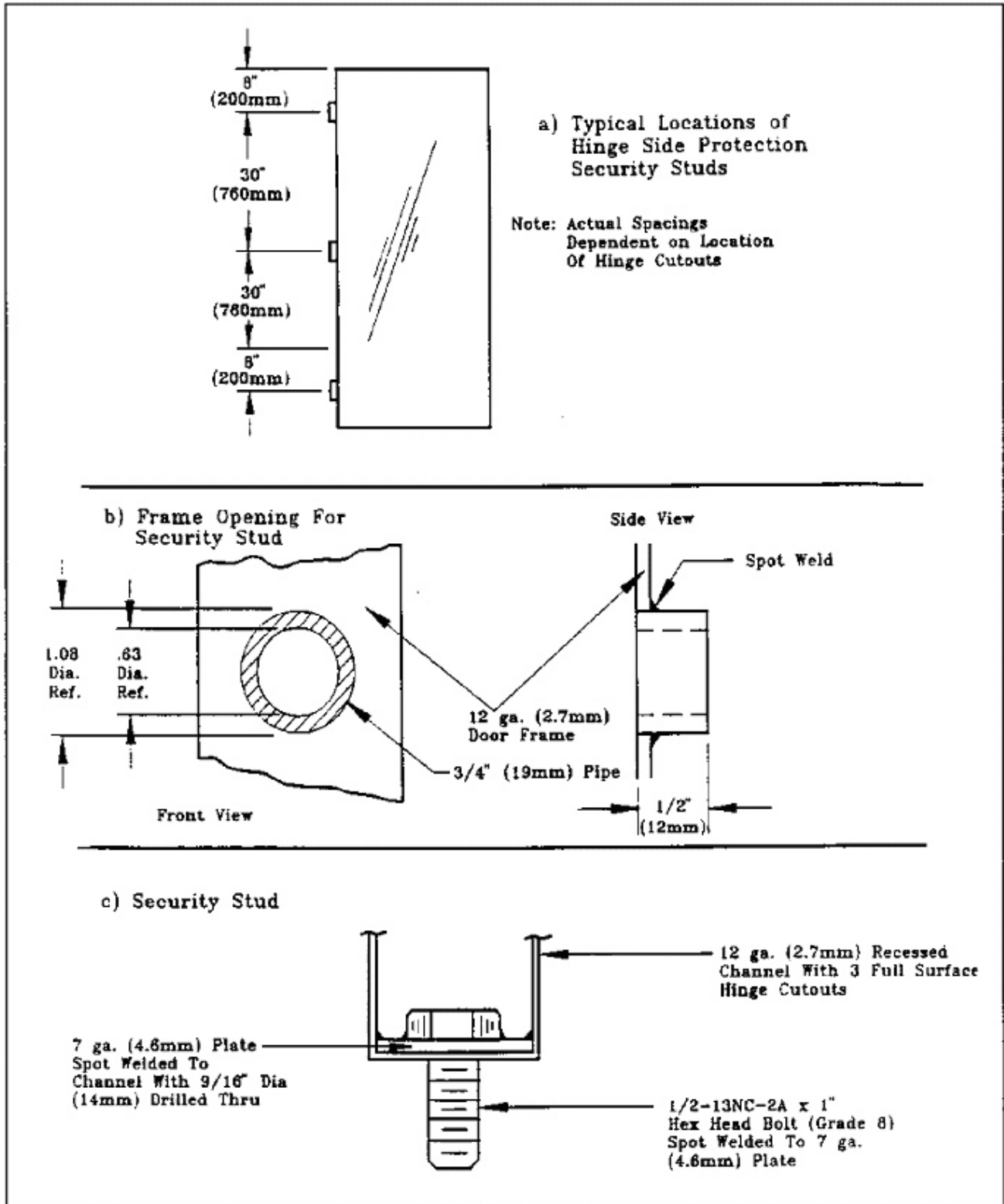
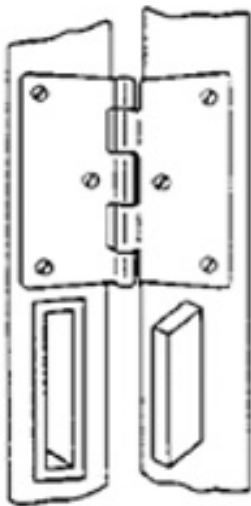
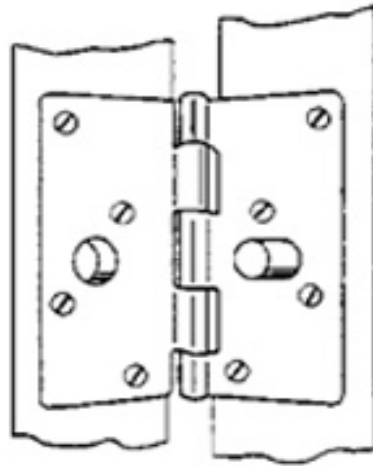


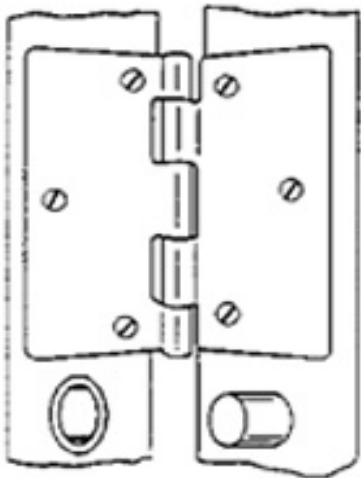
Figure 2: Perimeter Door, Medium-Security Hinge-Side Protection



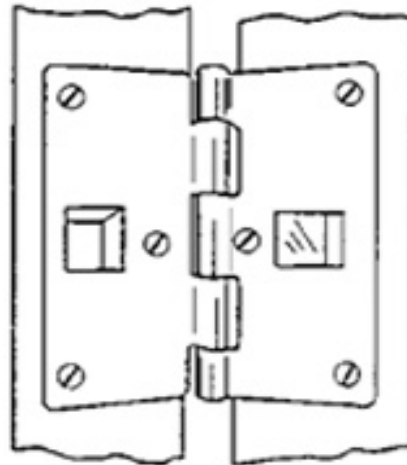
A) Metal lug and receptacle system.



B) Addition of a metal dowel-pin and socket to the existing hinge.



C) Installation of a metal dowel-pin in the door and reinforcing metal cup in the door frame.



D) Hinge with lug and matching socket formed into hinge at factory.

Note: Lugs, dowel-pins, etc., should be 1-inch-diameter (25.4mm) minimum.

Figure 3: Perimeter Door Anti-Pry Strips for Medium-Security Applications

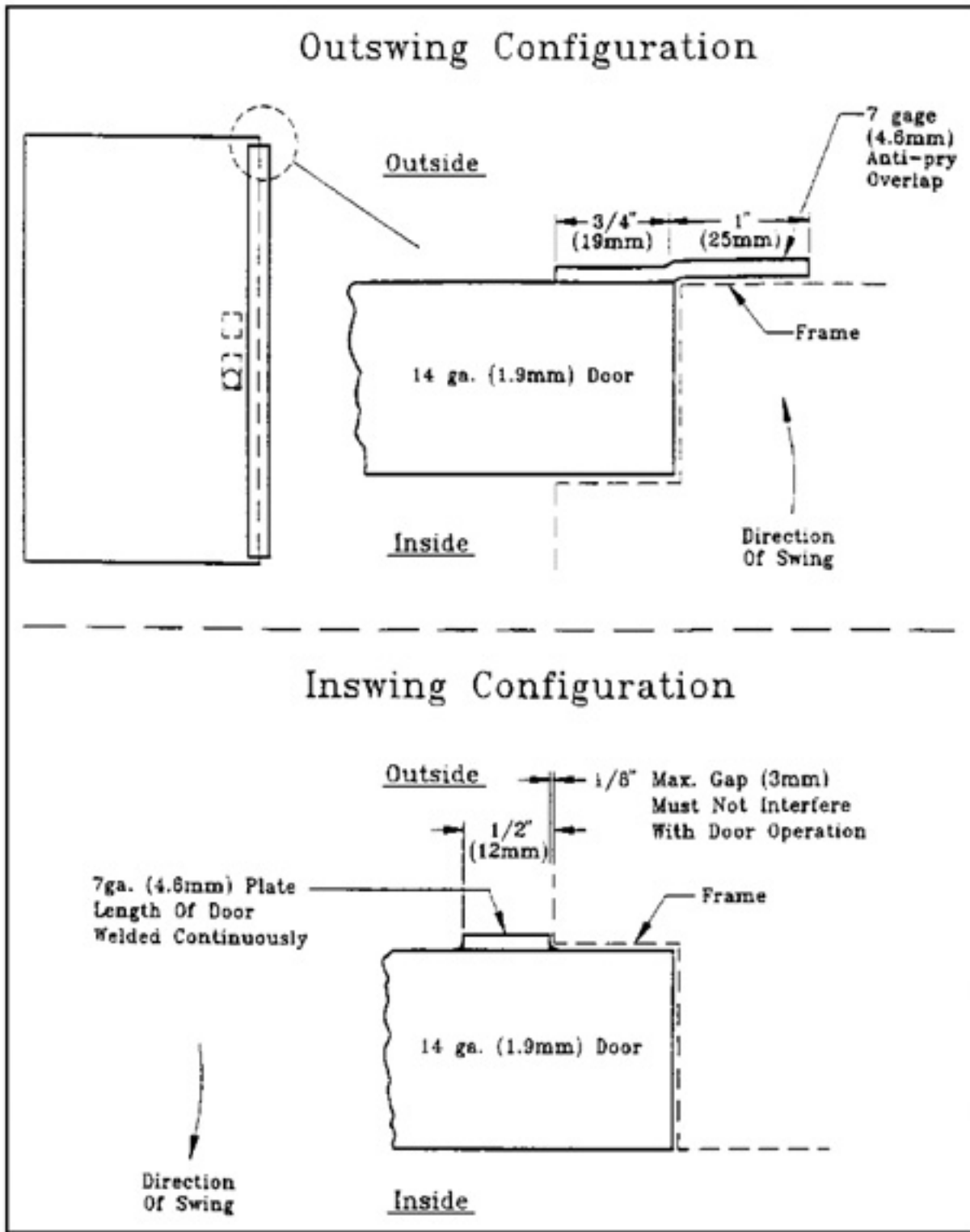
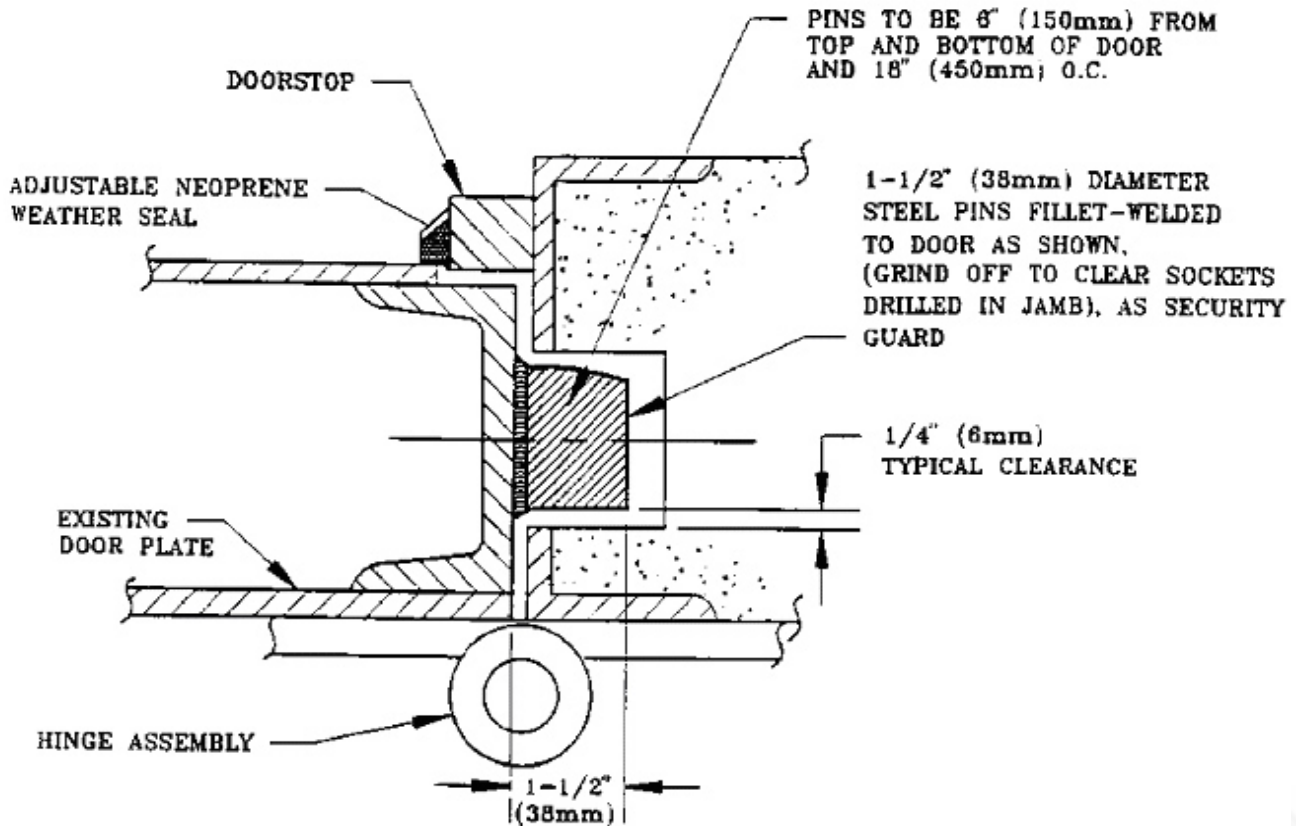


Figure 4: Hinge Side Protection Plan for Using a Pin-in-Socket Technique



VII. REFERENCES

- [MIL-HDBK-1013/1A](#), Design Guidelines for Physical Security of Facilities
- Land Port of Entry Design Guide
- Customs and Border Protection Lock Hardware Requirements for all Ports of Entry
- [AA-D-600D](#), Door, Vault, Security (with Amendment 1)
- [FF-L-2740A](#), Locks, Combination (with Amendment 1)

VIII. PERIMETER AND INTERIOR DOORS

Figure 5: Basic Perimeter Door

Basic Perimeter Door

Materials:

- Doors must be constructed of 12-gauge steel clad hollow core metal of single solid core wood, 1 ¾ inches thick, and hung in hollow metal frames. There will be no windows.

Hardware:

- Install Lockset H
- Install Cylinder A, keyed individually under a CBP Master
- Install Door Hardware G
- Install Door Hardware L, if door swings outward
- Install Door Hardware J, if door swings outward
- Install Door Hardware K

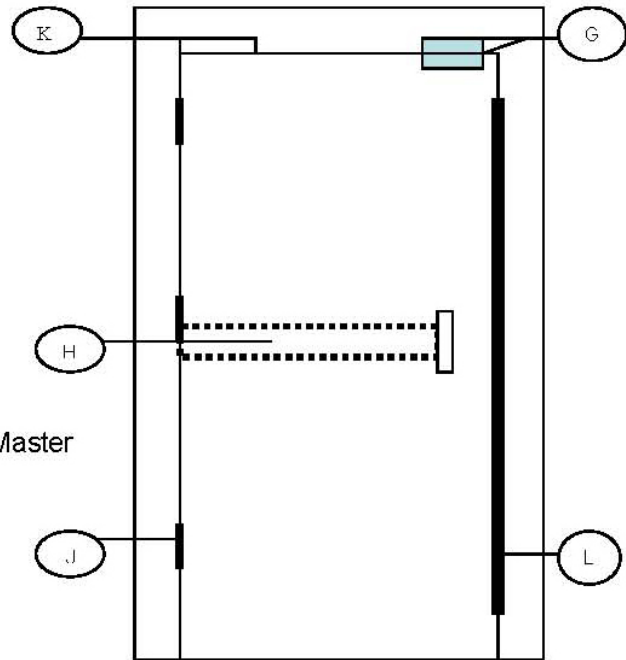


Diagram Key No.	Quantity	Manufacturer	Description	Part/Model No.
(K)	1	LCN	Pneumatic Door Closer	
(J)	Varies		Non-rechargeable hinge Pin (refer to Figure 2 for additional requirements)	
(G)	1	Sentro	Balanced Magnetic Alarm Switch	
(H)	1	Von Duprin	Panic Exit Device	
(L)	1		Anti-pry strip (installed on doors exterior) (Refer to Figure 3 for additional requirements)	

Security Hardware Set 1

Basic Perimeter Door

Figure 5: Basic Perimeter Door

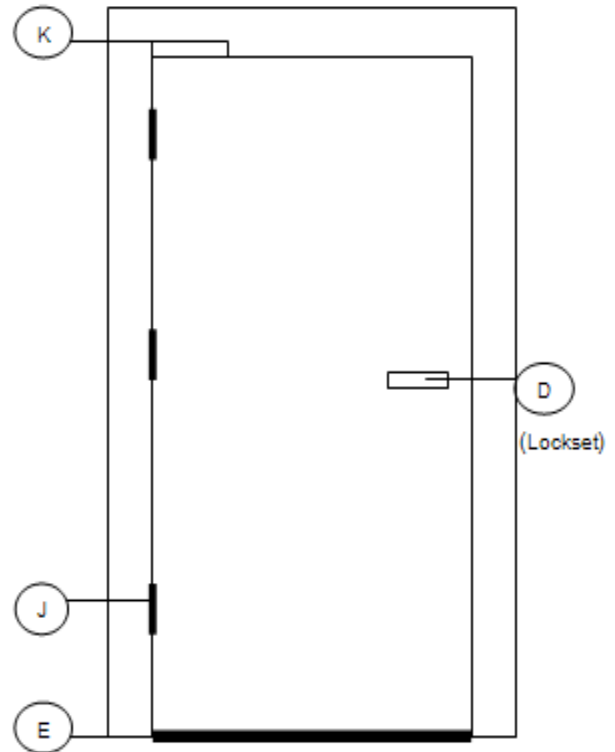
Security Hardware Set - 2

Materials:

- Doors must be constructed of 12-gauge steel clad hollow core metal of single solid core wood, 1 ¾ inches thick, and hung in hollow metal frames. There will be no windows.

Hardware:

- Install Lockset D
- Install Cylinder A, keyed individually under a CBP Master
- Install Door Hardware E
- Install Door Hardware F-1
- Install Door Hardware G
- Install Door Hardware J, if door swings outward
- Install Door Hardware K
- Install Door Hardware L, if door swings outward



DESCRIPTION OF COMPONENTS

Diagram Key No.	Quantity	Manufacturer	Description	Part/Model No.
(D) (Lockset)	1		Commercial Grade 1 – Mortise High Security Level Lockset with Deadbolt	
(E)	1		Door threshold	
(F-1)	1		Electric Strike for Deadbolt Lock Doors	
(G)	1		Balanced Magnetic Alarm Switch (BMS)	
(J)	Varies		Non-removable Hinge Pin (refer to Figure 2 for additional requirements)	
(K)	1	LCN	Pneumatic Door Closers	
(L)	1		Anti-Pry Strip	

Security Hardware Set 2





Security Hardware Sets		Door Hardware													Required Hardware															
Door Types	Exterior Doors	A	B	C	D	E	F-1	F-2	G	H	I	J	K	L	A	A	B	C	D	E	F	F	G	H	I	J	K	L	M	
		Astragal	Automatic Door Bottom	Door Coordinator	Door Stop	Door Threshold (Saddle)	Electric Strike for Deadbolt Lock Doors	Electric Strike for Non-Deadbolt Lock Doors	Balanced Magnetic Alarm Switch (BMS)	Flush Bolt	Latch Protector	Non-Removable Hinges (NRP)	Pneumatic Door Closer - Commercial Grade	Anti-Pry Strip	Access Control / Card Reader	UL 437 Compliant Lock Cylinder	Commercial Grade 1 - Mortise Lever Lockset - Classroom Function	Commercial Grade 1 - Mortise Lever Lockset with Thumb Turn Entrance Function	Commercial Grade 1 - Cylindrical Lever Lockset - Storeroom Function	Mortise High Security Lever Lockset with Deadbolt - Storeroom Function	Commercial Grade 1 - Mortise High Security Institutional Deadbolt Lever Lock	Commercial Grade 1 - Adams Rite Deadbolt/Dead Latch	Kaba Mas CDX-09 High Security Electomechanical Lock	High Security Exit Device with Deadbolt	Panic Exit Device	UL Group 1, Mechanical Combination Lock	Key Operated Padlock FF-P-2827 Compliant	GSA Approved High Security Padlock	GSA Approved Combination Padlock FF-P-110J Compliant	
SHW-1	Penetrator																													
SHW-2	Building Entrance																													
SHW-3	Emergency Exit																													
SHW-4	Overhead Colling Doors																													
Interior Doors																														
SHW-5	Interior-Penetrator																													
SHW-6	Counter-Terrorism Response suite (CTR)																													
SHW-6	Rover Coordination Center (RCC)																													
SHW-6	CBP Coordination Center (CCC)																													
SHW-6	Secondary Exam Podium and Baggage Belts Area (Port of Entry only)																													
SHW-7	CBP/APHIS Veterinary Services (VS) Bird Quarantine and Bird Holding Facilities (Port of Entry only)																													
SHW-8	Interview Rooms																													
SHW-9	Violator Waiting Area (Port of Entry only)																													
SHW-10	Violator Processing Area (Port of Entry only)																													
SHW-11	Search Rooms																													
SHW-10	Hold Rooms																													
SHW-12	Fraudulent Document Analysis Room (Port of Entry only)																													
SHW-12	Alien Baggage Storage																													
SHW-12	Joint Automated Booking System/Identification Room																													
SHW-12	Alien Documentation, Identifications, & Telecommunications Room (ADIT) (Port of Entry only)																													
SHW-13	Seizure Processing Area (Port of Entry only)																													

Legend	Required	Recommended	Either / Or	Optional
	R	E-1	E	X

Open the Door Switches Outward





APPENDIX 7.7: WINDOWS

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

I. GENERAL

A. Glazing Design

B. A necessary phase in designing glazing systems is developing the design criteria to describe what will happen when a bomb detonates near the structure. In this phase, it is important to define:

C. Performance goals to establish how the glazing will perform include:

1. Expected range of threats to establish the blast loading requirements.
2. Amount of damage allowed ensuring that the performance goals are met.

D. The design criteria will help establish a common basis of communication between security professionals and design engineers. Building functionality and various levels of performance for glazing systems are defined below:

1. Collapse Possible – Buildings designed for no protection against an explosive threat. Standard glazing and frame systems will be completely destroyed at this performance level.
2. Non-Repairable – Buildings designed for minimal protection against an explosive threat. The building will be heavily damaged but will not undergo “progressive collapse,” which has a dramatic impact on loss of life. This design allows for full disruption of the building functions and a high probability that the building will not be repairable. Standard glazing and frame systems will most likely fail at this performance level.
3. Extended Disruption – Repairable. Buildings designed for moderate protection against an explosive threat. The building will be damaged, but damage will be controlled and limited. The building will be out of service for an extended time (months to years) but probably will be repairable. All glazing systems will fail but fragments will be retained. Some frame failure will also occur at this performance level.
4. Repairable – Buildings designed for a high level of protection against an explosive threat. The building will be damaged but damage will be controlled and limited so that the building will be repairable in a matter of weeks to a few months. Most of the glazing systems will fail, but will remain anchored to the frame and wall.
5. Quickly Repairable – Buildings designed for a very high level of protection against an explosive threat. The damage will be very limited. Most functions will be restored in a brief time and the building will be fully operational in a matter of weeks. Some glazing systems will fail, but all will remain in place and resist the

[RETURN TO TOP](#)

effects of the design basis threat.

6. Essentially Operable – Buildings designed for maximum protection against an explosive threat. The damage will be of a superficial nature. All functions operable without significant interruption. Glazing systems are designed to withstand the applied pressures without failure.
- E. Design Threats. For the above performance categories there may be a range of possible threats. The threats are defined below.
1. Maximum Event. The largest explosive threat expressed as a net equivalent TNT hemispherical charge at a specified standoff distance.
 2. Controlling Event. An explosive threat source, expressed as a net equivalent TNT hemispherical charge at a standoff distance and location, which produces the most damage to the target. The controlling event may not be the largest event but is a function of explosive size, standoff distance, and location which produces the most damage.
 3. Design Events. A combination of explosive threats, expressed as net equivalent TNT hemispherical charge at a separation distance, which comprise a range of possible attack scenarios. This includes a variety of events of different sizes and locations.
- F. Based on the desired performance goals and threat, a structural engineer can define a set of response limits for the structure. Designing for operable/repairable construction can be very difficult and costly. Construction required protecting against a large explosive threat at close range would take the form of fully blast-hardened, bunker-type construction.
- G. Placement of the explosive is another major concern and all possible locations must be considered to find the critical location that produces the greatest damage to the structure.

II. GLAZING MATERIAL CHARACTERISTICS

- A. Glazing design is applicable to three performance levels: repairable, quickly repairable, and essentially operable.
- B. Glazing failure is a complex function dependent not only on the pressure-time loading but the glazing thickness, size, shape, type, and age. Flaws in the glazing material will cause the glazing to respond in an unpredictable manner, requiring the use of experiential procedures for glazing design.
- C. There are three types of glazing cross sections: monolithic, laminated, and insulated.

[RETURN TO TOP](#)

1. Monolithic cross sections consist of a single piece of glass or polycarbonate.
 2. Laminated cross sections consist of two or more plies of material bonded together with a tough interlayer material.
 3. Insulated cross sections consist of two or more sheets separated by a sealed airspace.
- D. Monolithic glass cross sections (not including polycarbonate) are very vulnerable to blast loads. Once the glass fails, there is nothing to keep the broken fragments from injuring personnel both inside and outside the structure.

1. The various types of materials available for use as monolithic glazing are:

- (a) Annealed glass
- (b) Heat strengthened glass
- (c) Thermally tempered glass
- (d) Chemically treated glass
- (e) Wire-reinforced glass
- (f) Polycarbonate
- (g) Acrylic

2. Annealed Glass:

- (a) Annealed glass is the most common form of glass available. Depending on manufacturing techniques, it is also known as plate, float, or sheet glass. During the manufacturing process, annealed glass is cooled slowly without tight controls. This process yields a product that has very little residual compressive surface stress and large variations in strength. When compared to tempered glass, annealed glass has relatively low bending strength.
- (b) Upon failure, annealed glass fractures into razor-sharp, dagger-shaped fragments. One-quarter inch annealed glass typically fails at 0.2-psi overpressure. Annealed glass should conform to American Society of Testing Materials (ASTM) Standard C1036.

3. Heat Strengthened Glass:

- (a) Heat-strengthened, heat-treated, or semi-tempered glass exhibits neither the higher tensile strength nor the small cube-shaped fracture pattern

associated with thermally tempered glass. The cooling process of heat strengthened glass is controlled more tightly than annealed glass, but less than thermally tempered glass. These results in large variations in the strength of heat strengthened glass as precompression levels vary. Heat strengthened glass is recommended for use in fire and environmental protection applications.

- (b) One-quarter inch heat strengthened glass typically fails at 0.4-psi overpressure. Heat strengthened glass should conform to ASTM C1048, Type HS.

4. Thermally Tempered Glass:

- (a) Thermally Tempered Glass (TTG) is the most readily available tempered glass on the market. It is manufactured from annealed glass (float, polished, or plate) by heating to a high, uniform temperature and then applying controlled, rapid cooling.
- (b) Thermally tempered glass is typically four to five times stronger than annealed glass.
- (c) Only tempered glass meeting the minimum fragment specifications of American National Standards Institute (ANSI) Z97.1-1984, American National Standard for Safety Glazing Materials Used in Buildings - Safety Performance Specifications and Methods of Test, or certified by the Safety Glazing Council (SGC), should be used.
- (d) The fracture characteristics of tempered glass are superior to those of annealed glass.
- (e) Due to the high strain energy stored by the prestressing, tempered glass will eventually fracture into small cube-shaped fragments instead of the razor-sharp, dagger-shaped fragments associated with the fracture pattern of annealed glass. However, even if the tempered glass breaks up initially into small fragments, high blast overpressures can propel these fragments at velocities high enough to constitute a severe hazard to personnel. One-quarter inch tempered glass typically fails at 0.8-psi overpressure.

5. Chemically Treated Glass:

- (a) Glass can be tempered chemically using a bath process; however, the fracture pattern resembles that of annealed glass. Most commercially available, chemically tempered glass for architectural purposes is manufactured from a soda-lime base. A common problem is surface flaws. The resulting stress will often induce premature failure. One-quarter inch chemically treated glass typically fails at 0.2-psi overpressure.

6. Wire-Reinforced Glass:

- (a) Wire-reinforced glass is a common glazing material. It consists of annealed glass with an embedded layer of wire mesh. Its primary use is as a fire resistant barrier. Wire-reinforced glass has the fracture and low strength characteristics of annealed glass and, although the wire binds some fragments, it still ejects a considerable amount of sharp glass and metal fragments. One-quarter-inch wire-reinforced glass typically fails at 0.2-psi overpressure.

7. Polycarbonate:

- (a) Thermoplastic polycarbonates are suitable for glazing systems designed to resist the effects of an explosion. Polycarbonate is available monolithically in thicknesses up to 1/2 inch. It can be fused together to obtain any thickness needed. In the 1/2-inch range of thickness, polycarbonate is twice as expensive as TTG glass but a third of the weight. Other than cost, polycarbonate's main disadvantage is that it is subjected to greater environmental degradation than glass, especially the effects of abrasion and degradation from ultraviolet radiation exposure.
- (b) Chemical coatings are available to protect polycarbonates from both abrasion and ultraviolet radiation. All exposed polycarbonates should have one of these surface coatings. With these coatings, a service life expectancy of 10 years or longer on externally exposed polycarbonate can be expected.
- (c) Polycarbonate is subject to high heat damage and tends to soften. Polycarbonate will burn when a flame is held to it; however, it will tend to extinguish when the flame is removed.
- (d) Rated as a class CC-1 material, it is much less combustible than acrylic plastic.
- (e) Local building codes should be consulted before polycarbonate is specified. Since polycarbonate can be difficult to break, local fire codes may require a percentage of polycarbonate glazing to pop out for emergency egress and venting.
- (f) Polycarbonate failure points are dependent on the thickness of the cross section. Having an adequate frame bite of 1 inch or more and allowing for expansion of the material are key factors in achieving satisfactory performance.

8. Laminated Cross Sections:

(a) Combining interlayer bonding materials with plies of glass, polycarbonate, or both, produces cross sections that perform well against blast loading. Laminated cross sections can include the following materials and combinations:

- Interlayer materials
- Thermally tempered laminated glass
- Laminated and fused polycarbonate
- Glass-clad polycarbonate
- Glass-clad ionomer

E. Interlayer Materials

1. Compatibility issues and cost drive selection of interlayer material. Consideration must be given to incompatibilities when bonding non homogeneous materials. As a consequence, only Plasticized Polyvinyl Butyral (PVB) and Aliphatic Urethane are used for the lamination of security glazing.
2. PVB is used universally by the glazing industry for laminating glass products together.
3. PVB is the most cost-effective interlayer material available. There are three grades available: architectural, aircraft, and automotive. Architectural grade PVB is the most widely used. Aircraft grade PVB is approximately twice as stiff as the architectural grade but costs about four times more. Automotive grade is the same cost and thickness as architectural grade PVB. The environmental durability of PVB is a known and proven quantity. Long-term use in automotive and aerospace industries indicates that few, if any, problems of environmental degradation will be encountered.
4. Polyether urethane interlayer material can also be used to laminate glass or polycarbonate materials. Urethane material has better viscoelastic (remain flexible) behavior at low temperatures than PVB material. Currently, there are only two interlayer materials that are compatible with polycarbonate for use in the lamination process. These materials are urethane and Copal_ (available only with General Electric polycarbonate glazing laminates). Polyether urethane is the only type of interlayer material that is commercially available to all laminators for laminating polycarbonate.

[RETURN TO TOP](#)

F. Thermally Tempered Glass (TTG)

1. TTG laminates use PVB or urethane for lamination.
2. Frame compatibility and light transmissibility establish a laminated glass thickness of 2.5 inches as a practical upper bound. However, if special circumstances warrant, thicknesses up to 5 inches are available.
3. When subjected to blast overpressure, laminated TTG will exhibit strength and behavior between that of a set of stacked glass sheets and a monolithic sheet, depending on temperature and duration of load. Both the Government and private industry use design strength of a PVB glass laminate at 75 percent that of a monolithic plate of the same thickness. For this load condition, the laminate is at ambient temperature.
4. A laminated, blast resistant glazing cross section offers a significant fragment retention advantage over monolithic glass. If glass failure does occur (which could happen if blast loads exceed the initial design), the interlayer material will retain most of the glass fragments. If catastrophic failure occurs from excessive blast overpressure, increased fragment retention can be obtained by installing a catch bar or fragmentation curtains on the interior of the glazing system.

G. Laminated and Fused Polycarbonate

1. Thickness of polycarbonate glazing exceeding 1/2 inch can be achieved by lamination or fusion (melting together). Whenever large thicknesses of polycarbonate are anticipated, a design review should be considered to determine if the frame and building will accept the design.
2. Polycarbonate is a moderate temperature insulator, and a large temperature differential can lead to delamination of a laminate or stress hardening of the monolithic material. This results in a phenomenon known as crazing or small cracks on the surface. Polycarbonate and urethane under blast overpressure loading are similar enough for a laminated cross section to be considered monolithic for design purposes.

H. Glass-Clad Polycarbonate (GCP)

1. Glass-clad polycarbonates are primarily designed to protect against forced entry and ballistic attacks. If a glass-clad polycarbonate was intended to resist a bomb attack, a conservative approach would be to calculate the resistance for either the glass or polycarbonate material, but not a combination of both. There are two configurations for glass-clad polycarbonate glazing cross sections, symmetrical and asymmetrical. Symmetrical cross sections are more environmentally stable.
2. Environmental conditions are an important consideration for laminates

- incorporating a polycarbonate core thickness greater than 5/8 inch. Because polycarbonate has a coefficient of expansion eight times that of glass, the interlayer material at the glass-polycarbonate interface must be thick enough to allow for movement. The de facto industry standard at the glass polycarbonate interface is 0.050 inch.
3. Aspect ratios (ratio of length to width) are an important consideration and must be kept as close to one as possible. Avoid designing glazing “ribbons” (long, narrow window openings) because they tend to create unbalanced stresses relative to the long and short sides of a glazing, which can pull the laminate apart.
- I. Glass-Clad Ionomer
 1. Glass-clad ionomer cross sections are produced only in a symmetrical arrangement. They are designed primarily for ballistic and forced entry resistance. There is little data available on the performance of glass-clad ionomer in resisting blast loads.
 - J. Other Materials
 1. Materials such as glass block could be substituted for traditional windows. Glass block has a substantially higher resistance compared to conventional glass panes. In this manner the windows can be upgraded to strengths at or near conventional wall strengths. There is little data available on the performance of glass block in resisting blast loads.
 - K. Fragment Retention Film (FRF)
 1. Thin plastic film that can be applied to standard annealed and tempered glass to retain fragments during an explosion, FRF is an injury mitigation measure and not intended to provide protection against the pressure effects of an explosion other than to reduce exposure to glass fragments. FRF is one of the most cost-effective methods for mitigating the effects of glass breakage in existing structures during an explosion.
 2. Select 10-mil film in a daylight (to the edge of frame) application regardless of loading conditions if fragment retention is the primary goal.
 3. Install a catch bar or single side (top) mechanical anchoring system for all daylight applications.
 4. For insulated (air-gap) glass installations and conditions where maximum retention of fragments is required, use a frame anchoring system (two-sided) for the film if existing frame conditions permit.

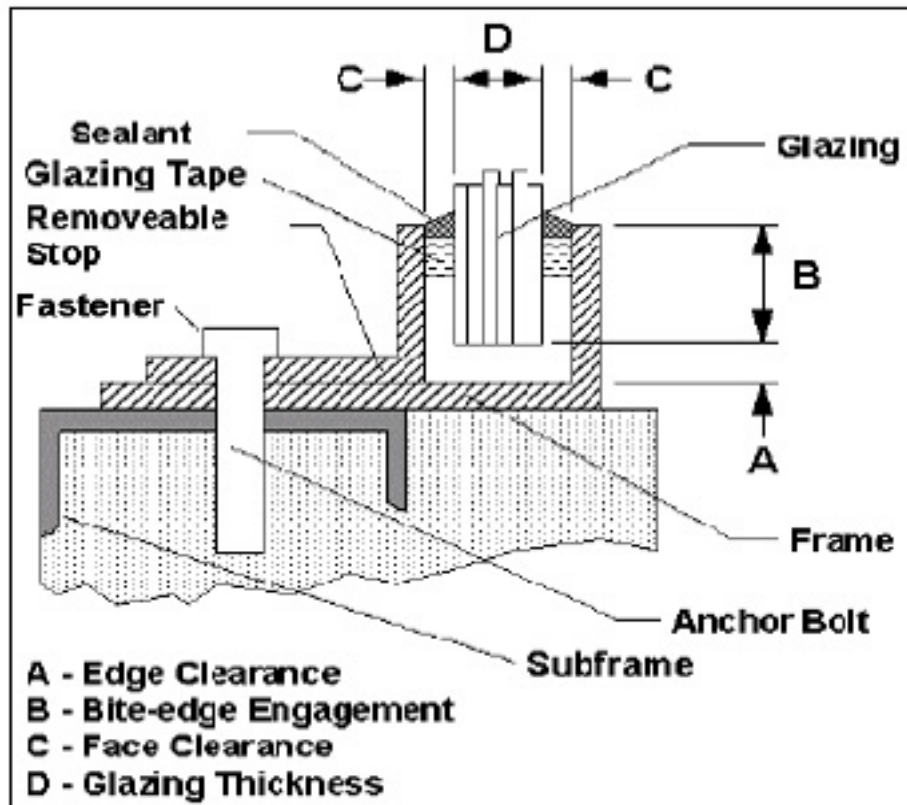
(a) See [Uses of Fragment Retention Film](#) for greater detail.

III. WINDOW FRAMES

A. Framing System

1. Window glazing frames provide a connection between the building envelope and the glazing material. This connection must be strong enough to transfer the edge load of the glazing into the building. A basic frame system consists of a main frame, sub frame, removable stop, fasteners, glazing tape, and sealant. More elaborate frame systems also include sub frames (see [Figure 1](#)).

Figure 1: Typical Frame Cross-Section



B. Main Frame

1. A main frame can be made from aluminum, aluminum with steel inserts, or steel. The frame must provide a system of drainage channels and flashing to allow water accumulation discharge to the exterior.
2. Operable frame designs, which allow the window to be opened, are not recommended for security applications where protection against explosive threats is a concern. The frame bite should be at least 1 inch or the minimum determined by the glazing manufacturer or design engineer. If the bite is sufficient to hold the glazing and resist the blast load, all pressure is transferred through the frame to the wall. This can be sizeable load acting on the wall, which

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

is additionally weakened by the presence of the opening. For high pressures, additional structural reinforcing around the window may be required.

C. Sub frame

1. A matching sub frame and outer frame are recommended to resist explosive effects. Sub frames are mounted in the concrete formwork prior to pouring concrete. Anchorage is embedded with studs welded directly to the building reinforcing steel. After pouring the walls, outer frames and glazing can be installed in the sub frames. A blast consultant is recommended for analyzing and designing the sub frame and anchorage system.

D. Removable Stop

1. The removable stop is a component of the frame that holds the glazing in place. The purpose of the removable stop is to allow installation of the glazing into the frame.
2. Better security integrity is achieved when the removable stop is on the interior side of the glazing. The removable stop must be capable of resisting the entire load collected by the glazing, both in positive inward loading and in negative rebound outward loading.

E. Glazing Tape and Sealant

1. Glazing tape and sealant provide a cushion between frame material and glazing to prevent glass breakage from thermal expansion, settling, and wind loads. Glazing tape and sealant support the glazing laterally. They set and maintain the face clearance between the frame bite and the glazing face. Setting blocks are used to establish and maintain the edge clearance of a glazing. The window seals should preclude the leakage of high blast pressures into the building.
2. A sealant provides resistance to environmental degradation effects around the edge of a glazing. Security laminates should be wet sealed with silicone sealant to obtain optimum performance in security applications.

F. Frame Anchorage

1. Blast resistant window framing must be capable of resisting the load transferred from the glazing. This requirement translates to rigid frames and frame-to-wall interfaces and flatness of the frame and glazing assembly. If the frame system is skewed or out of plane, the glazing can develop unbalanced stresses when loaded and fail prematurely.
2. Aluminum frames with steel sub frames can be used for small blast loads less than 5 psi.

(a) Above 5 psi, the entire frame system must be constructed from steel members.

3. Some frame designs for concrete construction use anchor bolts for a dual purpose. They serve to anchor the frame to the structure and as fasteners for the removable stop. Since a glazing must be removable without destroying the wall, careful consideration must be exercised when selecting the type of anchor bolt. Sleeved anchors and compression bolts, which cannot be reinstalled, are unacceptable.

G. Frame Design

1. The window frame must absorb the full load of the glazing pane (created by the blast pressure) for reliable performance. Unless this is done, frame deflections can induce higher tensile stresses in the glazing pane and reduce its ability to resist blast loading. Frame members must also resist the blast load directly applied on all exposed areas.
2. Selection and evaluation procedures for frames, anchorage, and walls are complex engineering processes and beyond the scope of this Guide. The assistance of a structural engineer with experience in blast overpressure analysis and design to carry out a comprehensive analysis of these components is highly recommended.

H. Security Glazing Installation Notes and Recommendations

1. All security glazing cross sections should be fixed to maximize their effectiveness.
2. Movable glazing that is open when a blast occurs can leave assets and personnel vulnerable to the forces resulting from the explosion. Acceptable glazing material for blast resistance in new construction includes laminated annealed glass, laminated thermally tempered glass, laminated chemically tempered glass, monolithic polycarbonate and air gap polycarbonate, and glass systems (polycarbonate laminates with glass on the outboard face separated by an air gap).
3. Annealed glass, monolithic thermally tempered glass, heat-treated (semi-tempered) glass, wire-reinforced glass, soda-lime-based chemically tempered glass, and acrylic sheets are unacceptable glazing materials for new construction where explosive blast loading is a concern. Insulated or air gap glazing systems provide significant heat transfer benefits and associated cost savings. Typically, an air gap glazing can reduce the temperature gradient inside a structure by as much as 50 percent. This is an important consideration for security applications requiring larger thicknesses of polycarbonate, where thermal stresses can significantly reduce the life of a product.

[RETURN TO TOP](#)

IV. BALLISTIC THREAT CHARACTERISTICS

A. A ballistic threat depends on caliber, type, shape and weight, impact velocity, angle of impact, muzzle energy, multiple versus single impact, and target range. The most probable threat is from pistol, rifle, submachine gun, shotgun, or automatic weapons fire.

1. Caliber – The caliber of a bullet refers to its diameter and is expressed in either decimals of an inch (caliber) or in millimeters. Typical examples include the 0.303-caliber and 7.62-mm NATO Ball.

B. Bullet Characteristics

1. Bullet characteristics vary as follows:

(a) Armor-Piercing (AP) - A bullet with a hardened metal core, a soft metal envelope, and a copper bullet jacket. When the AP bullet strikes armor, the envelope and jacket are stopped, but the armor-piercing core continues forward to penetrate the armor. The AP bullet is characterized by high accuracy in flight and high velocity.

- If AP is considered a threat, windows should be eliminated since they cannot cost-effectively defeat this threat.

(b) Ball - A non-armor-piercing bullet having a lead or mild steel core.

(c) Full Metal Jacket - A copper outer shell that encapsulates the core and increases accuracy and penetration characteristics.

C. Bullet Configurations

1. The different bullet designs are spire point (long, acutely pointed), round nose, flat point, full metal jacket (completely copper coated), hollow point, short jacket (copper coated at tip), cast bullet, and wad cutter. Ballistic performance during flight and on impact is sensitive to a projectile's shape and construction (e.g., whether or not the bullet is jacketed; the length, thickness, and hardness of the jacketed material; the presence of a hollow nose, a cavity, and hollow base; and the hardness of the lead).
2. A pointed projectile will initiate fracture of the target. By comparison, a flat-nosed projectile would favor plugging of the target around the projectile as it advances into the target. A lighter bullet will slow down quickly on impact while a heavier bullet will penetrate further into the target. An AP-type bullet has a greater capacity to penetrate than the ball type because the AP bullet has a hardened steel core that resists deformation on impact.

D. Oblique Attack Effect

1. Penetration resistance is affected by the angle at which a projectile strikes the target. A projectile impacting the surface at an angle approaching parallel to the surface must travel through more material to penetrate.

E. Projectile Energy

1. In security glazing, the initial impact layer must be hard to deform the projectile on initial impact. This allows the tough polycarbonate layer behind to “catch” the bullet before it penetrates the cross section.

F. Multiple Impacts

1. The effect of multiple hits depends on separation of the points of impact and the degree to which the glazing material is damaged by preceding impacts. Where a small area of dispersion of successive hits fall within the crater of the first projectile, the possibility of penetration increases.

Table 1: Ballistic Tactic Threat Ballistic Severity Levels

Threat Severity Level	Standard	Caliber Weapon	Bullet Weight and Type	Minimum Velocity (ft/s)	Number of Shots Resisted by Test Article
Low	UL-752-95* Level 1	9 mm	124 grain, full metal jacket with lead core	1,175	3
Medium	UL-752-95* Level 2	.357 Magnum	158 grain, jacketed lead soft core	1,250	3
	UL-752-95* Level 3	.44 Magnum Revolver	240 grain, lead semi-wadcutter gas checked	1,350	3
High	UL-752-95* Level 4	.30 Caliber Rifle	180 grain, lead core soft point	2,540	1
	UL-752-95* Level 5	7.62-mm Military Rifle	150 grain, lead core full metal jacket, military ball.	2,750	1
	UL-752-95* Level 6	9 mm	124 grain, full metal jacket	1,350	5
Supplement Shotgun (High)	UL-752-95* Supplementary shotgun	12-ga.	00 lead buckshot (12 pellets) or	1,200	3
			437 grain rifled lead slug	1,585	3
Very High	UL-752-95* Level 7	5.56-mm Military Rifle	55 grain, lead core full metal jacket, military ball	3,080	5
	UL-752-95* Level 8	7,62-mm Military Rifle	150 grain, lead core full metal jacket, military ball	2,750	3
*Underwriters Laboratories, Inc., Standard for Bullet-Resisting Equipment					

V. THREAT SEVERITY LEVELS

- A. Low Threat Severity Level – The low threat severity level is ANSI/Underwriters Laboratories (UL) Level 1 described in ANSI/UL-752. This threat normally would be employed against facilities when the main objective of the attacker is to persuade someone to turn over items of high value, such as cash or drugs.
- B. Medium Threat Severity Level – The medium threat severity levels are ANSI/UL Levels 2 & 3 described in ANSI/UL-752. This threat normally would be employed when the attacker knows that ballistic resistant glazing is installed.
- C. High Threat Severity Level –The high threat severity levels are ANSI/UL-752 Levels 4, 5, and 6. This threat would normally be employed for sniper situations and conditions where 9-mm automatic weapons might be expected. ANSI/UL-752 also describes the high severity threat level as a 12-gauge 437-grain rifled slug and double 0's buckshot.
- D. Very High Threat Severity Level – The very high threat severity level, 5 shots from a 5.56 or 7.62 NATO Ball Military round, is described in ANSI/UL-752 as Levels 7 and 8. This threat normally would be employed for locations where paramilitary attacks are expected.

VI. DESIGN OF BALLISTIC RESISTANT GLAZING

A. Ballistic Resistance

- 1. The term “ballistic resistance” denotes protection against complete penetration, passage of projectiles, or spallation (chip or splinter off the backside) of the protective material to the degree that injury would be caused to a person standing directly behind the bullet-resisting barrier. This definition is set forth in the ANSI/UL-752, “Standard for Bullet-Resisting Equipment.” The ANSI/UL definition of bullet-resisting glazing material specifies that there should be no penetration of the projectile. Fragments of the projectile or fragments should not penetrate the glazing assembly with sufficient force to embed into or damage 1/8-inch-thick corrugated cardboard indicators placed a distance of 18 inches behind the protected side of the test sample.

B. Ballistic Resistant Glazing

- 1. Ballistic resistant glazing is composed of materials with the dual properties of being virtually transparent while having a resistance to penetration of small-arms projectiles and fragments. In general, ballistic glazing is a laminated composite of glass and elastomers. A potential disadvantage of glass is breakup on projectile impact and the subsequent shattering and formation of sharp, needle-like splinters. Safety glass, which consists of two or more sheets of tempered glass bonded together by synthetic resin, produces cube-shaped pieces when

[RETURN TO TOP](#)

fractured that usually have rounded edges. The energy absorbing mechanics of polycarbonate materials offer an advantage over glass, which will spall on impact. Polycarbonate can often be used to reduce shatter. When combined with glass as a spall shield or a laminated glass/plastic configuration (with polycarbonate on the inside face), polycarbonate can inhibit the shattering of the glass by containing the glass particles. The suppression of spallation is a powerful method that can be used to increase the impact resistance of ballistic resistant glazing. A laminated and bonded composite cross section consisting of TTG and polycarbonate layers provides visual clarity and tested resistance to small-arms projectiles.

VII. GLAZING SELECTION STRATEGIES

- A. Selection of security glazing systems for ballistic resistance can include several strategies either alone or in combination, including concealment of the asset, providing resistance to the anticipated threat using glazing systems, or using alternative ballistic resistant systems.
1. Concealment - The strategy for the low level of protection is concealment of assets by elimination of sight lines. Concealment provides a low-cost and effective solution. Concealment can be achieved by arranging windows or locating assets in visually inaccessible places and the using window-obscuring treatments such as reflective Mylar film, blinds, or draperies. Concealment can also be achieved through the use of standoff walls that shield the target from direct line-of-sight fire. Wall systems selected from [Table 2](#) can be used for this purpose. The benefit of concealment is that aggressors usually will not fire at targets they can not see.
 2. Resistance - Use bullet resistant windows for a high level of protection. Bullet resistant windows essentially constitute transparent armor. As for all attack resistant construction, the degree of protection provided by a bullet resistant window should equal that of the adjoining wall system.
 3. Alternate Systems - Components such as bullet resistant window shutters can be combined with obscuring window treatments and used on conventional windows. This allows the building occupant to control the level of protection.
- B. Design Considerations for Bullet Resistant Windows:
1. If bullet resistance is required for a window, select a manufactured unit or design an assembly using tested materials that are manufactured, marketed, and certified as ballistic resistant. The various materials available and issues that should be considered in selecting or designing a bullet resistant window are discussed below.

[RETURN TO TOP](#)

- (a) Glazing Materials - Ballistic resistant glazing systems can provide protection for all threat severity levels, although glazing which resists armor-piercing rounds may not be available from all manufacturers. The most significant considerations for the glazing include cost; weight, thickness, and early replacement from environmental considerations or abuse. When selecting a security glazing system to defeat an identified threat, it is important to also consider the frame and surrounding wall systems.
- (b) Frames - Frames specified for ballistic resistant glazing systems must be capable of resisting the same ballistic threat as the glazing and surrounding wall system. Bullet resistant window frames are fabricated from various types and grades of aluminum, carbon steel, or stainless steel, and they are typically reinforced internally with armor-grade steel shapes. Aluminum is also used by some manufacturers to improve appearance or for corrosion resistance. Custom fabricated wood-clad or wood-trimmed assemblies may be available from some manufacturers when aesthetic concerns warrant the additional (and considerable) expense. The frame, sash, mullions (vertical member between window lites), and muntins, if used, must also be designed to resist the identified threat.
- Fixed windows may be fabricated of steel channels or angles to provide integral anchorage, but the steel must be specified as bullet resistant. Specify bullet resistant frame and sash material either by the tested threat severity level or by an actual material designation. Sills for exterior use should be designed to allow drainage. Coordinate window design with glazing manufacturers to ensure adequate size, bite, glazing bead, and sealant compatibility. Eliminate weak areas in the assembly such as visible connectors or hardware. Sashes and glazing stops should not be removable from the outside. Where possible, use fixed sashes to eliminate hinge and lock components. Mullions and muntins are rarely used in bullet resistant windows because to be effective, particularly against higher ballistics threats, the sections must be extremely heavy, which may detract from the window design.
 - Also, when the glazing is bullet resistant glass, it has a tendency to completely disintegrate when struck by bullets. For best performance, eliminate mullions and muntins and size lites in accordance with the manufacturer's recommendations.
- (c) Anchorage - Methods of anchorage depends upon the type of window frame and the wall construction in which the window is anchored. Methods include masonry anchors, wood or steel stud anchors, silicone adhesives, gasket systems, and curtain wall glazing systems. Windows may also

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

be detailed into a wall system such that the wall provides an integral stop, although moisture entrapment is a concern with this approach. Manufacturers of window assemblies recommend anchorage methods that provide adequate support and protection for the window's threat resistance.

- (d) Construction - Manufacturers use different thicknesses of glazing materials and vary the frame and sash details to meet the same threat levels. Because design details, structure to support the increased weight of bullet resistant materials, and anchorage requirements influence wall construction, consult at least three manufacturers for specific information on specific window designs to meet job-specific criteria. Detail the window installation accordingly and include governing characteristics in window specifications (such as the maximum weight of the window). Consider the weight of bullet resistant windows designed to meet a specific threat severity level when designing the surrounding wall structure.
- (e) Wall Systems - Wall systems described in [Table 2](#) will provide equivalent penetration resistance at the threat severity levels listed. When selecting security glazing systems, it is important to consider the ability of the surrounding wall system to resist the same level of threat. If this factor is not considered, the value of an expensive glazing system could be substantially reduced.

Table 2: Minimum Thickness for Ballistic-Resistant Walls

Threat Severity Level	CMU (grouted) or Brick Thickness (in.)	Reinforced Concrete (3,000 psi) Thickness (in.)
Low	4	2
Medium	4	2-1/2
High	8	4
Very High	(a) or (b)	8

(a) 4-inch solid C MU, 3/4-inch rigid urethane, and 8-inch grout-filled CMU.

(b) 6-inch, grout-filled CMU, insulation plus 6-inch grout-filled CMU.

VIII. TYPICAL THICKNESSES FOR BALLISTIC RESISTANT GLAZING

- A. [Tables 3, 4, 5](#) and [6](#) provide information on typical cross sections that would normally be required to resist specific threat levels. These tables should be used for reference and cost estimating purposes only. Any material must be independently tested to UL standards before use to ensure performance of the cross section at the desirable level.

Table 3: Typical Thickness for Low Threat Severity Level Ballistic-Resistant Glazing Cross Sections

Type	Cross Section (in.)
Air Gap	1/4 Laminated strengthened glass 1/4 Air gap 3/8 Laminated polycarbonate
Glass-Clad Polycarbonate	1/4 Laminated chemically strengthened glass 1/4 Laminated polycarbonate
	1/4 Laminated strengthened glass 3/8 Laminated polycarbonate
	3/16 Strengthened glass 1/4 Annealed glass 3/8 Laminated polycarbonate
Laminated Glass	1-1/8 Laminated annealed glass
Laminated Polycarbonate	1 Laminated polycarbonate

Table 4: Typical Thickness for Medium Threat Severity Level Ballistic-Resistant Glazing Cross-Section

Type	Cross Section (in.)	
Air Gap	1/2 Laminated strengthened glass 1/4 Air gap 1/2 Laminated polycarbonate	
	1/4 Laminated strengthened glass 1/4 Air gap 3/4 Laminated polycarbonate	
Glass-Clad Polycarbonate	3/8 Laminated chemically strengthened glass 1/2 Laminated polycarbonate	
	1/4 Strengthened glass 3/8 Annealed glass 3/8 Laminated polycarbonate	
	7/8 Laminated annealed glass 1/4 Polycarbonate	
	7/8 Annealed glass 1/4 Polycarbonate	
	1/8 Strengthened glass 5/16 Annealed glass 1/2 Laminated polycarbonate	
	1/8 Chemically strengthened glass 5/8 Laminated annealed glass 3/8 Polycarbonate	
	Laminated Glass	1-3/4 Laminated annealed glass
	Laminated Polycarbonate	1-1/4 Laminated polycarbonate

Table 5: Typical Thickness for High Threat Severity Level Ballistic-Resistant Glazing Cross-Section

Type	Cross Section (in.)
Air Gap	3/4 Laminated strengthened glass 1/4 Air gap 15/16 Laminated polycarbonate
Glass-Clad Polycarbonate	1/8 Strengthened glass 3/4 Laminated annealed glass 3/8 Polycarbonate
	1 Laminated annealed glass 1/4 Polycarbonate
	1-1/8 Laminated strengthened glass 3/16 Polycarbonate
	1-1/8 Laminated annealed glass 3/8 Laminated polycarbonate
Laminated Glass	2 Laminated annealed glass

Table 6: Typical Thickness for Very High Threat Severity Level Ballistic-Resistant Glazing Cross-Section

Type	Cross Section (in.)
Glass-Clad Polycarbonate	1-5/8 Laminated annealed glass 1/4 Polycarbonate
	1/8 Strengthened glass 1-1/8 Laminated annealed glass 3/16 Polycarbonate

IX. SPECIFYING BALLISTIC GLAZING

A. Performance Specifications

1. Use performance-based specifications whenever possible. Include all relevant performance criteria such as ballistic resistance, thermal transmission, and sound transmission. Glazing should be specified for exterior or interior use, depending upon the specific application. Indicate which specific ballistics test standard and threat severity level must be met. Terminology
2. Specify “bullet-resistant glazing,” because specifying “bullet-resisting glass” precludes the use of plastics, composites, and multi-layer systems. Do not use

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

the term “bulletproof” as a performance requirement because no glazing systems are bulletproof.

B. Test Standards

1. Clearly describe the test or performance standard that must be met. Because most standards are subject to periodic revisions, the designer should obtain the most recent revision and develop specifications accordingly. Although using the threats listed in UL-752 is recommended, other design threats can also be specified. When non-standard ballistic threats are specified, include information on the:
 - (a) Weapon
 - (b) Bullet type
 - (c) Velocity
 - (d) Distance between the weapon and the test material
 - (e) Number of shots required
 - (f) Interval between each shot
 - (g) Temperature requirements of the sample
 - (h) Angle at which the bullet is to strike the sample
 - (i) Failure criteria when using non-standard threats, it is recommended that an independent testing laboratory be required to test the window and that the manufacturer be required to submit certified test results to the designer.

C. Tested Windows

1. Specify windows tested to a recognized standard (such as UL-752) when possible. Not all test standards require complete testing of all window components. Some standards test only the glazing. Some do not designate where specific rounds are to be placed in the tests. Carefully review selected test standards before using them. Verify that the standard meets the design criteria required. If not, add additional testing or certification requirements to the specification.
2. If the costs of such job-specific testing are prohibitive or unwarranted, inform the facility user that only certain components will be certified as ballistic resistant.

D. Installation

1. Indicate anchorage into surrounding construction and coordinate instructions for window installation with the manufacturer.

E. Markings

1. Some ballistics test standards require that each manufactured unit be permanently and legibly marked or labeled with the manufacturer's name, date of manufacture, ballistics rating, strike face (if any), and exterior/interior application. Bullet resistant windows should be checked for required markings in the field prior to installation. Markings or labels may be omitted or installed to be visible only from the protected side, if required by specification, so the window's resistance level will not be divulged. Consult the facility user for a preference as to whether or not marks or labels are required.

X. WINDOW SYSTEMS DESIGNED TO RESIST FORCED ENTRY

A. Levels of Threat for Forced Entry

1. There are five threat levels normally associated with forced entry protection. Only three of these threat levels are appropriate for security glazing systems: very low, low, and medium. Moving from low to very high threat severity levels increases the required technical skill or sophistication level of the adversary.
2. Very Low Level Threat. Aggressor uses quiet methods of entry such as saws and hand drills, or a single blow to break the glass using rocks, etc.
3. Low Level Threat. Aggressor uses low-observable hand tools.
4. Medium Level Threat. Aggressor uses unlimited hand tools (high and low observable) and limited battery powered tools.
5. High Level Threat. Aggressor uses unlimited hand, power, and thermal tools. Glazing systems are not available to protect against this level of attack.
6. Very High Level Threat. Aggressor uses unlimited hand, power, and thermal tools, plus explosives. Glazing systems are not available to protect against this level of attack. While security glazing systems will provide some resistance to threat levels above medium, they are not recommended for these applications. Specifying windows to resist the high or very high threat severity levels is not possible because there are no glazing systems currently available that can cost-effectively resist the combination of power and thermal tools, and powerful explosive breaching charges associated with these threat levels.

B. Selection of Glazing Systems for Forced Entry Protection

1. To specify a security glazing cross section, first identify the forced entry threat severity level the window must resist (very low, low, or medium). As previously mentioned, there is currently no security glazing system available that will cost effectively withstand the high and very high threat levels.
2. Very Low Forced Entry Threat Severity Level
 - (a) Install 10-mil fragment retention film (FRF) as described.

C. Low Forced Entry Threat Severity Level

1. Select a tested cross section from [Table 7](#) that will provide protection against a low threat severity level. Ensure the wall system for the structure is at least equal to one of the wall cross sections listed in [Table 8](#).
2. Specify the following minimum frame requirements:
 - (a) Frame Thickness = 1/4-inch steel
 - (b) Removable Stop Thickness = 3/16-inch steel
 - (c) Bite Depth = 1-inch
 - (d) Glazing Rabbet Depth = 1-1/4 inches
 - (e) Width Between Frame Members = 42 inches
 - Specify a minimum 3/8-inch lag bolt with a 3-inch embedment into the structure surrounding the frame.
 - Lag bolt spacing must be a minimum of 9 inches from the frame corner to the first bolt on each side of the corner and a minimum of 18 inches on center between all other bolts.
 - Removable stop anchor bolts shall be 3/8-inch, shouldered at least two per side.
 - Spacing for stop anchor bolts will be a minimum of 9 inches from the frame corner to the first bolt on each side of the corner and a minimum of 18 inches on center between all other bolts.

D. Medium Forced Entry Threat Severity Level

1. Select a tested cross section from [Table 9](#) that will provide protection against a low threat severity level. Ensure the wall system for the structure is at least equal to one of the wall cross sections listed in [Table 10](#).

[RETURN TO TOP](#)

2. Specify the following minimum frame requirements:

- (a) Frame Thickness = 1/4-inch steel
- (b) Removable Stop Thickness = 3/16-inch steel
- (c) Bite Depth = 1 inch
- (d) Glazing Rabbet Depth = 1-1/4 inches
- (e) Width Between Frame Members = 42 inches
 - Specify either a 1/2-inch, one-piece expansion sleeve with a 3-inch embedment into the structure surrounding the frame; or a 3/8-inch taper bolt with a 3-inch embedment into the structure surrounding the frame.
 - Bolt spacing must be a minimum of 6 inches from the frame corner to the first bolt on each side of the corner and a minimum of 12 inches on center between all other bolts.
 - Removable stop anchor bolts shall be 3/8-inch, shouldered at least two per side.
 - Spacing for stop anchor bolts will be a minimum of 9 inches from the frame corner to the first bolt on each side of the corner and a minimum of 18 inches on center between all other bolts.

Table 7: Minimum Glazing Requirements for Low Threat Severity Level

Type	Cross Section (in.)
Air Gap	1/4 Laminated annealed glass, 1/4 Air gap, 1/2 (13) Laminated polycarbonate
Extruded Ionomer	3/16 Annealed glass, 1/2 Extruded ionomer, 1/8 Annealed glass
Glass-Clad Polycarbonate	3/16 Annealed glass, 3/8 Polycarbonate, 3/16 Annealed glass
Monolithic Polycarbonate	3/8 Polycarbonate

Table 8: Minimum Wall Thickness for Low Threat Severity Level

Wall Construction	Minimum Wall Thickness (in.)
Wood Frame	1-inch tongue-and-groove wood siding over 3/4-inch plywood on 2-inch by 4-inch stud framing with plaster board on the interior
Reinforced Grout-Filled Concrete Block	6-inch w/number 4 reinforcing bars in each cavity and horizontal joint reinforcement every course
Reinforced Concrete	4-inch with 6 inches by 6 inches welded wire mesh at center line

Table 9: Minimum Glazing Requirements for Medium Threat Severity Level

Type	Minimum Thickness (in.)
Air Gap	1/4 Laminated annealed glass, 1/4 Air gap, 1-1/8 Laminated polycarbonate
Extruded Ionomer	7/8 Laminated annealed glass, 1 Extruded ionomer, 3/32 Annealed glass
Glass-Clad Polycarbonate	3/16 Strengthened glass, 1/4 Annealed glass, 3/8 Laminated polycarbonate
Laminated Polycarbonate	1-1/4 Laminated polycarbonate

Table 10: Minimum Wall Thickness for Medium Threat Severity Level

Wall Construction	Minimum Wall Thickness (in.)
Reinforced Grout-Filled Concrete Block	8-inch with number 4 reinforcing bars through each cavity and horizontal joint reinforcement at each course
Reinforced Concrete	6-inch with number 4 reinforcing bars at 6 inches on center each way

XI. INSTALLATION OF SECURITY GLAZING SYSTEMS FOR FORCED ENTRY

A. Frames, Sash, Mullions, and Muntins

1. Fully grout frames to minimize access to anchors and make the frame more rigid, or use anti-spreading frame reinforcements at maximum 8-inch intervals.
2. Provide heavy or reinforced sash, frames, and other elements rated for the appropriate threat severity level and delay time.
3. Conceal exterior fasteners or use tamper-proof fasteners.
4. Use non-removable exterior stops.

B. Operators and Hardware

1. Where possible, use fixed sash (inoperable) windows. If windows must be operable, provide key-operated dead bolt locking devices on the inside face.

C. Anchorage

1. Conceal fasteners from the exterior or use tamperproof fasteners, provide non-removable exterior stops, grout frames to minimize access to anchors, and provide a steel channel along the inside and out side of the window opening to minimize access to anchors by thermal or power cutting tools.

D. Fragment Retention Film

1. Fragment Retention Film (FRF) is an optically clear tough film attached to the inside of a glass surface with a strong, pressure-sensitive adhesive. Films are composed of polyester, polyethylene terephthalate, or composite materials. FRF is also known as shatter resistant film, safety film, or protective film.

E. Uses of Fragment Retention Film

1. Airborne glass fragments produced during an explosion or other type of attack pose a significant danger to occupants of a building. Tests on annealed glass subjected to explosion show that a large number of small, sharp fragments are disbursed throughout the test area at high velocity. Tests on thermally tempered glass show similar results, although there are typically more fragments that are not quite as sharp, but just as deadly.
2. FRF offers a relatively inexpensive solution that can reduce the destructive capability of glass fragments. FRF is particularly beneficial for retrofitting existing glass windows. FRF provides no added value on polycarbonate glazing. FRF provides some protection from glass hazards when subjected to ballistic attack and added protection (delay time) when attacked with simple hand tools. It will also provide protection against injury from glass fragments during earthquakes, hurricanes, and other extreme weather conditions. When combined with solar tinting, it can also provide ultraviolet protection and improved energy efficiency.

F. Ballistic Attack

1. When subjected to ballistic impact (or shrapnel), the projectile creates a hole in the FRF reinforced glazing approximately the size of the projectile, leaving the remainder of the glass intact. The glass around the impact area continues to adhere to the FRF so fragmentation is minimized. FRF will not provide any substantial resistance to ballistic resistance unless the entire glazing system is designed to defeat the intended threat (i.e., 1/2- to 3/4-inch laminated glass with 10-mil FRF would be required to defeat an underwriters Laboratories (UL) Level I threat).

G. Forced Entry Attacks

1. A substantial increase in forced entry resistance can be gained by using a 10-mil FRF for protection against very low level forced entry threats. When glass reinforced with FRF is struck with an ax or other impact tool, the hole will approximate the size of the tool used. Multiple impacts will be necessary to enlarge the hole to a size large enough for entry. FRF for forced entry protection should be limited to situations where nominal additional delay and sound will deter an attack (smash and grab situations such as storefronts). The use of FRF specifically to resist forced entry threats is not recommended. Ten-mil FRF is recommended as the most cost-effective film thickness for protection against thrown objects or simple weapons.

H. Effects of Explosives

1. FRF is not intended to resist blast loads. Its only purpose is to retain fragments of the shattered glass and minimize the number of fragments disbursed into a

[RETURN TO TOP](#)

protected area.

2. Blast testing with very short duration blasts characterized by a small, close-in explosion shows that FRF tends to hold the glass in position even though the glass shatters. Under long duration blast loads characterized by large, distant explosions, the fractured glass tends to be propelled as a single unit or as a group of large fragments with little retention in the frame.
3. The use of a catch bar ([Figures 2](#) and [3](#)) attached to the inside is recommended to reduce injury caused when the FRF system will not be retained in the frame. Ten-mil FRF is the most practical and cost-effective alternative for retention of glass fragments. Limited testing by manufacturers shows that under certain explosive conditions (3 to 9 psi, 35 to 80 psi-ms impulse), 4-mil film retained approximately 80 percent of the glass fragments, while 7-mil film retained 90 percent and 10-mil film retained 98 percent. Thicker films retained only slightly higher fragment percentages. Thicker films retain about the same fragment percentage as 10-mil film. Based on this information, 10-mil FRF appears to provide a substantial increase in performance at an additional installed cost that is only 50 percent more than the installed cost of 4-mil.

Figure 2: Catch Bar Sequence During an Explosion

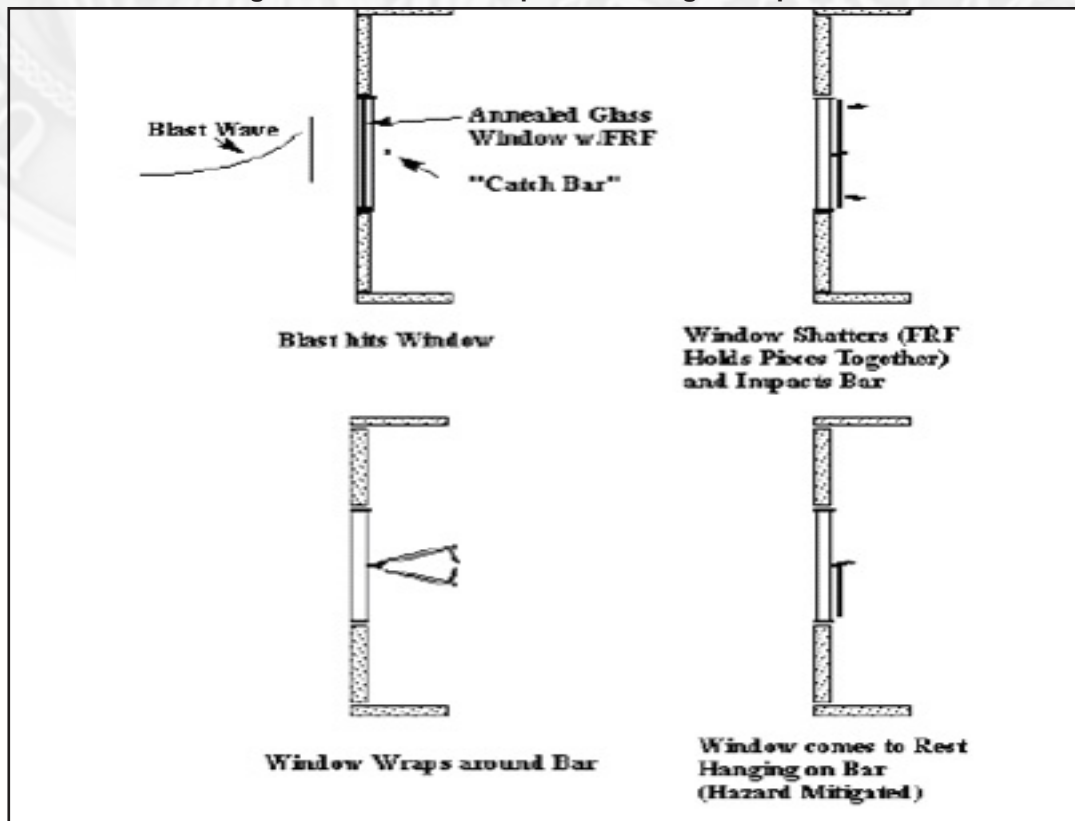
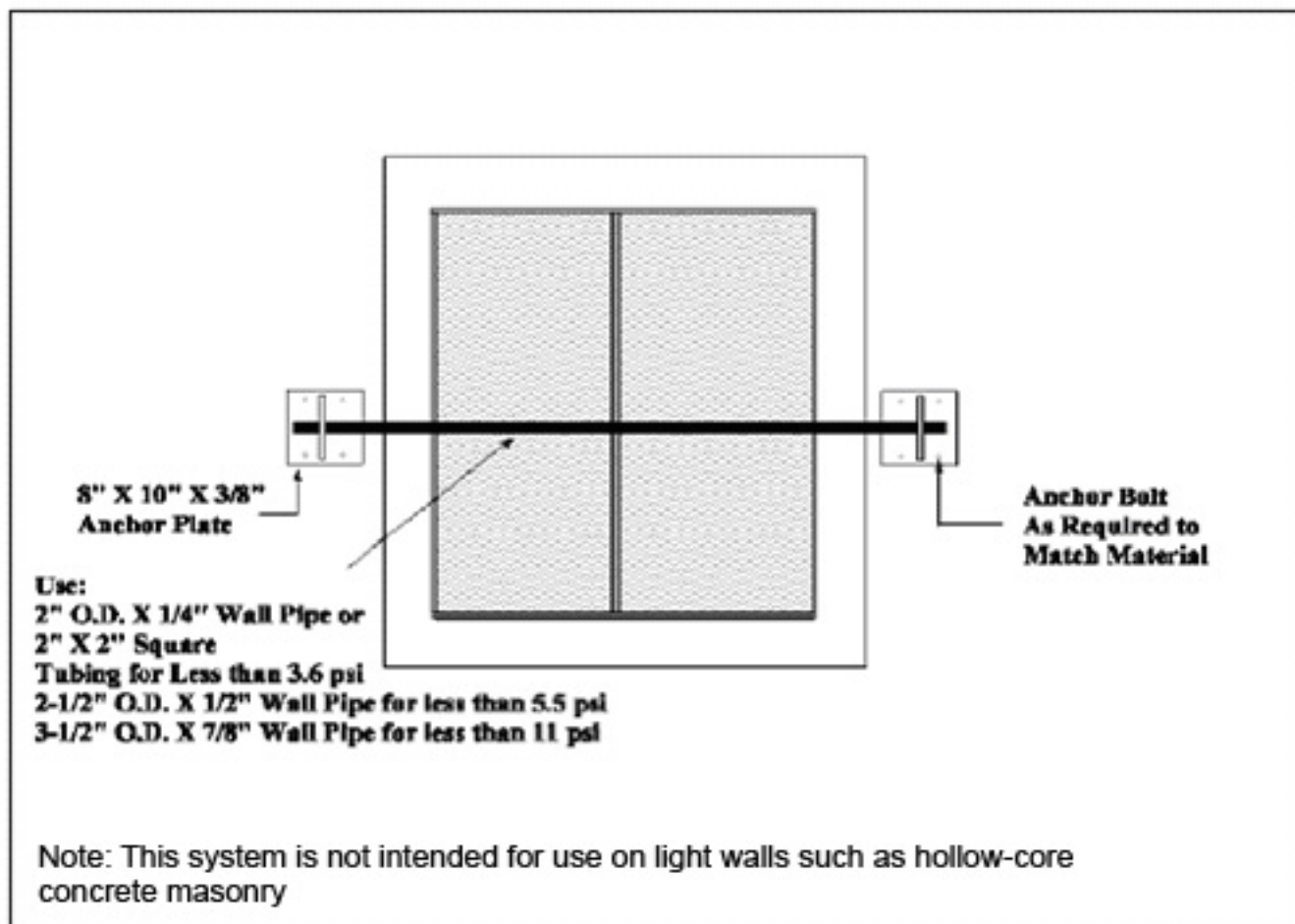


Figure 3: Catch Bar Detail



XII. DESIGN OF FRAGMENT RETENTION FILM SYSTEMS (FRF)

A. Design

1. Design factors for a FRF system include composition, thickness, and tint, surrounding construction, and glazing materials.

B. Composition

1. Films are composed of polyester, polyethylene terephthalate, or composite materials.

C. Thickness

1. Based on limited testing, the use of 10-mil FRF appears to be the most cost-effective choice for most applications. Ten-mil FRF appears to provide more protection than lighter films from flying fragments of glass due to blast loads or other threats. Heavier film provides about the same performance at greater cost.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

D. Tints

1. FRF is available in tinted versions. The most common has a silver tint and has the added benefit of improving the thermal energy performance of a building while providing a degree of obscuration from the outside. Although tinted film in darker colors is available, this film can cause internal heat buildup and internal stresses in the glazing, which can result in a weakened glazing system.

E. Surrounding Construction

1. When using 10-mil and thicker FRF that is anchored, the frame must have sufficient strength to allow the FRF to perform at maximum capacity; a qualified structural engineer should investigate building components adjacent to the frame for adequate transfer of the blast load or other threats.

F. Glazing Materials

1. The film manufacturer must be provided with the type of glass to be reinforced as well as information about gaskets, frame type, and configuration, depending on the type of application selected.

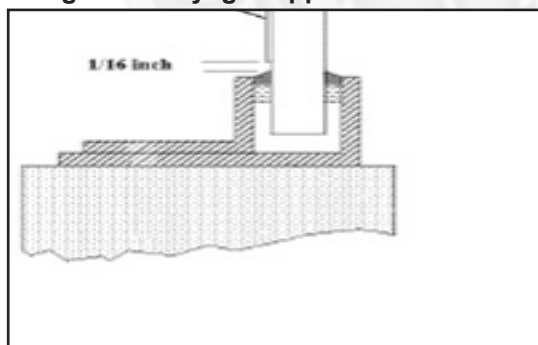
G. Applications

1. There are a number of ways FRF is applied. They are described here and shown in order of lowest to highest cost.

H. Daylight Applications

1. Daylight applications (film installed only on the area of glass that allows light to pass, see [Figure 4](#)) are the least costly and serve only to hold the glazing material together during an explosion. This application does not improve the blast resistance of the glazing material. In a daylight application, the FRF is trimmed back 1/16-inch from the edge of the frame. For all daylight applications, a catch bar or blast curtains are recommended to restrict movement of the glass panel when blown out of the frame.

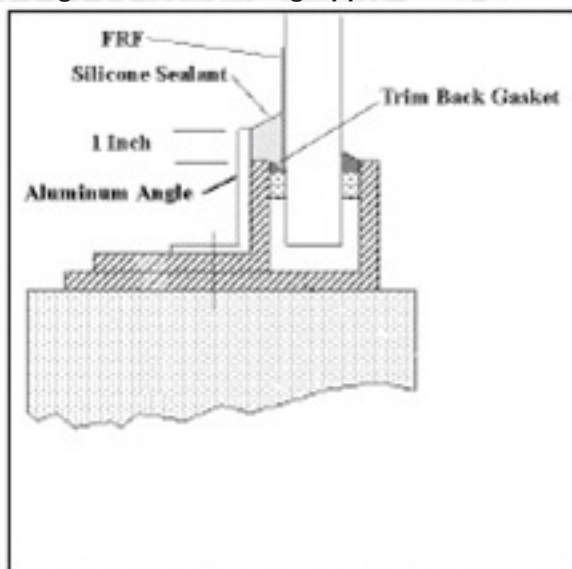
Figure 4: Daylight Application for FRF



XIII. WET GLAZING

- A. Wet glazing (film installed beyond the “daylight” area and secured along the edges with silicone “wet” glazing, see [Figure 5](#)) is used when the film can not be installed under the frame stops or various gaskets. This application is normally selected only when some additional fragment retention of the panel is desirable. For this application, the gasket is trimmed back as far as possible and the film embedded as deeply as possible beyond the frame edge. The gap between the frame and glass is then filled with an approved structural silicone caulking material. If trimming the gasket is not possible or adequate, an aluminum angle can be installed along the frame edge to form a reservoir for the structural silicone. For all wet glazing applications, a catch bar ([Figures 2 and 3](#)) or blast curtains are recommended to restrict movement of the glass panel when blown out of the frame.

Figure 5: Wet Glazing Application for FRF

**XIV. MECHANICAL ANCHORING SYSTEMS**

- A. These mechanical anchoring systems ([Figure 6](#)) are used to improve the performance of FRF. They can be either one-sided (along the top edge) or two-sided (on the long sides of the window). For this application, the film is brought past the edge of the glass and down along the frame. Using a steel or aluminum anchor bar with rounded edges, double-sided foam tape, and adequate anchor bolts, the film is normally wrapped around the anchor bar that is then bolted to the frame (depending on the manufacturer). The mechanical anchor holds the film to the frame and allows the film to retain a maximum percentage of fragments. Mechanical anchoring systems should be used only with 10-mil or thicker film material.
- B. When considering the use of a mechanical anchoring system, always require independent testing that will show performance characteristics under the loading

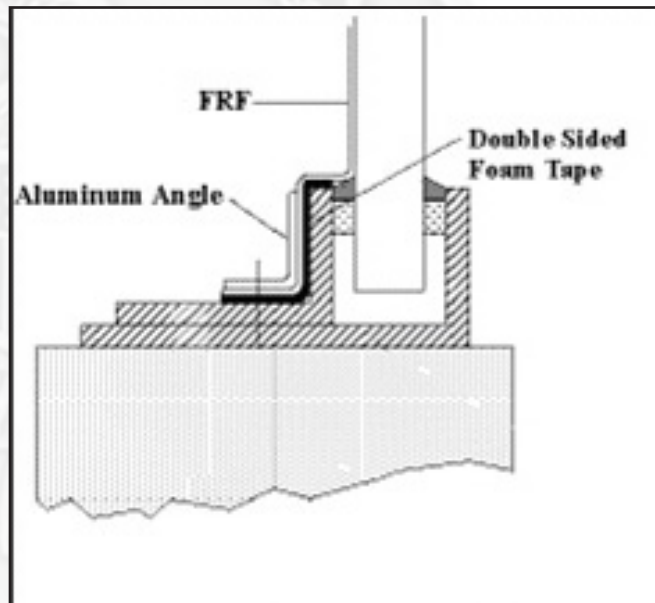
[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

conditions anticipated. If expected blast loads will exceed the performance capabilities of the installed system, always include a catch bar or blast curtains to restrict movement of the glass panel.

- C. Two-sided mechanical anchoring is strongly recommended for insulated glass. Two-sided anchoring will provide a higher level of glass retention for the unprotected outer glazing system than “daylight” or single side anchoring.

Figure 6: Mechanical Anchoring for FRF



XV. FILM SPECIFICATION

A. Minimum Requirements

- (a) The FRF will be optically clear polyester, polyethylene terephthalate, or a composite. It must be multi-layered or factory laminated. The film will include an abrasion resistant coating on the exposed surface. The film will be supplied with an optically clear, weather resistant, pressure-sensitive adhesive. The adhesive will contain ultraviolet (UV) inhibitors that prevent 95 percent of the radiation between 300 and 380 nanometers. The adhesive will not be water activated. A water-soluble detackifier and/or release liner may be used over the adhesive to make film application easier.

B. Minimum Performance

1. As a minimum level of performance, film must pass American National Standards Institute (ANSI) Z97.1 or 16 CFR § 1201, Category II impact tests. These standards set a minimum level of performance for FRF on reinforced glass (termed organic-coated glass) based on impact strength, tensile strength, and

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

adhesion. These tests include samples that have a simulated 1-year exposure to sunlight and UV radiation.

C. Test Sample

1. For the purpose of the test, the film should be attached to a piece of 1/4-inch thick flat glass conforming to the requirements of ASTM C 1036, Type I, Class 1, Quality q3.

D. Passing Criteria

1. After the impact portion of the test, satisfactory performance of the test specimen is determined using ANSI Z97.1, on the interpretation of results. To be acceptable for use as FRF, the manufacturer must provide a statement that the film satisfactorily performed according to ANSI Z97.1.

E. Tensile Strength

1. The tensile strength of the film should be 25,000 psi minimum.

F. Thickness

1. Minimum thickness should be based upon design requirements. Ten-mil film is recommended for most applications.

G. Peel Strength

1. The peel strength should be a minimum of 4.7 pounds/inch for 7-mil and thicker films.

H. Optics and Tint

1. All film, regardless of color, should be optically clear from the inside to ensure an undistorted view through the glass. Color, tint, and reflectivity, when required, should be specified. The amount of reflectivity of solar radiation is specified as a percentage.

I. Flame Spread and Smoke Density

1. When required by life safety or local building codes, specify a flame spread rating and a smoke density rating for the film. The film should not exhibit a flame spread index exceeding 25 and a smoke density index exceeding 100 when tested in accordance with ASTM E 84. For the purpose of testing, the specimen should be mounted to 1/2-inch thermally tempered glass.

J. Manufacturer's Qualifications

1. Specifications for FRF should require the manufacturer to have at least 3 years of experience in the manufacture of FRF, and that the film be a standard product of the manufacturer and intended for the purpose described in the specifications. Only films designed for fragment retention will perform in an acceptable manner.

K. Cleaning Instructions

1. Always specify that the manufacturers provide cleaning instructions with the film materials. Many cleaning compounds are not compatible with film.

XVI. INSTALLATION

A. New Construction

1. Quarter-inch laminated glass in a standard frame will perform about the same as a daylight application of 10-mil film and will last for the life of the structure.

B. Retrofit Application

1. Film can be installed beyond the frame edge to improve retention characteristics of the glass panel. However, any extension of the film past the inner frame edge will require at least partial frame dismantling. For this application, the glazing should be removed and the film applied to the outside edges of the glazing material, which extend into the frame bite. If dismantling is too expensive, specify a "daylight" application where the film is applied to within 1/16 inch of the edge of the visible glazing. Although it is less likely the glazing will be retained in its frame under a blast load, it is still a substantial improvement in fragment retention. If this method is used, install a catch bar ([Figure 3](#)) to prevent the glass section from penetrating the protected area.

C. Film Splice

1. The film may be spliced or lapped when a glazing dimension exceeds 60 inches in either direction. All seams or splices will be applied with a butt joint. For windows with seams, catch bars should be placed at 90 degrees to the seam direction. For installations where "smash and grab" theft is also a concern, seams should always be horizontal.

D. Visual Inspection

1. Within 30 days of application, the adhesive should be 95-percent cured. No water bubbles, foreign particles, or excessive distortion should be visible when viewed by the unaided eye from a distance of up to 10 feet from the interior room side at angles up to 45 degrees.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

E. Application

1. This film is attached directly to the glass surface. FRF should be applied on the interior of windows for protection from the effects of spalling. For double-glazed units (insulated glass), apply the film to the room (protected) side of the innermost frame. Specify that the film must be applied in strict accordance with the manufacturer's application instructions. If the film is used on double-glazed units, film anchorage on two sides is strongly recommended to improve glass retention of the unprotected outside glazing.

F. Qualifications of Personnel

1. Specify that personnel applying or supervising the application of the FRF be trained and certified by the film manufacturer.

G. Environmental Issues

1. The film will not be applied if there are visible dust particles in the air, if there is frost on the glazing, or if any room conditions such as temperature or humidity do not meet the manufacturer's instructions. The manufacturer must be informed about the environment the film must withstand, such as interior or exterior atmosphere, solvents, chemicals, or excessive humidity. After film application, room conditions should be kept as required by the manufacturer's instructions to allow proper curing of the adhesive. The manufacturer must also know the characteristics of the glass being treated with the film to ensure compatibility.

XVII. BLAST CURTAINS, SHADES, AND SPALL SHIELDS

- A. There are several types and styles of blast curtains, shades, and spall shields that are commercially available that can be used in situations where film and laminated glass are not suitable, such as on windows with multiple panes or where film would be subject to excessive abuse. Blast curtains and shades are manufactured from tough fiber materials such as Kevlar or Spectra, which have strong tear resistance. They can also be used in conjunction with Fragment Retention Film (FRF) in place of a catch bar or mechanical anchoring. Spall shields are rigid barriers usually made with thin sheet (1/8-inch to 1/4-inch) polycarbonate, intended to absorb fragments before they enter an occupied space.

- B. Blast curtains, shades, and spall shields must be designed to withstand the loading conditions anticipated.

C. Blast Curtains

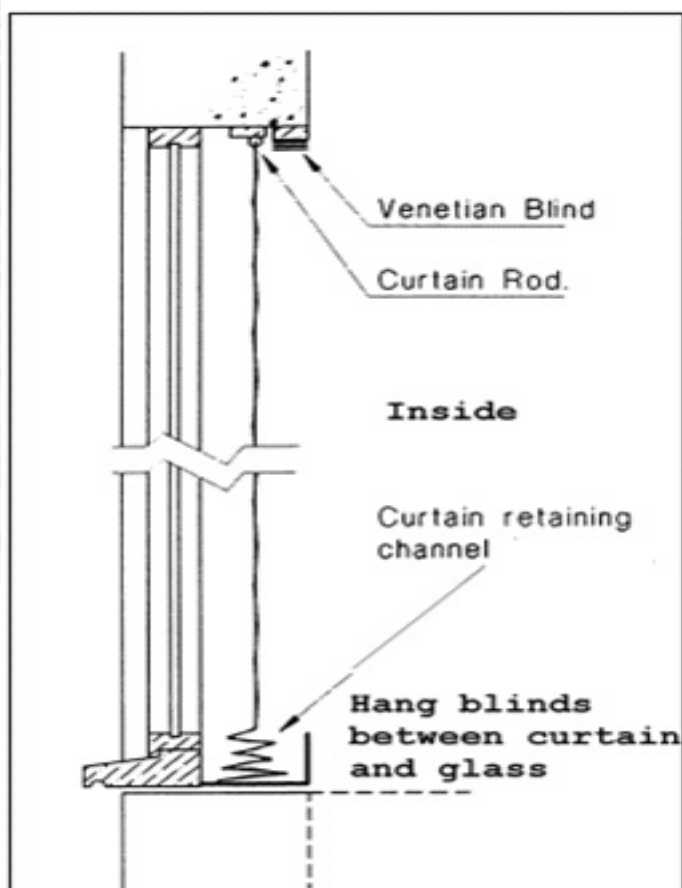
1. Commercially available blast curtains ([Figure 7](#)) are made of various materials such as Kevlar- or Spectra-polyethylene fiber or knitted polyester. Blast curtains allow venting of the blast wave while at the same time "catching" any fragments

[RETURN TO TOP](#)

resulting from an explosive blast.

2. The concept of a blast curtain is to allow sufficient fabric and strength to give with the blast load and prevent glass fragments from flying into the occupied space. Drapes should be treated to withstand fading, mildew, and soiling. Before selecting a blast curtain for use, insist on independent testing of the product to ensure it will perform as required. It is vitally important to have supporting test data that will demonstrate the product's effectiveness within the range of threats anticipated. Drapes should allow light to enter the protected space and allow some degree of visual access. Opaque drapes that must be opened for light and vision will be useless during an explosive event.

Figure 7: Blast Curtain Detail



D. Blast Shades

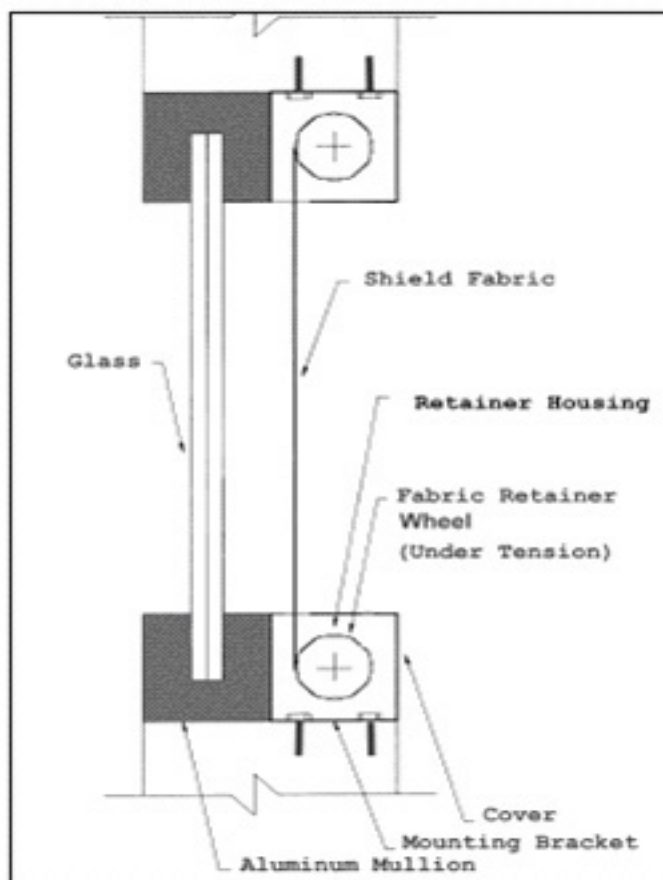
1. Blast shades ([Figure 8](#)) are also intended to prevent or minimize injuries to occupants of buildings in the event of a terrorist bombing. Blast shades are rigidly mounted to the interior wall of the structure, in back of the glazing system. They are most commonly used for retrofit installation where Fragment Retention Film would not be effective (such as multi-pane glass lites). Blast shades should be treated to resist fading, mildew, and soiling.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

2. Commercially available blast shades are normally made with Kevlar or Spectra polyethylene fiber. Before selecting blast shades for use, insist on independent testing of the product to ensure it will perform as required. It is vitally important to have supporting test data that will demonstrate the product's effectiveness within the range of threats anticipated. Shades should allow light to enter the protected space and allow an acceptable degree of visual access from inside the room. They should be permanently attached, but allow for access to the glazing system for maintenance.

Figure 8: Blast Shade Detail



E. Spall Shields

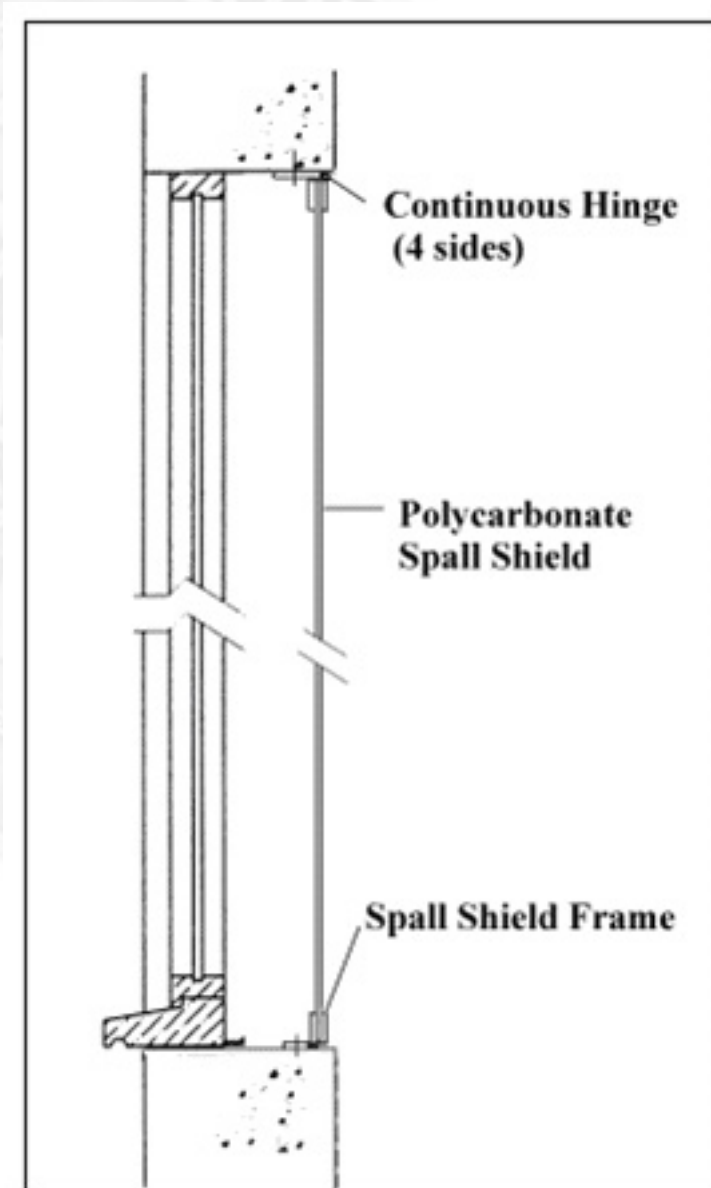
1. A spall shield ([Figure 9](#)) is a secondary glazing system mounted behind and away from the existing glazing system. A spall shield will effectively absorb glass fragments generated during an explosive event. The spall shield is constructed with clear polycarbonate and has its own frame and mounting system (four-sided attachment).
2. Before selecting a spall shield for use, insist on independent testing of the product to ensure it will perform as required. It is vitally important to have

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

supporting test data that will demonstrate the product's effectiveness within the range of threats anticipated.

Figure 9: Spall Shield



XVIII. EFFECT OF THE ENVIRONMENT ON GLAZING

A. Exterior Environments

1. Polycarbonate and Glass-Clad Polycarbonate:

- (a) If a polycarbonate cross section is exposed to conditions of high humidity or salt air, consider hard-coating the surface of the polycarbonate to protect it from abrasion and contaminant penetration. Extreme temperature differentials and large thicknesses of polycarbonate can produce bending stresses that will eventually lead to delamination. Glass-clad polycarbonate systems are particularly prone to this effect because of the 8:1 difference in coefficient of expansion between glass and polycarbonate materials. If thick cross sections of polycarbonate (greater than 5/8 inch) are exposed to temperature swings greater than 70°F, use an air gap system and adequate ventilation to reduce moisture accumulation. An air gap will minimize the temperature impact on the polycarbonate material.
- (b) Certain temperature and humidity conditions, either interior or exterior, can also cause a slight bowing in polycarbonate, usually in the direction of the higher temperature or humidity. This bowing is reversible and flatness can be restored to the sheet by equalization of the factors that cause bowing.
- (c) Although bowing doesn't affect visibility, it can cause distorted reflections. Specifying thicker polycarbonate sheet and increasing the edge engagement are ways of reducing distortion and bowing. The amount of additional edge engagement needed for expansion or contraction depends on the dimensions of the polycarbonate sheet. Edge engagement ranges from 1/16 inch for a 24-inch sheet to 3/8 inch for a 120-inch sheet. The exact requirement can be calculated by multiplying the length of the sheet in inches times the temperature span (minimum to maximum expected temperature) times 0.0000375 (coefficient of expansion). This figure is added to the structural requirement for edge engagement, which is normally 1 to 1-1/4 inches. When large variations of temperature are expected, dry glazing (using silicone or neoprene gaskets) is recommended over wet glazing (high-grade silicone sealants and fully cured butyl tapes).

B. Physical Abuse

1. Polycarbonate:

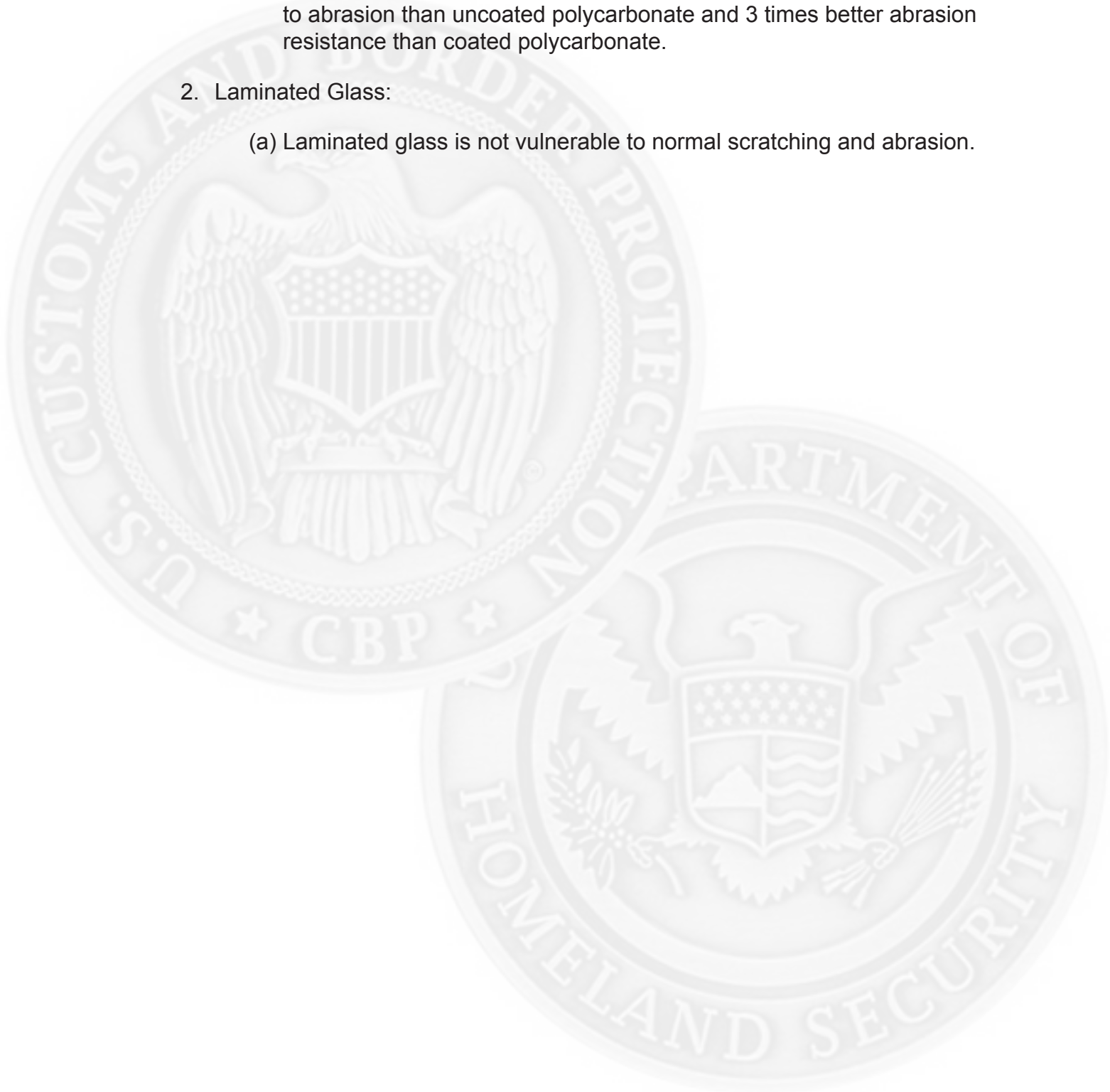
- (a) If a polycarbonate cross section is exposed to high traffic conditions or conditions where the material can be physically abused by occupants of the building, consider hard-coating the surface of the polycarbonate to

[RETURN TO TOP](#)

protect it from abrasion and scratching. If a serious condition exists, a laminated cross section with annealed glass facing the inside will protect the polycarbonate against abuse. Glass has 30 times the resistance to abrasion than uncoated polycarbonate and 3 times better abrasion resistance than coated polycarbonate.

2. Laminated Glass:

- (a) Laminated glass is not vulnerable to normal scratching and abrasion.





APPENDIX 7.8: OPENINGS

I. OPENINGS

A. Operable Openings are doors, windows, transoms, skylights and all similar devices that can be opened or closed to allow or prevent passage of people, air, or light. Openings can also include, but are not limited to, elevators, penthouses, hatchways, or doors to the roof. Roof doors are often overlooked because of infrequent use. These openings are the usual points of entry for intruders especially at ground level and in their concealed and semi-concealed locations. Operable openings are also the hardest points to protect simply because they are designed for passage.

B. Protecting operable openings shall be based on the following criteria:

1. Is the opening really required?

2. Is the opening 96 square inches or larger?

3. Validate existing openings that may no longer be required. If not required:

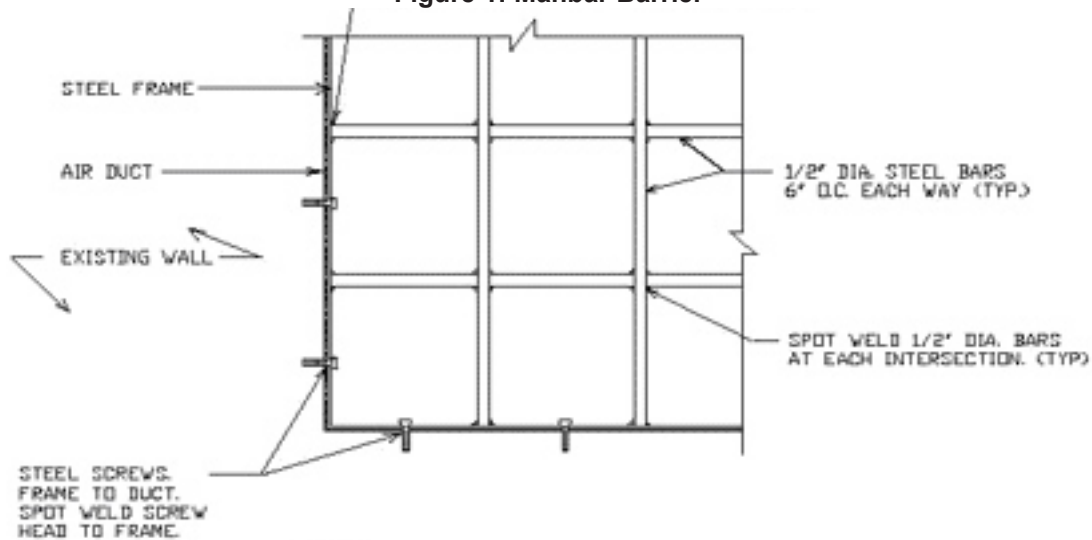
(a) Is the opening less than 18 feet from the ground or less than 14 feet from another structure? If yes, than it shall be covered with bars or grilles and equipped with intrusion detection device.

(b) Permanently seal the wall in a manner that maintains the penetration resistance of the wall containing the opening

(c) The door is eliminated from the brick wall, the door assembly will be removed and the opening bricked up; properly anchoring new construction.

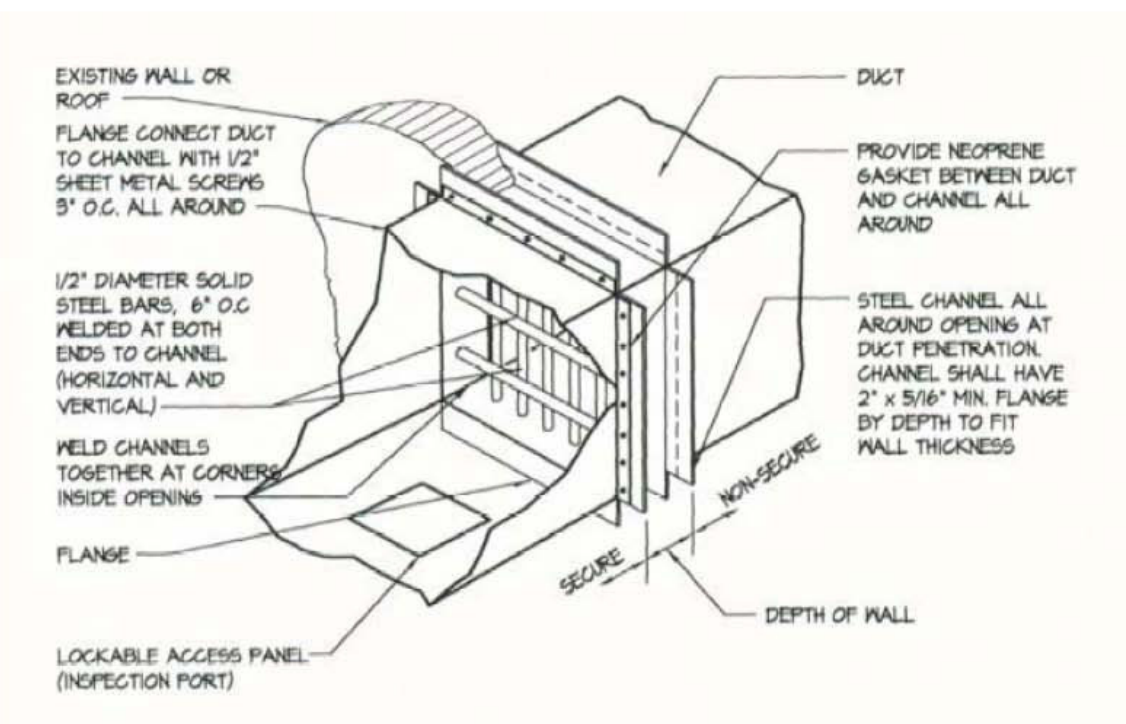
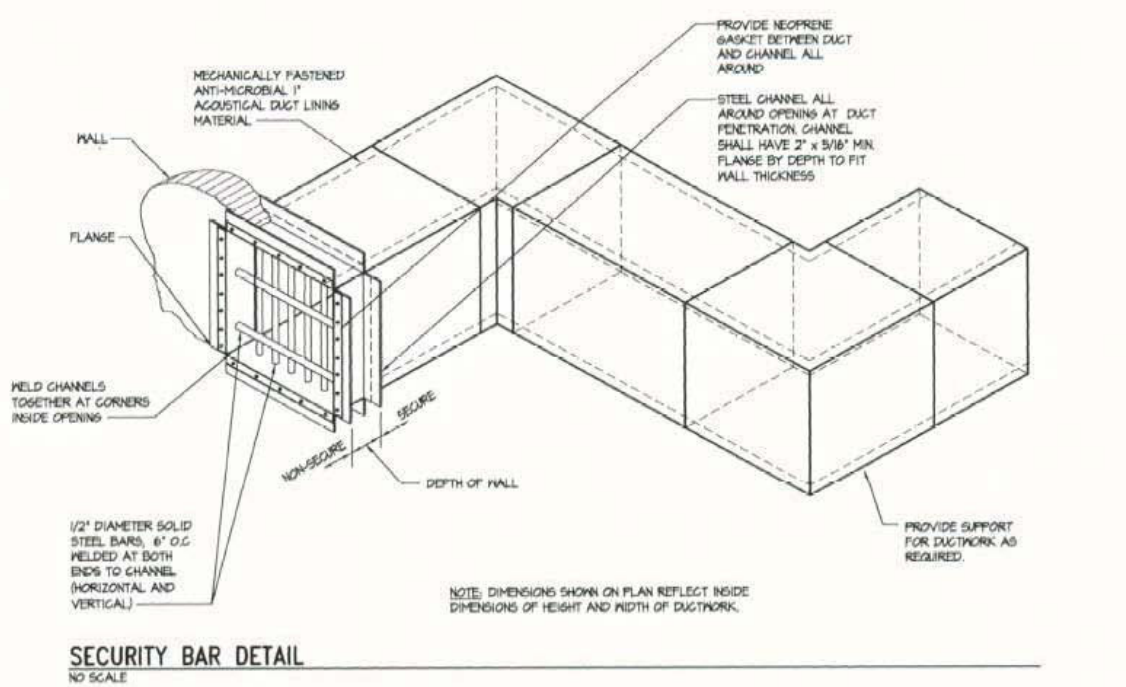
- Miscellaneous Openings. Any miscellaneous openings, open ducts, pipes, registers, sewers in excess of 96 square inches (619.2 centimeters) in area and over 6 inches (15.24 centimeters) in its smallest dimension shall be equipped with barriers. Acceptable barriers are 9 gauge expanded metal mesh, or rigid metal (steel) bars at least one-half inch in diameter, welded vertically and horizontally 6 inches on center. The rigid metal bars shall be securely fastened at both ends to preclude removal. Crossbars shall be used to prevent spreading of the bars. Solid caulking shall be used between the sleeve or conduit to give evidence of surreptitious entry attempt. Access for inspection of barriers should be in accordance with agency policies. Note [Figure 1](#).

Figure 1: Manbar Barrier



NOTE: MANBARS SHALL BE REQUIRED FOR ANY PENETRATION LARGER THAN 96 SQ.IN OF ANY PERIMETER WALLS, GUN VALLTS, AND EVIDENCE ROOMS.

Figure 2: Security Bar Detail



II. MANHOLES

- A. Manholes can provide entrances into buildings for service purposes or provide access to utility tunnels containing pipes for heat, gas, water, telephone transmission conduits, cables, and other utilities.
- B. Manhole covers 10 inches or more in diameter must be secured to prevent unauthorized opening. They may be secured with locks and hasps by welding them shut or by bolting them to their frame. Ensure that hasps, locks, and bolts are made of materials that resist corrosion.
- C. A case-hardened chain and high security padlock can be used to secure a manhole cover; the use of a heavy-duty hinged-steel dead bar secured with a high security padlock and heavy-duty hasp is an alternative method.
- D. Keyed bolts (which make removal by unauthorized personnel more difficult) are also available. If very high security is required, manhole covers that resist shattering after being artificially “frozen” by an aggressor should be considered.
- E. If a tunnel penetrates the interior of a building, the manhole cover should be secured. A chain or padlock can be used to secure a manhole. Steel grates and doors flush with the ground level may provide convenient access. If the frame is properly secured, the grates or doors can be welded into place or they can be secured with a chain and padlock. Sewers or storm drains which might provide an entrance should be secured.

III. ACCESSIBLE STEEL GRATES AND DOORS

- A. Grates and doors on ground level are other potential access points into a facility. These types of openings often serve as service entrances or exterior elevator entrances or they may simply provide light and air to the basement level of the building.
- B. The mounting frame must be properly secured. The grates or doors can be welded into place, or they can be secured with a steel chain and high security padlock.

IV. SEWERS AND STORM DRAINS

- A. Accessible openings to sewers and storm drains shall be secured if the areas of the openings associated with them are larger than 96 sq. in. (619.4 sq. cm) and more than 6 inches (15.2 cm) in any one dimension.

V. ROOF OPENINGS

- A. Access to a building’s roof can allow entry to the building and access to air intakes

and building Heating, Ventilating, and Air-Conditioning (HVAC) equipment (e.g., self-contained HVAC units, laboratory or bathroom exhausts) located on the roof.

- B. All glass skylights on the roof of any building or premises used for business purposes and subject to the provisions hereof, shall be provided with:
 - 1. Iron bars of at least 1/2-inch round or 1-inch by 1/4-inch inch flat steel material under the skylight and securely fastened; or
 - 2. Steel grill of at least one-eighth-inch material of two-inch mesh under the skylight and securely fastened.
- C. All hatchway openings on the roof of any building or premises used for business purposes and subject to the provisions hereof shall be secured as follows:
 - 1. If the hatchway is of wooden material, it shall be covered on the inside with at least sixteen (16)-gauge sheet steel attached with screws.
 - 2. The hatchway shall be secured from the inside with a slide bar or slide bolts.
 - 3. Outside hinges on all hatchway openings shall be provided with non-removable pins. Such hinge pins may be welded, flanged, or secured by non-removable screws.
- D. All air duct or air vent openings exceeding eight (8) inches by twelve (12) inches on the roof of any building or premises used for business purposes and subject to the provisions hereof shall be secured by covering the same with either of the following:
 - 1. Iron bars of at least 1/2-inch round or 1-inch by 1/4-inch flat steel material, spaced no more than five inches apart and securely fastened.
 - 2. Steel grill of at least one-eighth-inch material of two-inch mesh and securely fastened.
- E. If the barrier is on the outside it shall be secured with rounded head flush bolts on the outside.

VI. ROOF ACCESS

- A. Design locking systems to meet the requirements of the International Building Code and limit roof access to authorized personnel. Skylights are another source of entry from the roof. These openings can be protected with bars or mesh.
- B. Fencing or other barriers should restrict access from adjacent roofs. Access to roofs should be strictly controlled through keyed locks, keycards or similar measures. Skylights are another source of entry from the roof.

VII. ROOF SECURITY BARRIERS

- A. Barbed wire fencing, razor wire fencing, chain link fencing or any other like security barrier shall not be installed at roof level in such a manner as to obstruct egress or access in the event of fire or other emergencies.

VIII. BUILDING ACCESS CONTROL DEVICES

- A. Access control devices must be approved by the CBP/IA/SMD. These include bars, grates, gates, electric or magnetic locks or similar devices that would inhibit rapid fire department emergency access to the building.
- B. For all new and existing buildings covered by these standards, access to roofs must be controlled to minimize the possibility of aggressors placing explosives or chemical, biological, or radiological agents in that area or that could threaten building occupants or critical infrastructure.
- C. For new buildings, all external roof access must be eliminated by providing access from internal stairways or ladders, such as in mechanical rooms.
- D. For existing buildings, external access must be eliminated where possible, otherwise they must have secure external ladders or stairways with locked cages or similar mechanisms.

IX. ROOF DOORS SECURITY MEASURES LOCKING DEVICES

- A. All doors that exit onto the roof of any building or premises used for business purposes and subject to the provisions hereof shall comply with the following requirements:
 - 1. Doors with glass panels and any glass panels that are adjacent to the door frame shall be protected as follows: 1/4-inch
 - (a) The glass portion shall be covered with iron or steel grills of at least one-eighth-inch material of no more than two-inch mesh securely fastened.
 - (b) If the door or glass panel barrier is on the outside, it shall be secured with rounded head flush bolt on the outside.
 - (c) If the remaining portion of a door panel exceeds eight inches by twelve (12) inches (excluding door frame) and is of wood, but not of solid core construction, or is less than 1 3/8-inches thick, said portion shall be covered on the inside with at least sixteen (16) gauge sheet steel attached with screws.
 - 2. Wood doors not of solid-core construction, or with panels therein less than 1 3/4

inches thick, shall be covered on the inside with at least 16-gauge sheet-steel attached with screws.

3. All roof doors shall be provided with a lock that will permit the door to be opened from the inside without the use of a key or any special knowledge or effort. Outside hinges on all roof doors shall be provided with non-removable pins. Such hinge pins may be welded, flanged, or secured by non-removable screws.

X. MECHANICAL AREAS

- A. Mechanical system design standards address limiting damage to critical infrastructure and protecting building occupants against CBR threats. The primary goal of a mechanical system after a terrorist attack should be to continue to operate key life safety systems. This can be accomplished by locating components in less vulnerable areas, limiting access to mechanical systems, and providing a reasonable amount of redundancy.
- B. Critical infrastructure systems must be located away from high-risk areas (e.g., garages and loading docks). The system controls and power wiring to the equipment should be protected, and the system should be connected to emergency power to provide smoke removal. Smoke removal equipment should be provided with standalone local control panels that can continue to individually function in the event the control wiring is severed from the main control system.
- C. Designers should consider the following:
 1. Do not mount plumbing, electrical fixtures, or utility lines on the inside of exterior walls, but, when this is unavoidable, mount fixtures on a separate wall at least 6 inches from the exterior wall face.
 2. Avoid placing plumbing on the roof slab.
 3. Avoid suspending plumbing fixtures and piping from the ceiling.
 4. Reduce the number of utility openings, manholes, tunnels, air conditioning ducts, filters, and access panels into the structure.
 5. Locate utility systems away from likely areas of potential attack, such as loading docks, lobbies, and parking areas.
 6. Protect building operational control areas and utility feeds to lessen the negative effects of a blast.
 7. Design operational redundancies to survive all kinds of attack.
 8. Use lockable systems for utility openings and manholes where appropriate.

- D. Infrequently-used utility covers/manholes can be tack-welded to lock tamper-resistant covers.

XI. MECHANICAL AREA DESIGN STANDARDS

- A. The mechanical room provides space for the HVAC and domestic hot water equipment, the water treatment system, and the heater serving the main building. It is located adjacent to the main building support spaces.

- B. Main Building

- 1. Power: Normal convenience power standards and as required by mechanical equipment.
- 2. Lighting: General fluorescent, 50 FC.
- 3. HVAC: Normal ASHRAE HVAC standards.
- 4. Plumbing: As required by mechanical equipment and floor drain.
- 5. Floor: Sealed concrete sloped to drain.
- 6. Walls: 8" CMU.
- 7. Ceiling: No finished ceiling required Voice Communications.
- 8. Material: 1 3/4" 12 gauge steel clad hollow door and frame. Provide double doors, as required.
- 9. Hardware: Standard lockset keyed individually and to a CBP master key.

- C. Commercial Building

- 1. Power: Normal convenience power standards and as required by mechanical equipment.
- 2. Lighting: General fluorescent, 50 FC.
- 3. HVAC: Normal ASHRAE HVAC standards.
- 4. Plumbing: As required by mechanical equipment and floor drain.
- 5. Floor: Sealed concrete sloped to drain.
- 6. Walls: 8" CMU.
- 7. Ceiling: No finished ceiling required Voice Communications.

8. Material: 1 ¾" 12 gauge steel clad hollow door and frame. Provide double doors, as required.
9. Hardware: Standard lockset keyed individually and to a CBP master key.

XII. SITE UTILITIES

- A. Utility systems can suffer significant damage when subjected to the shock of an explosion. Some of these utilities may be critical for safely evacuating people from the building. To minimize the possibility of such hazards, apply the following measures:
 1. Where possible, provide underground, concealed, and protected utilities.
 2. Provide redundant utility systems to support site security, life safety, and rescue functions.
 3. Consider quick connects for portable utility backup systems if redundant sources are not available.
 4. Prepare vulnerability assessments for all utility services to the site, including all utility lines, storm sewers, gas transmission lines, electricity transmission lines, and other utilities that may cross the site perimeter.
 5. Protect water treatment plants and storage tanks from waterborne contaminants by securing access points, such as manholes; maintain routine water testing to help detect waterborne contaminants.
 6. Minimize the number of signs identifying critical utility complexes (e.g., power plants and water treatment plants). Provide fencing to prevent unauthorized access and use landscape planting to conceal above ground systems.
 7. Locate petroleum, oil, and lubricant storage tanks and operations buildings down slope from all other buildings. Site fuel tanks at an elevation lower than operational buildings or utility plants. Locate fuel storage tanks at least 100 feet from buildings.
 8. Locate the main fuel storage away from loading docks, entrances, and parking. Access should be restricted and protected (e.g., locks on caps and seals).
 9. Provide utility systems with redundant or loop service, particularly in the case of electrical systems. Where more than one source or service is not currently available, provisions should be made for future connections. In the interim, consider "quick connects" at the building for portable backup systems.
 10. Decentralize a sites communications resource when possible; the use of multiple

communications networks will strengthen the communications system's ability to withstand the effects of a terrorist attack. Careful consideration should be made in locating, concealing, and protecting key network resources such as network control centers.

11. Place trash receptacles as far away from the building as possible; trash receptacles should not be placed within 30 feet of a building.
 12. Conceal incoming utility systems within building and property lines, and give them blast protection, including burial or proper encasement, wherever possible.
 13. Consider incorporating low impact development practices to enhance security, such as retaining storm water on site in a pond to create stand-off, instead of sending into the sewer system.
 14. Locate utility systems at least fifty (50) feet from loading docks, front entrances, and parking areas.
 15. Route critical or fragile utilities so that they are not on exterior walls or on walls shared with mail rooms.
 16. Where redundant utilities are required in accordance with other requirements or criteria, ensure that the redundant utilities are not co-located or do not run in the same chases. This minimizes the possibility that both sets of utilities will be adversely affected by a single event.
 17. Where emergency backup systems are required, ensure they are located away from the systems components for which they provide backup.
 18. Mount all overhead utilities and other fixtures weighing 31 pounds (14 kilograms) or more to minimize the likelihood that they will fall and injure building occupants. Design all equipment mountings to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction. (This standard does not preclude the need to design equipment mountings for forces required by other criteria such as seismic standards.)
- B. All utility penetrations of a site's perimeter barrier, including penetrations in fences, walls or other perimeter structures, should be sealed or secured to eliminate openings large enough to pass through the barrier. Typical penetrations could be for storm sewers, water, electricity, or other site utility services. Specific requirements of various openings are discussed below:
1. All utility penetrations of the site's perimeter should be screened, sealed, or secured to prevent their use as access points for unauthorized entry into the site. If access is required for maintenance of utilities, secure all penetrations with screening, grating, latticework, or other similar devices so that openings do not

allow intruder access. Provide intrusion detection sensors and consider overt or covert visual surveillance systems if warranted by the sensitivity of assets requiring protection.

2. Drainage ditches, culverts, vents, ducts, and other openings that pass through a perimeter and that have a cross-sectional area greater than 96 sq. in. and whose smallest dimension is greater than 6 inches shall be protected by securely fastened welded bar grilles.
3. As an alternative, drainage structures may be constructed of multiple pipes, with each pipe having a diameter of 10 inches or less. Multiple pipes of this diameter may also be placed and secured in the inflow end of a drainage culvert to prevent intrusion into the area.
4. Ensure that any addition of grills or pipes to culverts or other drainage structures is coordinated with the engineers so that they can compensate for the diminished flow capacity and additional maintenance that will result from the installation.

XIII. PROTECTING ABOVEGROUND FUEL STORAGE TANKS

A. General

1. CBP stores and dispenses a large quantity of fuel for its patrol vehicle fleet. At many locations, CBP maintains fueling stations. CBP also performs its own maintenance on much of this fleet and requires lubricant oils for this maintenance. CBP has above ground fuel storage tanks, and mobile fuel dispensing trucks used in its operations to fuel its patrol and transport vehicles, aircraft, construction equipment and boats. This handbook identifies general physical security requirements for aboveground fuel storage tanks. The tank shall meet requirements herein or be a CBP/IA/SMD pre-approved equal.

B. Site Location

1. Fuel Storage Tanks shall be located on federally controlled property. The main fuel storage shall be located away from loading docks, entrances, and parking. Access shall be restricted and protected (e.g., locks on caps and seals). Aboveground fuel storage tanks should be no closer than 50 ft in any direction to any entrance, vehicle circulation, and parking or maintenance area and no closer than 100-150 feet from a building.

C. UL/ULC Listing

1. The tank shall be tested to and listed (and carry UL/ULC labels) for the following:
 - UL – 142, aboveground tanks for flammable and combustible liquids.

- UL – 2085, two hour furnace fire test and two hour simulated pool fire test for insulated tank.
- UL – 2085, insulated and protected secondary containment aboveground tanks for flammable and combustible liquids.
- UL – 2085 and UFC SECTION (79-7) APPENDIX #A-II-F-1, ballistic and vehicle impact test for protected tank.
- UL – 2085 Non-Metallic Secondary Containment and Venting by Form of Construction.

D. General Requirements For Both Ballistic Resistant And Non Ballistic Aboveground Tanks

1. Access Control

- (a) Automated access control systems may be used. The system shall be capable of maintaining a record of who accessed the fuel tank. Access control systems may use a keypad, card reader, or a combination of both.
 - Closed Circuit Television (CCTV). For manned facilities, provide a CCTV L. system with cameras viewing the exterior entrance and all areas of the aboveground fuel tank. The system must be continuously monitored at a staffed central control position. For more information on CCTV refer to [Appendix 8.12: CCTV](#).
 - Intrusion Detection System (IDS). For more information on IDS, refer to [Appendix 8.9 IDS](#) and [Appendix 7.15 Loading Docks and Service Access](#).

2. Bullet Resistance

- (a) The tank shall withstand bullet resistance tests in compliance with UFC Section (79-7), Appendix #A-II-F-1.

3. Fire Extinguisher and Clean-up Kit

- (a) Portable fire extinguishers must be provided for the suppression of fires in accordance with NFPA 10 and UFC for high hazard area. Fire extinguisher and clean-up kit shall be sized and provided by the tank manufacturer. Fire extinguisher shall be mounted on the exterior of the generator enclosure with 316 stainless steel bracket and fasteners. Clean-up kit shall be similarly mounted inside the generator enclosure.

4. Flame Arrestors

- (a) Approved flame arrestors or pressure vacuum breather valves shall be installed in normal vents.

5. Fuel Piping

- (a) All fuel piping shall be schedule 40, 316 stainless steel (screwed or welded).

6. Overfill Protection

- (a) The tank shall be provided with the following methods to protect against overfill:

- Direct reading level gauge at the tank which is visible from fill pipe location;
- Valve located within fill pipe access to close automatically at a specified fill level; and,
- Audible high level alarm activated by a float switch at a specified fill level.

7. Security Fence

- (a) Provide security fencing around all petroleum facilities to ensure safety and prevent unauthorized access. For storage tanks within fenced perimeter provide standard 8ft. fence and if stand alone provide 12 foot impound lot fence. For more information on fencing refer to [Appendix 7.3 Fencing](#).

8. Uplift Restraints

- (a) The tank shall be supplied with flood-resistant tie-down brackets/hurricane hold-down restraints.

9. Venting

- (a) The tank system shall be furnished with a 2 inch normal vent and an emergency pressure relief system. The standard emergency relief system furnished with the tank shall open if the tank pressure exceeds ½ psi. The tank system shall conform to code requirements and UL/ULC Standards for venting. All vents and fittings utilized on the fuel tank shall be constructed of stainless steel.

E. Additional Requirements For Non-Ballistic Resistant Aboveground Tanks

1. BALLISTIC RESISTANT ENCLOSURES shall be constructed for aboveground fuel storage tanks that do not meet ballistic resistant requirements in UFC Section (79-7), Appendix #A-II-F-1.
 - (a) Minimum level III on housing wall requirements. [NIJ Standard 0108.01](#)
 - (b) Fuel Storage Tanks shall be hardened against small arms fire (UL 752).
 - (c) Harden support systems (standby power sources, electrical system conduits, mechanical system conduits and roof-mounted equipment) to protect them from sabotage.

F. Installation

1. Tank shall be installed as per manufacturer's requirements and as per the drawings. Tank shall be installed by qualified personnel who have been approved by the manufacturer and who have knowledge of, and possess the skills and equipment necessary, to install this type of aboveground storage tank properly and safely. Do not handle or move the tank unless it is empty. Under no circumstances should a tank containing petroleum product be moved. Do not drop or drag the tank.
2. Installation, operation and maintenance of the tank must be carried out in accordance with the applicable codes and regulations. Aboveground storage tanks are intended for installation in accordance with NFPA 30, 30A, 31 and UFC Appendix II-F.

G. Foundation

1. The foundation for the tank must be designed (and approved by tank manufacturer) to support the tank plus the weight of the maximum amount of product the tank will be storing. The foundation design must also include provision for draining surface water away from the tank to minimize the risk of fuel accumulation under the tank from the overfill or spills.
2. For more information, visit the EPA's [Source Water Protection Practices Bulletin](#).

XIV. BUILDING HVAC SYSTEMS

- A. Ventilation shafts, vents, or ducts, and openings in the building to accommodate ventilating fans or the air conditioning system can be used to introduce Chemical, Biological, and Radiological (CBR) agents into a facility.
- B. Decisions concerning protective measures should be implemented based on

[RETURN TO TOP](#)

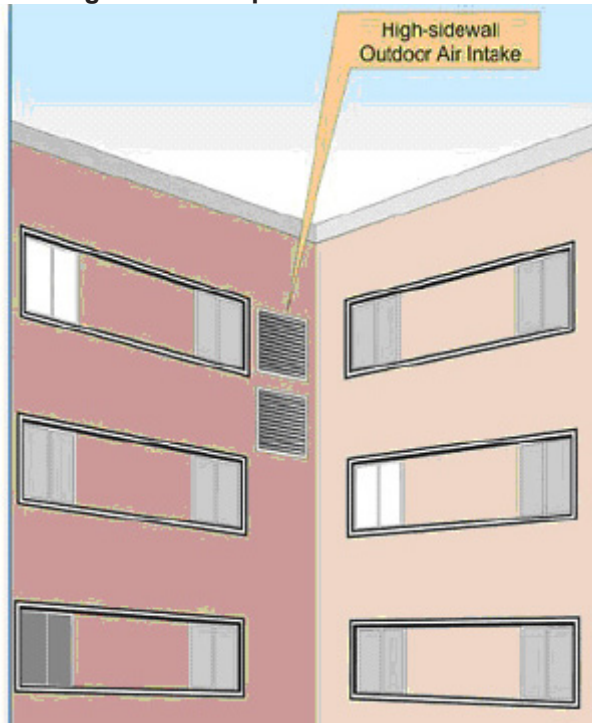
the perceived risk associated with the facility and its tenants, engineering and architectural feasibility, and cost. Specific physical security measures to consider for the protection of the building HVAC system are cited below. HVAC systems must be capable of operating on emergency power (generators).

- C. Windows should be blocked in or hardened to provide the same level of protection as walls. Accordingly, the ventilation system must be designed to support spaces that will be accommodating higher-than-average numbers of personnel without direct openings to the outside.
- D. Physical security for mechanical rooms to prevent the direct introduction of hazardous materials into the system of ducts that distributes air to the building should be maintained. This includes locking and controlling the access to all mechanical rooms containing HVAC equipment.

XV. KEY HVAC SYSTEM CONSIDERATIONS

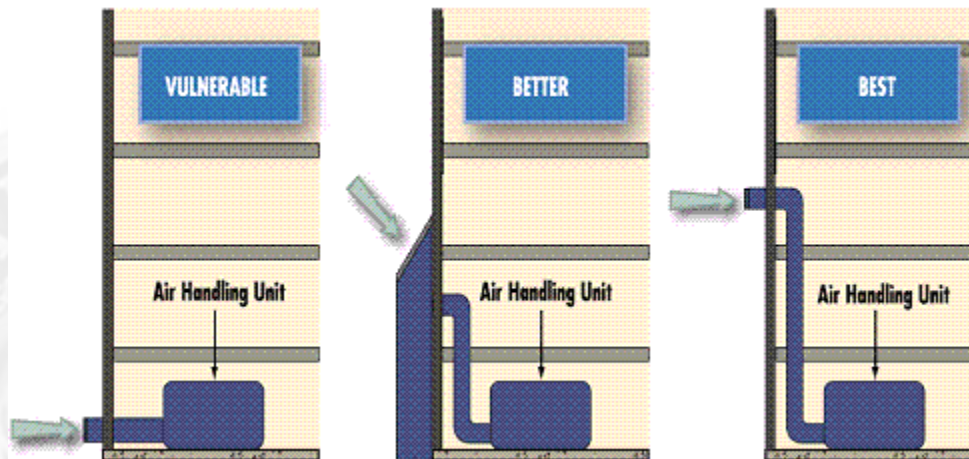
- A. The following HVAC design measures should be considered to mitigate the risk of CBR threats for high security buildings.
 - 1. Placing intakes at the highest practical level on the building is beneficial. For protection against malicious acts, the intakes should also be covered by screens so that objects cannot be tossed into the intakes or into air wells from the ground.
 - 2. Such screens should be sloped to allow thrown objects to roll or slide off the screen, away from the intake. Many existing buildings have air intakes that are located at or below ground level.

Figure 3: Example of Elevated Air Intake



3. For those that have wall-mounted or below-grade intakes close to the building, the intakes can be elevated by constructing a plenum or external shaft over the intake. An extension height of 12 feet will place the intake out of reach of individuals without some assistance.
4. For existing, buildings with air intakes below grade at ground level or wall-mounted outside secure areas, some protection can be gained with physical security measures (e.g., placing fencing, surveillance cameras, and motion detectors around the intakes to facilitate monitoring by security personnel).
5. Physical security for mechanical rooms to prevent the direct introduction of hazardous materials into the system of ducts that distributes air to the building should be maintained. This includes locking and controlling the access to all mechanical rooms containing HVAC equipment.
6. Public access to building roofs should be prevented. Access to the roof may allow entry to the building and access to air intakes and HVAC equipment (e.g., self-contained HVAC units, laboratory or bathroom exhausts) located on the roof. From a physical security perspective, roofs are like other entrances to the building and should be secured appropriately. Roofs with HVAC equipment should be treated like mechanical areas. Fencing or other barriers should restrict access from adjacent roofs.

Figure 4: Example of Protecting Outdoor Air Intake



7. Access to building operation systems by outsiders should be restricted. A building staff member should escort maintenance workers throughout their service visit and should visually inspect their work before final acceptance of the service.

B. Prevent Access to Outdoor Air Intakes

1. One of the most important steps in protecting a building's indoor environment is the security of the outdoor air intakes. Outdoor air enters the building through these intakes and is distributed throughout the building by the HVAC system. Publicly accessible outdoor air intakes located at or below ground level are at most risk – due partly to their accessibility (which also makes visual or audible identification easier) and partly because most CBR agent releases near a building will be close to the ground and may remain there

C. Relocate Outdoor Air Intake Vents

1. Relocating accessible air intakes to a publicly inaccessible location is preferable. Ideally, the intake should be located on a secure roof or high sidewall. The lowest edge of the outdoor air intakes should be placed at the highest feasible level above the ground or above any nearby accessible level (i.e., adjacent retaining walls, loading docks, and handrail).

D. Extend Outdoor Air Intakes

1. If relocation of outdoor air intakes is not feasible, intake extensions can be constructed without creating adverse effects on HVAC performance. In general, this means the higher the extension, the better – as long as other design constraints (excessive pressure loss, dynamic and static loads on structure) are appropriately considered.

(a) An extension height of 12 feet (3.7 m) will place the intake out of reach of

[RETURN TO TOP](#)

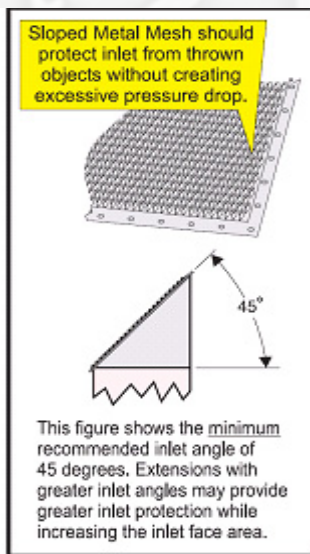
individuals without some assistance.

- (b) Also, the entrance to the intake should be covered with a sloped metal mesh to reduce the threat of objects being tossed into the intake. A minimum slope of 45 degrees is generally adequate.
- (c) Extension height should be increased where existing platforms or building features (i.e., loading docks, retaining walls) might provide access to the outdoor air intakes.

E. Establish a Security Zone around Outdoor Air Intakes

- 1. Physically inaccessible outdoor air intakes are the preferred protection strategy. When outdoor air intakes are publicly accessible and relocation or physical extensions are not viable options, perimeter barriers that prevent public access to outdoor air intake areas may be an effective alternative.
- 2. Iron fencing or similar see-through barriers that will not obscure visual detection of terrorist activities or a deposited CBR source are preferred. The restricted area should also include an open buffer zone between the public areas and the intake louvers. Thus, individuals attempting to enter these protective areas will be more conspicuous to security personnel and the public. Monitoring the buffer zone by physical security, CCTV, security lighting, or intrusion detection sensors will enhance this protective approach.

Figure 5: Minimum Recommended Inlet Angle



F. Secure Return-Air Grilles

- 1. Similar to the outdoor-air intake, HVAC return-air grilles that are publicly accessible and not easily observed by security may be vulnerable to targeting for

CBR contaminants. Public access facilities may be the most vulnerable to this type of CBR attack. A building-security assessment can help determine, which, if any, protective measures to employ to secure return-air grilles. Take caution that a selected measure does not adversely affect the performance of the building HVAC system.

2. Some return-air grille protective measures include:

- (a) Relocating return-air grilles to inaccessible, yet observable locations.
- (b) Increasing security presence (human or CCTV) near vulnerable return-air grilles.
- (c) Directing public access away from return-air grilles.
- (d) Removing furniture and visual obstructions from areas near return-air grilles.

G. Other Accessible Exterior Openings

- 1. All exterior openings larger than 96 square inches which are less than 18 ft above the ground or an adjacent roof must have protection against intrusion. This may consist of special louvers or grids of 15 mm reinforcing bars, placed at 150 mm on center and welded at intersections.

XVI. MAIL ROOM VENTILATION

A. To ensure airborne chemical, biological, and radiological agents introduced into mail rooms do not migrate into other areas of buildings in which the mail rooms are located, provide separate, dedicated air ventilation systems for mail rooms. Refer to the DoD Security Engineering Design Manual for additional guidance, specifically Appendix B, page B16, B-3.4 Standard 13 “Mail Rooms” and page B17, B-4.2 Standard B-17 “Mail Room Ventilation”.

- 1. Also see [United Facilities Criteria \(UFC\) DoD Minimum Antiterrorism Standards for Buildings](#) and [GSA’s Guidelines for Safe Mail Centers](#).

B. Dedicated Exhaust Systems

- 1. Provide dedicated exhaust systems within mail rooms to maintain slight negative air pressures with respect to the remainder of the buildings in which the mail rooms are located so that the flow of air is into and contained in the mail rooms. Though the airflow into the mail rooms will not eliminate the potential spread of contamination by personnel leaving the mail room, it will limit the migration of airborne contaminants through openings and open doorways.

C. Outside Intakes and Exhausts

1. Provide mail room ventilation system outside air intakes and exhausts with low leakage isolation dampers that can be closed to isolate the mail rooms.

D. Isolation Controls

1. Provide separate switches or methods of control to isolate mail rooms in the event of a suspected or actual chemical, biological, or radiological release.

XVII. EMERGENCY AIR DISTRIBUTION SHUTOFF

- A. For all new and existing inhabited buildings, provide an emergency shutoff switch in the HVAC control system that can immediately shut down air distribution throughout the building except where interior pressure and airflow control would more efficiently prevent the spread of airborne contaminants and/or ensure the safety of egress pathways. Locate the switch (or switches) to be easily accessible by building occupants. Providing such a capability will allow the facility manager or building security manager to limit the distribution of airborne contaminants that may be introduced into the building.

B. Utility Distribution and Installation

1. Utility systems can suffer significant damage when subjected to the shock of an explosion. Some of these utilities may be critical for safely evacuating personnel from the building or their destruction could cause damage that is disproportionate to other building damage resulting from an explosion. To minimize the possibility of the above hazards, apply the following measures.

C. Utility Routing

1. For all new inhabited buildings, route critical or fragile utilities so that they are not on exterior walls or on walls shared with mail rooms. This requirement is recommended, but not mandatory, for existing buildings.

D. Redundant Utilities

1. Where redundant utilities are required in accordance with other requirements or criteria, ensure that the redundant utilities are not collocated or do not run in the same chases. This minimizes the possibility that both sets of utilities will be adversely affected by a single event.

E. Emergency Backup Systems

1. Where emergency backup systems are required in accordance with requirements or criteria, ensure that they are located away from the system components for

which they provide backup.

XVIII. FIRE ESCAPES AND BUILDING WALLS

A. Exterior fire escapes usually do not provide access directly into a building. If a fire escape is not properly designed it can provide a potential intruder with easy access to the roof or to openings high above ground level. Physical security safeguards must be coordinated with appropriate fire and safety officials to ensure they do not interfere with emergency systems, procedures, or equipment. In some instances, it may not be possible to reduce completely the physical security hazard posed by a fire escape or similar safety feature. In these cases, alternative security measures are necessary to control identified risks, such as CCTV, IDS, and guard patrols.

1. Windows or other openings leading off fire escapes should meet both security standards and life safety code requirements if they provide potential access points for an intruder. Measures taken to secure windows must be coordinated with the appropriate fire and safety officials to ensure that they do not impede safety processes.
2. To promote security, the fire escape should not extend all the way to the ground. If the fire escape must reach all the way to the ground for safety reasons, alternative security safeguards that meet life safety requirements may be needed.
3. Coordination with fire and safety officials is necessary in relation to any security measures directly affecting the fire and safety systems and procedures.

B. Wall Safeguards

1. Wall structures and masonry barriers present potential vulnerabilities for restricting access at a facility, particularly where light construction or improper securing of structural elements would enable an intruder to gain access. A common example is a shared wall between adjacent rooms, one of which is a restricted area.
2. When a vulnerable wall separating controlled space from an adjacent non-controlled space is identified, countermeasures to reduce risk to an acceptable level are needed. The objective is to secure the wall with a level of physical security to match the value of the assets being protected and the threats.
3. See [Whole Building Design Guide \(WBDG\) Building Types](#) and the [DoD Minimum Antiterrorism Standards for Buildings](#).

C. Extending Interior Wall Construction to Ceiling or Roof Deck

1. This is often possible when the vulnerability is caused by a wall that does not

[RETURN TO TOP](#)

extend entirely from floor to ceiling providing the potential for illicit access over the top of the wall.

2. Possible solutions include extending the wall to the ceiling or constructing an expanded metal barrier to close the intervening space between the top of the existing wall and the ceiling.
3. When the primary concern is merely to detect unauthorized access attempts, lightweight construction such as plasterboard can be used. When lightweight materials are used, consider installation of an intrusion-detection sensor in the ceiling space to detect attempts at forced entry.

D. Reinforced Wall

1. Covering the entire wall with 9-gauge expanded metal may be appropriate to control identified risks.

E. Intrusion-Detection Sensors

1. If the primary concern is that entry may be possible by forcible means without detection, as might be the case in a storage room or similar area, the use of intrusion-detection sensors can be an effective solution.
2. Vibration detectors placed on a wall surface is one way of sensing attempts at forcible entry through a wall.





APPENDIX 7.15: LOADING DOCKS AND SERVICE ACCESS

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

I Loading Docks And Service Access

A. General

1. Loading docks and service access areas are commonly required for a building and are typically desired to be kept as invisible as possible. For this reason, special attention should be devoted to these service areas in order to avoid undesirable intruders. Design criteria for loading docks and service access include the following:

- (a) Separate (by at least 50 feet) loading docks and shipping and receiving areas in any direction from utility rooms, utility mains, and service entrances, including electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.
 - Locate loading docks so that vehicles will not be allowed under the building. If this is not possible, the service should be hardened for blast. Loading dock design should limit damage to adjacent areas and vent explosive forces to the exterior of the building;
 - Monitor any necessary loading zones or drive-through areas and restrict height to keep out large vehicles;
 - Avoid having driveways within or under buildings;
 - Provide adequate design to prevent extreme damage to loading docks. Significant structural damage to the walls and ceiling of the loading dock may be acceptable; however, the areas adjacent to the loading dock should not experience severe structural damage or collapse. The floor of the loading dock does not need to be designed for blast resistance if the area below is not occupied and/or does not contain critical utilities; and
 - Provide signage to clearly mark separate entrances for deliveries.

B. Loading Dock Roll-up Doors

1. Roll-up doors should be equipped with a balanced magnetic switch interlocked with a CCTV camera to automatically train the TV camera on the area inside the door when the door is open.
2. Overhead roll doors not controlled or locked by electric power should be protected by slide bolts on the bottom bar. Chain link doors should be provided with an iron keeper and pin for securing the hand chain, and the shaft on a crank operated door should be secured. A solid overhead, swinging, sliding, or accordion type garage door should be secured with a cylinder lock or padlock.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Also, a metal slide bar, bolt or crossbar should be provided on the inside. Metal accordion grate or grill-type doors should have a secured metal guide track at the top and bottom and be secured with a cylinder lock or padlock.

C. Loading Dock Personnel Doors

1. A card reader should be provided at the personnel door of the loading dock. A balanced magnetic switch interlocked with a CCTV camera should be provided. The interlock should automatically train the TV camera on the inside of the door when the door is open. A local alarm should be set off at the same time.
2. Loading docks and receiving and shipping areas should be separated by at least 50 feet in any direction from utility rooms, utility mains, and service entrances including electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc. Loading docks should be located so that vehicles will not be driven into or parked under the building. If this is not possible, the service shall be hardened for blast.

D. Critical Building Components

1. The following critical building components should be located no closer than 50 feet in any direction to any main entrance, vehicle circulation, parking, or maintenance area (project-specific information to be provided). If this is not possible, harden as appropriate:
 - (a) Emergency generator including fuel systems, day tank, fire sprinkler, and water supply;
 - (b) Normal fuel storage;
 - (c) Main switchgear;
 - (d) Telephone distribution and main switchgear;
 - (e) Fire pumps;
 - (f) Building control centers;
 - (g) UPS systems controlling critical functions;
 - (h) Main refrigeration systems if critical to building operation;
 - (i) Elevator machinery and controls;
 - (j) Shafts for stairs, elevators, and utilities; and
 - (k) Critical distribution feeders for emergency power.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

E. Additional Features

1. Areas of Potential Concealment

- (a) To reduce the potential for concealment of devices before screening points, avoid installing features such as trash receptacles and mail boxes that can be used to hide devices. If mail or express boxes are used, the size of the openings should be restricted to prohibit insertion of packages.

II. POWER FOR CRITICAL BUILDING COMPONENTS AND SECURITY SYSTEMS

A. General

1. CBP requires that all alarm systems, CCTV monitoring devices, fire protection systems, public address systems and access control devices, etc., be connected to emergency power sources. The tenant is responsible for determining which computer or communication systems require backup power.
2. Regardless of the quality of design and installation, most access control systems are vulnerable to electric power losses. Some systems may not be able to reset automatically and would require operator intervention to restore. Potential intruders may be aware of these vulnerabilities and may seek to cut or interrupt power if they cannot circumvent the system by other means. It is critical that all elements of the system have backup power systems incorporated into the design and operation to guarantee the system's uninterrupted integrity, alarm reporting, situation assessment, and the response force's reaction.
3. Consultations during the design phase of an access control system are the best time to define power, line conditioning, and battery or other backup power requirements. Backup power for fixed systems may be from uninterruptible power supplies (UPS), generators, or automatic bus power transfer switches.

B. Commercial Power

1. Primary electrical power for non-portable security equipment should be commercial alternating or direct current.
2. If a risk assessment determines that commercial electrical power distribution hubs need to be secured, strongroom standards are to be applied to electrical vaults, rooms and closets. For further information, see [Appendix 8.8, Strongrooms](#).

C. Emergency Generators

1. Emergency backup generators must be located away from loading docks, entrances, and parking areas. More secure locations include roofs, protected

[RETURN TO TOP](#)

grade levels (building exterior) and protected interior areas. The generator should not be located in any areas that are prone to flooding. Emergency backup generators must be designed in compliance with [UFC 3-540-04N](#). Emergency generators should be located at least 100 feet from communications frame equipment to avoid radio frequency interference and they must provide 150% of the present design loads of the facility.

2. The generators shall serve distribution panel boards in the main electrical room through a 4-pole automatic transfer switch (ATS). This emergency system shall provide power for the life safety/security systems and other essential loads upon failure of the normal electrical power service for a minimum of 72 hours (120 hours for remote locations) continuous operation prior to re-fueling.

D. Generators Located Outdoors

1. If the emergency generator is to be installed outdoors, it should be housed in a structure that is constructed to strongroom standards and have provisions to ensure reliable starting in cold weather. For more information refer to [Appendix 8.8, Strongrooms](#).
2. Physical access to the emergency generator must incorporate an access control system and be monitored with CCTV to protect it from sabotage. For more information refer to [Chapter 11, Access to Facilities](#) or [Appendix 8.12, CCTV](#).
3. Provide security fencing around all enclosures housing emergency generators to ensure safety and prevent unauthorized access. For enclosures within fenced perimeter provide standard 8ft. fence and if stand alone provide 12-foot impound lot fence. For more information refer to [Appendix 7.3, Fencing](#).

E. Generators Located Indoors

1. Emergency generators that are installed indoors will be housed in rooms constructed to strongroom standards.
2. To prevent unauthorized access to the generator, incorporate an access control system and CCTV.

F. Generator Doors

1. Material:
 - (a) Doors must be constructed of 12-gauge steel clad hollow core metal, and hung in hollow metal frames.
2. Hardware:
 - (a) Tamperproof with high security deadlock and no master key. Provide card

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

reader/keypad to track users, but not as a substitute for a deadlock. The card reader shall be integrated to the locking mechanism. One shouldn't work without the other. Appropriately authorized card and key should be necessary for access. The door must be fitted with a UL 437 approved high security locking cylinder dead bolt lock (or equivalent). The keying must be different from all other keys and must be keyed off a master key.

(b) For further information on generator door hardware, see [Appendix 7.6. Doors and Door Hardware](#).

G. The electrical load of the Emergency Generator should include the following critical building systems/functions (this list is not all inclusive):

1. Egress and exit lighting;
2. Fire alarm system;
3. Generator auxiliaries;
4. Smoke control systems (if required by code);
5. Fire pump;
6. Lighting;
7. Telephone switch;
8. Security systems;
9. Mechanical control systems;
10. Building Automation System (BAS);
11. Elevators (one per bank);
12. Sump pumps;
13. Sewage ejector pumps;
14. Exhaust fans removing toxic, explosive or flammable fumes; and
15. Uninterruptible power systems (UPS) serving computer rooms
 - (a) Air conditioning systems for computer and UPS rooms;
 - (b) Exhaust fan in UPS battery rooms;
 - (c) Power and lighting for Fire Control Center and Security Control Center;

[RETURN TO TOP](#)

- (d) Lighting for main electrical room, electrical closets, and communications closets;
- (e) Air conditioning systems for communications closets;
- (f) Emergency power receptacles;
- (g) Horizontal sliding doors; and
- (h) Other associated equipment designated by code.

H. Uninterruptible Power Supply (UPS)

1. All electrical and electronic equipment shall be powered from a UPS provided as specified in [UFGS-26 32 33.00 10](#)
 - (a) Uninterruptible Power Supply (UPS) System above 15 KVA Capacity
2. Battery power units must comply with Underwriters Laboratories (UL)
 - (a) National Industrial Security Systems (UL 2050)
3. The UPS shall be sized to provide at least 24 hours battery back-up in the event of primary failure. Batteries will be of the sealed non-gassing type.
4. If batteries are used as auxiliary electrical power, they will be maintained at full electrical charge by automatic charging circuits

I. Microprocessor Based Systems

1. Uninterruptible power supply systems shall be furnished and installed to supply power to all microprocessor based systems. This shall include, but not be limited to:
 - (a) Communication systems;
 - (b) Intrusion detection system (IDS) and duress alarm control equipment;
 - (c) Automated access control multiplexers, controllers, and central processing units;
 - (d) Closed circuit television (CCTV) multiplexers, switchers, recorders; and
 - (e) Alarm signal transmission equipment.
2. It is the intent that if normal power is interrupted the state of the microprocessor will not be altered, nuisance and false indication alarms are not generated, and volatile memory will not be lost.

3. Systems controlled by the microprocessor are not required to remain in a fully operational state during the power transition period, provided that:
 - (a) The security of the facility is not compromised for any period of time due to an unlocked condition, and
 - (b) Power shall be interrupted to all electrified locking hardware in a fire or smoke alarm zone that is in an alarm condition.

J. Locking Systems

1. Uninterruptible power supply systems shall be furnished and installed to supply power to all fail safe electromechanical locking systems. This shall include, but not be limited to:
 - (a) Magnetic locks;
 - (b) Electric strikes;
 - (c) Electrified spring and dead bolts.
2. It is the intent that if normal power is interrupted the security of the facility is not compromised for any period of time due to an unlocked condition, and access through electrically controlled locks may be affected.

K. Security Lighting Systems

1. Security Lighting Systems that use high intensity discharge lamps to provide illumination to critical areas will be provided UPS service if incandescent or fluorescent lamps are not used as backup lighting.
2. Uninterruptible power will be supplied until a transfer to emergency back up power can be completed.

III Communications Room (Telephone and Radio)

A. Description

1. A communications room, separate from the computer room, is required to house and support CBP telecommunications and radio equipment and connections. In addition to provisions for an IDS that provides perimeter and volumetric protection/detection of unauthorized access, special construction details are required for this room including the installation of 9-gauge diamond mesh expanded metal wall/ceiling reinforcement or 8-in. concrete masonry units (CMU). The installation of 9-gauge diamond mesh expanded metal must be inspected by CBP prior to covering. Provide tamperproof hardware with a UL-437 compliant cylinder or equal high security deadlock with no master key.

[RETURN TO TOP](#)

2. A card reader/keypad must be provided in addition to, but not as a substitute for, the deadlock allowing CBP to track access by users. All necessary cabling and conduit must be provided to support the equipment furnished and installed by the government.

B. Communications Room Technical Design Standards

1. IDS:

- (a) Provide IDS and alarm with UPS backup monitored on a 24-hour basis by the security office. Provide keypad control inside room adjacent to entry door.

2. Walls:

- (a) 3/4-in. fire resistant painted plywood over 9-gauge diamond mesh (1 1/2-in. X 2-in. maximum diamond) expanded metal securely fastened to metal studs. 3/4-in. plywood over 8-in. CMU is also acceptable.

3. Ceiling:

- (a) 5/8-in. gypsum board over 9-gauge diamond mesh (1 1/2-in. X 2-in. max. diamond) expanded metal. Overlap joints.

4. Material:

- (a) 1 3/4-inch solid core wood or 12-gauge steel clad hollow metal door and frame.

5. Hardware:

- (a) Tamperproof hardware with a UL-437 compliant cylinder or equal high security deadlock. No master key. At mid-size and large airports, also provide a card reader / keypad in addition to, but not as a substitute for, the deadlock allowing CBP to track.

6. Provide all necessary cabling and conduit to support the equipment furnished and installed by the government.

7. Special construction note:

- (a) Installation of 9-gauge diamond mesh expanded metal wall / ceiling reinforcement must be inspected by CBP prior to covering.

IV General Storage/File Room

A. Description

1. The general storage / file room is required for the storage of CBP supplies, equipment, files and other miscellaneous items required for CBP operations. Eighteen inch deep heavy-duty adjustable metal shelving and filing cabinets are required as specified by CBP.

B. General Storage/File Room Technical Design Standards

1. Fixed Security Equipment 18-in. deep heavy-duty adjustable metal shelving, filing cabinets as specified by CBP.
2. Walls:
 - (a) 5/8-in. gypsum board over metal studs.
3. Ceiling:
 - (a) 5/8-in. gypsum board. Acoustical tile not permitted.
4. Material:
 - (a) 1 3/4-in. wood or hollow metal, 40-42 inches wide, in hollow metal frame.
5. Hardware:
 - (a) Standard lockset keyed individually and to a CBP master.

V Secure Storage Room(s)

A. Description

1. The Secure Storage Room is specified by CBP for the secure storage of documents, seized narcotics, and other contraband. In addition to provisions for IDS that provides perimeter and volumetric protection/detection of unauthorized access, special construction details are required for this room including the installation of 9-gauge diamond mesh expanded metal wall / ceiling reinforcement or 8-in. CMU. The installation of 9-gauge diamond mesh expanded metal must be inspected by CBP prior to covering.

B. Secure Storage Room(s) Technical Design Standards

1. IDS: For each secure room, provide IDS and alarm with
 - (a) Uninterruptible Power Supply (UPS):

[RETURN TO TOP](#)

- UPS backup monitored on a 24-hour basis by the airport security office. Provide keypad control inside room adjacent to entry door.

(b) Closed-Circuit Television (CCTV):

- Fixed CCTV camera w/wide-angle lens in room to be monitored and recorded at the CCC or other CBP designated location.

2. Floor:

- (a) Resilient tile over concrete slab.

3. Walls:

- (a) 5/8-in. gypsum board over 9-gauge diamond mesh (1 1/2-in. X 2-in. max. diamond) expanded metal securely fastened to metal studs. Overlap joints. 8-in. concrete masonry units are also acceptable.

4. Ceiling:

- (a) 5/8-in. gypsum board over 9-gauge expanded metal.

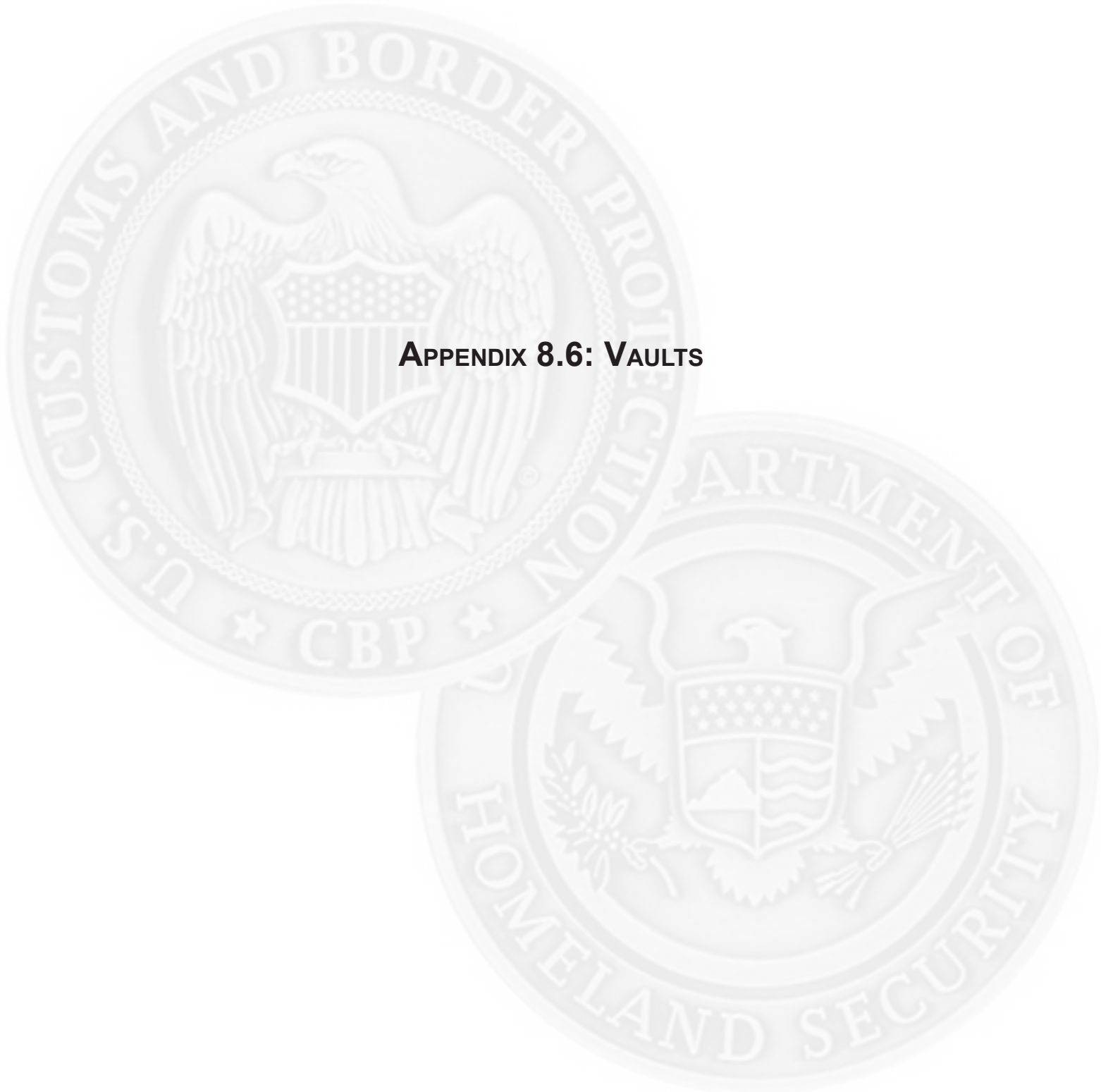
5. Material:

- (a) 1 3/4-in. solid-core wood or 12-gauge steel clad hollow metal door and frame.

6. Hardware:

- (a) Tamper-proof hardware with a UL-437 compliant cylinder or equal high security deadlock. No master key. At mid-size and large airports, also provide a card reader/keypad in addition to, but not as a substitute for, the deadlock thus allowing CBP to track users.





APPENDIX 8.6: VAULTS

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

I. CBP VAULT MINIMUM STANDARDS

A. General

1. A vault is a completely enclosed space with a high degree of protection against forced entry. Vaults are commonly used for storing Top Secret information, special access program information, and extremely valuable materials.
2. This appendix pertains to the permanent or temporary storage of seized drugs (narcotics/controlled substances), weapons, ammunition, and other high-value items. Temporary storage refers to storage of 72 hours or less. Permanent storage refers to a length of storage greater than 72 hours.
3. For more information on temporary storage only, please refer to the Strong Room Construction Standards in [Appendix 8.8, Strongrooms](#).

B. Scope

1. This document establishes minimum construction requirements for CBP Vaults, for Armory standards refer to [Appendix 10: Storage of Weapons and Ammunition](#). The following vault standards apply to all new construction, reconstruction, alterations, modifications, and repairs to existing vaults. All vaults shall have an Intrusion Detection System ((IDS), see [Chapter 8.9, IDS](#); a Closed Circuit Television System ((CCTV), see [Chapter 8.12, CCTV](#)); and an Access Control System (see [Chapter 11, Access to Facilities](#)).

C. Referenced Documents

1. Government Publications:
 - (a) The following documents outline vault minimum standards:
 - Federal Standard Construction Methods and Materials for Vaults
 - [FED-STD 832](#)
2. Vault Systems:
 - (a) [AA-V-2737](#), Modular Vault Systems, 25 April 1990
 - (b) [AA-V-2737 Amendment 2](#), Modular Vault Systems, 30 October 2006
 - (c) [QPL-AA-V-2737-5](#), Modular Vault Systems, 17 October 2007
 - (d) [AA-V-2940](#), Vault System, Armory, Assembled, 20 February 2008
3. Vault Door:

[RETURN TO TOP](#)

- (a) [AA-D-600D](#), Door, Vault, Security, 15 May 2000
- (b) [AA-D-600D Amendment 2](#), Door, Vault, Security, 20 April 2007
- (c) [QPL-AA-D-600-8](#), Door, Vault, Security, 20 May 2008

4. Locks:

- (a) [FF-L-2740 Locks, Combination](#)
- (b) [QPL-FF-L-2740-8 Products Qualified Under Federal Specification FF-L-2740](#)
- (c) [FF-L-2937 Combination Lock, Mechanical 05](#)
- (d) [FF-L-2937 Combination Lock, Mechanical Amendment 2](#)
- (e) [CIS HB 4400-01A Seized Asset Management & Enforcement Procedures Handbook 2002](#)

5. General Requirements for Vaults:

- (a) There are three classes of vaults for the storage of classified material and equipment A, B and C. Class A vaults offer the maximum protection against tool and torch attack. Class B vaults offer less than maximum protection. A lightweight, portable “modular vault” meeting Federal Specification AA-V-2737 may also be used to store classified material and equipment. The modular vault is equivalent to a Class B vault Class C vaults offer less than maximum protection and may be used where unique structural circumstances do not permit construction of concrete vault construction. Utilization of any vault class, or the modular vault, is dependent upon the physical location environment where the vault is to be erected. Reference: [FED-STD 832](#) (This document establishes minimum construction requirements for all Federal agencies for high security vaults for storage of classified information and weapons).

D. The minimum construction requirements for each class of vault are described as follows.

1. Detailed Requirements:

(a) Class A Vaults. Minimum Construction. Required for New Construction

- Vault Walls. The walls of class A vaults shall be constructed of 8-inch thick (200 mm) reinforced concrete. Concrete reinforcement shall consist of 5/8-inch (16mm) re-bar, 6 inches on center each way, staggered each frame. The walls are to extend to the underside of the roof slab

[RETURN TO TOP](#)

above. When vault walls are adjacent to the exterior walls, the vault wall must be set back from the exterior part of the exterior wall to allow 4 inches (100 mm) for the normal wall facing to cover the vault wall. Wall reinforcement shall be tied into floors and ceilings;

- Vault Floor. The floor of class A vaults shall be constructed of 8 inch thick (200 mm) reinforced concrete. Concrete reinforcement shall consist of # 5 rebar (5/8 inch-16 mm), 6 inches on center each way, staggered each frame;
- Vault Ceiling. The ceiling of class A vaults shall be constructed of monolithic reinforced concrete 8 inch thick (200 mm). Concrete reinforcement shall consist of # 5 rebar (5/8 inch-16 mm), 6 inches on center each way, staggered each frame;
- Vault Door. Vault door and frame shall conform to Federal Specification AA-D-600;
- Miscellaneous Openings. Any miscellaneous openings, open ducts, pipes, registers, sewers in excess of 96 square inches (619.2 centimeters) in area and over 6 inches (15.24 centimeters) in its smallest dimension shall be equipped with barriers. Acceptable barriers are 9 gauge expanded metal mesh, or rigid metal (steel) bars at least one-half inch in diameter, welded vertically and horizontally 6 inches on center. The rigid metal bars shall be securely fastened at both ends to preclude removal. Crossbars shall be used to prevent spreading of the bars. Solid caulking shall be used between the sleeve or conduit to give evidence of surreptitious entry attempt. Access for inspection of barriers should be in accordance with agency policies. Note figure 1.
- For further information, see [Vault Door Guidance](#).

(b) Class B Vaults. Minimum Construction.

- Construction. Class B vault shall conform to Federal Specification AA-V-2737.
- Class B vaults are GSA approved modular vaults and shall be six (6) sided (floor, ceiling, and four sides) as specified in [AA-V-2737](#).
- Vault door. Vault door and frame shall conform to Federal Specification AA-D-600, Class 5 vault door.

(c) Class C Vaults. Minimum construction for steel-lined vaults.

- Vault construction. Where unique structural circumstances do not

[RETURN TO TOP](#)

permit construction of concrete vault, construction will be of steel alloy-type of 1/4 inch thick, having characteristics of high yield and tensile strength. The metal plates are to be continuously welded to load-bearing steel members of a thickness equal to that of the plates. If the load-bearing steel members are being placed in a continuous floor or ceiling of reinforced concrete, they must be firmly affixed to a depth of one-half the thickness of the floor and ceiling. If the floor and/or ceiling construction is less than six inches of reinforced concrete, a steel liner is to be constructed the same as the walls to form the floor and ceiling of the vault. Seams where the steel plates meet horizontally and vertically are to be continuously welded together;

- Vault Ceiling and Floor. If the floor and/or ceiling construction is less than six inches of reinforced concrete, a steel liner is to be constructed the same as the walls to form the floor and ceiling of the vault. Seams where the steel plates meet horizontally and vertically are to be welded together;
- Vault Door. Vault door and frame shall conform to Federal Specification AA-D-600, Class 5 vault door; and

E. See [Chapter 8.7, Vault Doors](#), for more information.

F. Vault door guidance for all vault types follow:

1. Vault door and frame shall conform to Federal Specification AA-D-600, Class 5 vault door.
2. Armory vault doors and security vault doors are both manufactured according to Federal Specification AA-D-600, Door, Vault, Security. The difference between the two doors is that armory vault doors, used to protect AA&E, are fitted with UL Standard 768, Group 1, mechanical combination locks. Security vault doors, used to protect classified information, are fitted with locks meeting Federal Specification FF-L-2740, Locks, Combination. The armory vault door label (silver with red letters) states that it is a “GSA Approved Armory Vault Door.” The security vault door label reads “GSA Approved Security Vault Door” (label also silver with red letters).
3. There are numerous GSA-approved Class 5 security vault doors being used for the protection of weapons, which is authorized under ([AA-D-600D](#)), however It is strongly recommend that locks be changed out to the UL Standard 768, Group 1, mechanical combination lock, when and if a failure occurs with an X-07, X-08 or X-09 lock. When that change is made it must be noted on the [Optional Form 89](#) (Maintenance Record for Security Containers/Vault Doors). It shall also be noted on the front of the armory door that is not authorized for the protection of classified information.

[RETURN TO TOP](#)

4. Miscellaneous Openings. Any miscellaneous openings, open ducts, pipes, registers, sewers in excess of 96 square inches (619.2 centimeters) in area and over 6 inches (15.24 centimeters) in its smallest dimension shall be equipped with barriers. Acceptable barriers are 9 gauge expanded metal mesh, or rigid metal (steel) bars at least one-half inch in diameter, welded vertically and horizontally 6 inches on center. The rigid metal bars shall be securely fastened at both ends to preclude removal. Crossbars shall be used to prevent spreading of the bars. Solid caulking shall be used between the sleeve or conduit to give evidence of surreptitious entry attempt. Access for inspection of barriers should be in accordance with agency policies. Note [Figures 1](#) and [2](#).

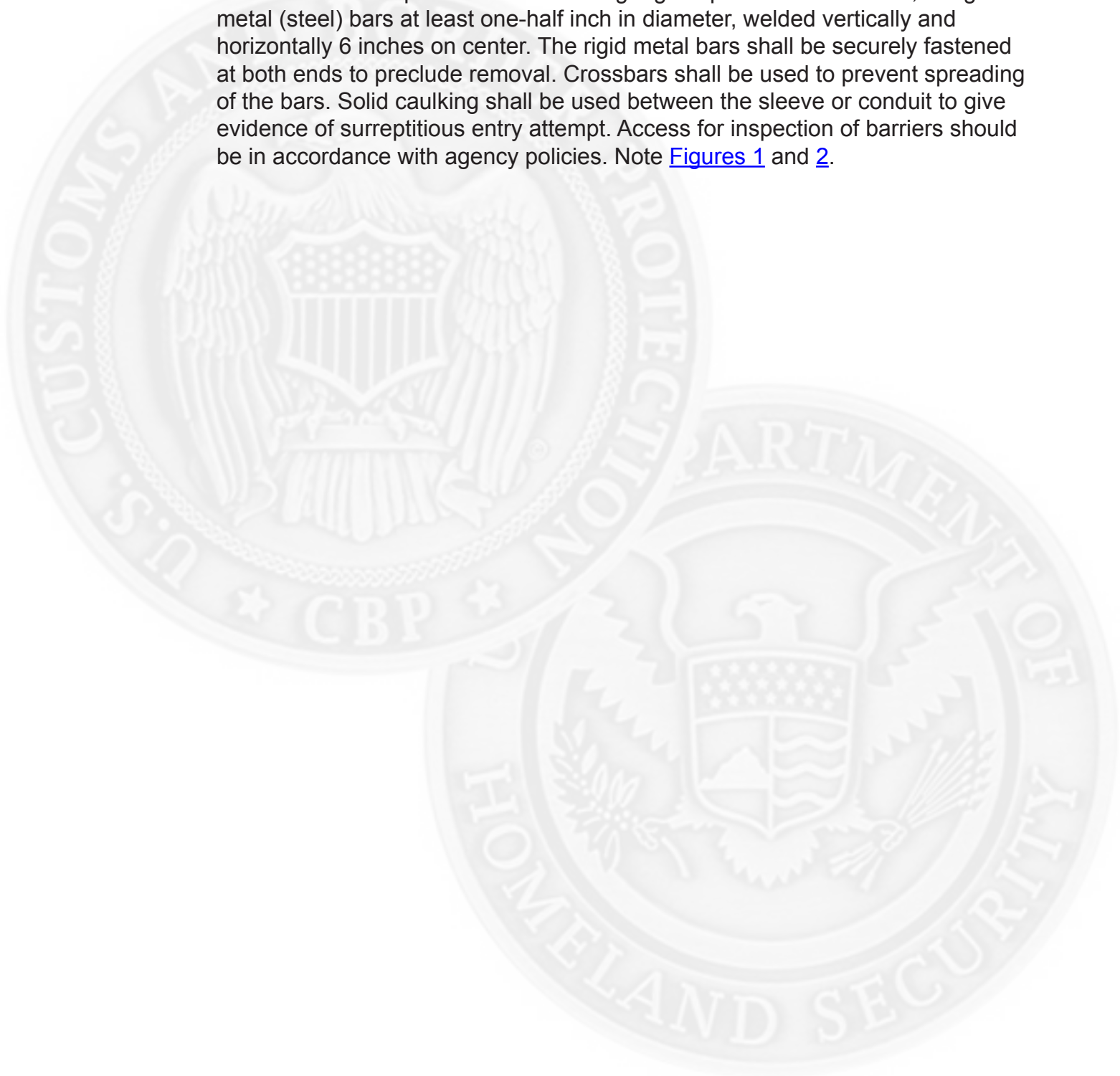
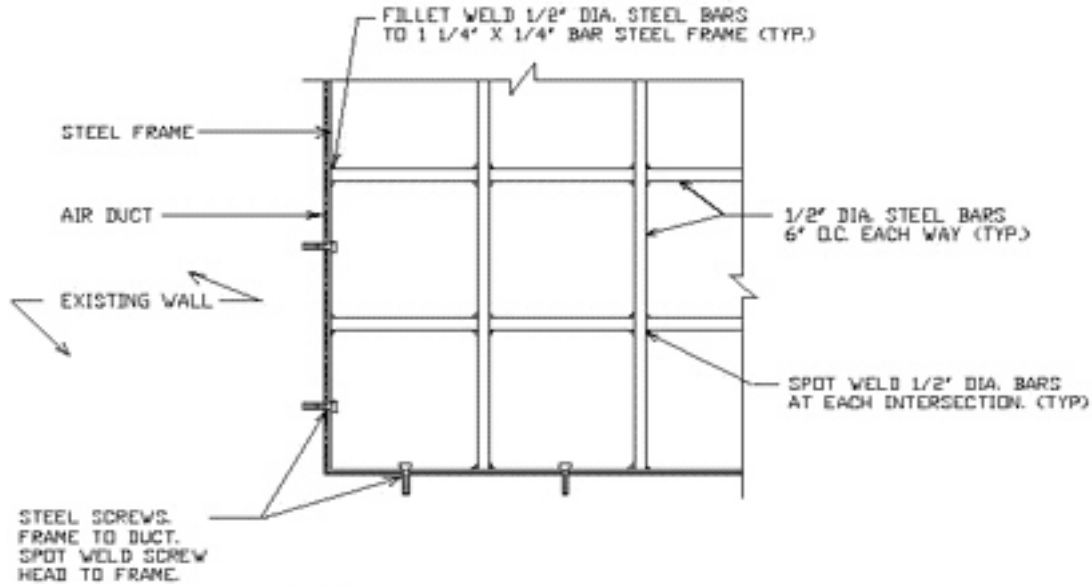


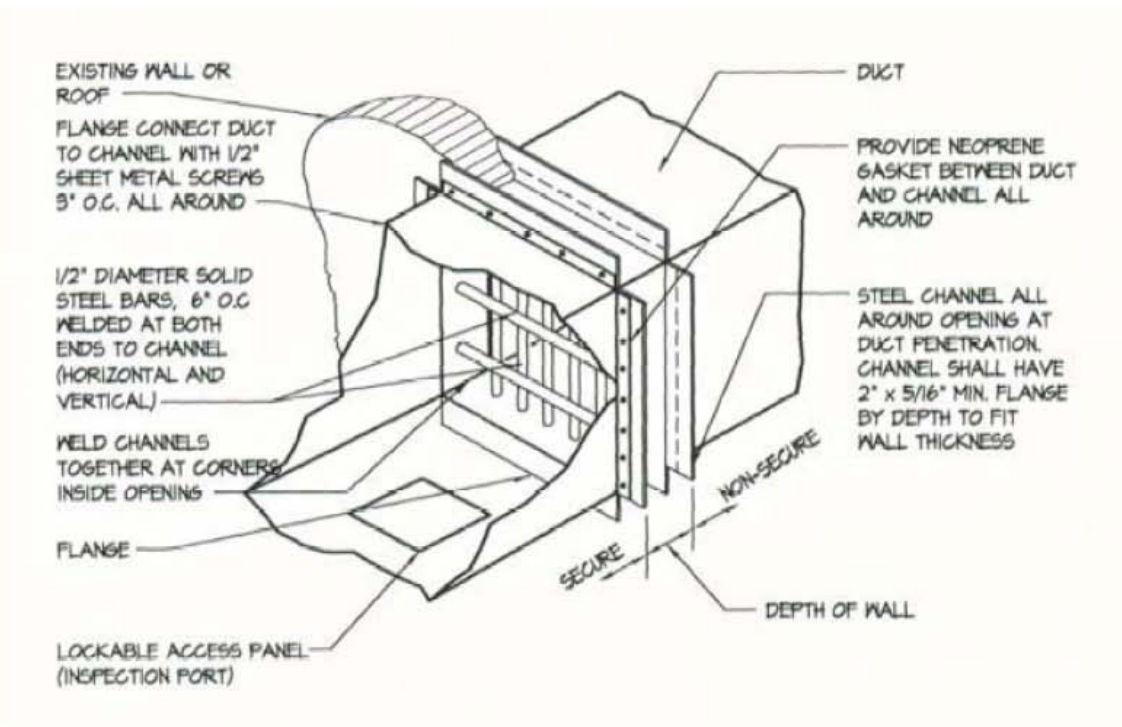
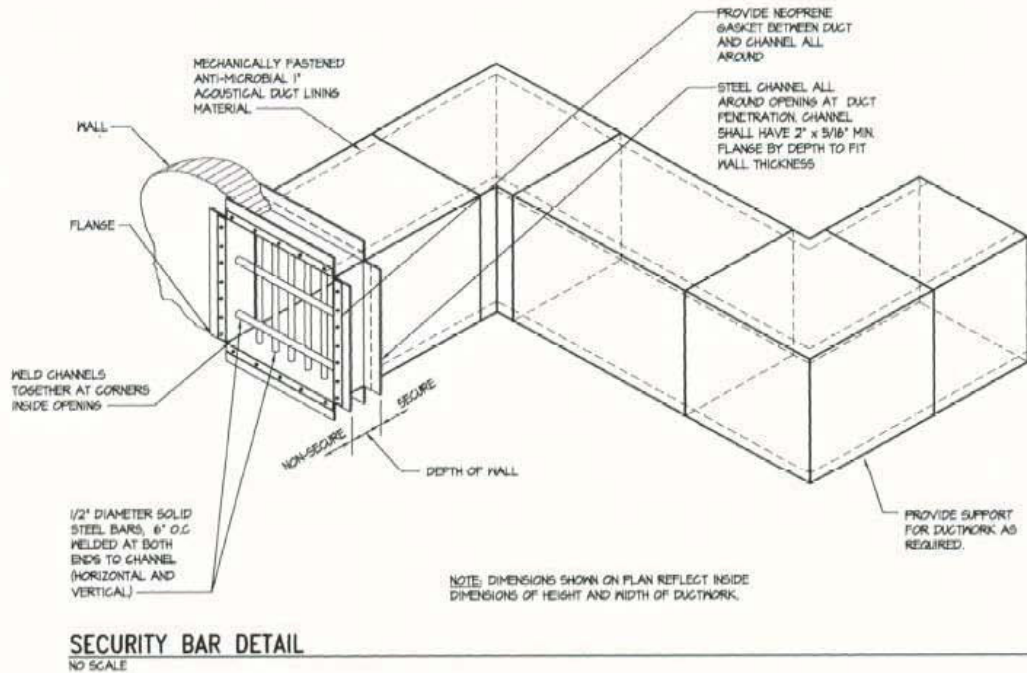
Figure 1: Manbar Barrier



NOTE:
MANBARS SHALL BE REQUIRED FOR ANY PENETRATION LARGER THAN 96 SQ.IN OF ANY PERIMETER WALLS, GUN VAULTS, AND EVIDENCE ROOMS.

NOT TO SCALE
REV: 02-01-2007

Figure 2: Security Bar Detail



BACK

[Return to Table of Contents](#)

Federal Specification: AA-D-600D

Title: Federal Specification Door, Vault, Security

Scope: This specification covers vault doors that are designed to conform to the minimum standards for physical security equipment as required by the Information Security Oversight Office Directive governing the safeguarding of national security information. The doors provide protection against unauthorized entry for the periods of time specified.

Classes: Class 5-V:

Security vault door shall be resistant to 20 man-hours surreptitious entry, 30 man-minutes covert entry and 10 man-minutes forced entry.

Class 5-A:

Armory vault door shall be resistant to 30 man-minutes covert entry and 10 man-minutes forced entry.

Class 5-B:

Ballistic vault door shall be resistant to 20 man-hours surreptitious entry, 30 man-minutes covert entry, 10 man-minutes forced entry, ballistic resistant.

[RETURN TO TOP](#)

GSA Approved Armory Vault Doors

All armory vault doors listed below are Class 5 and are fitted with a UL Standard 768 combination lock. GSA approved armory vault doors can be purchased direct from the manufacturers using the National Stock Numbers listed below. See the Order tab for manufacturer information.

NSN Description

7110-01-475-9598 Left hand swing, without optical device.

7110-01-475-9596 Right hand swing, with optical device.

7110-01-475-9595 Right hand swing, without optical device.

7110-01-475-9593 Left hand swing, with optical device.

7110-01-475-9590 Double leaf, right opening swing active leaf, with optical device.

CLASS	SPECIFICATIONS	INSULATED	AVAILABLE	PROTECTION
5	AA-D-600	No	Yes	10 Minutes forced entry; 30 minutes covert entry; 20 hours surreptitious entry
6	AA-D-600	No	No	Nor forced entry requirement; 30 minutes covert entry; 20 hours surreptitious entry
8	AA-D-2757	No	No	15 Minutes forced entry; 30 minutes covert entry; 20 hours surreptitious entry

5. General Services Administration label. The label shall be affixed to the outside face of the door. The label shall have a silver background and red letters not less than 3 mm in height. The label shall show the following:

**GENERAL SERVICES ADMINISTRATION
APPROVED SECURITY VAULT DOOR
MANUFACTURER'S NAME**

- (a) Identification label. The label shall be affixed to the inside face of the door frame. The label shall show the door model and serial number, date of manufacture, and Government contract number.
- (b) Certification label. A certified label shall be affixed to the inside face of the door bearing the following certification:

6. Day Gate. Vaults shall have self-closing class 5 metal day gate with an automatic locking device controlled by key on the outside of gate. The gate shall be constructed of expanded mesh or solid bars finished to match vault door and

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- frame. The day gate must have a key lock that is manipulation resistant (UL-437), high security, and is keyed off-master. The thumb throw latch release shall be on the inside of the gate, with thumb throw accessible only to the inside.
7. Vault Vestibule. A vestibule is required in a vault when access to the vault or secured area is in public view. If a vault contains a vestibule, the entrance portal shall contain a 12-gauge hollow metal door and frame. The door shall be equipped with a tamper resistant UL-437 dead bolt and keyed lock set.
 - (a) For large vaults, an overhead door leading from the vestibule to the exterior may be installed.
 - Overhead doors will be the roll up, flush fitting type. The door will be metal, dual slat manufactured with 12, 14, or 16-gauge exterior slats and 18, 20, 22, or 24-gauge interior slats with insulated centers. The doors are to be factory fitted with a slide bolt that can be extended through each of the metal slide rails. Each slide bolt will be fitted to the door within 6 inches of the floor and designed to accommodate the use of a high security padlock. A dealer after-market, manufacturer approved slide bolt locking system will be acceptable. The doors will be fitted with the appropriate electric motor system supplied by the manufacturer. The motor system shall have a manual override feature in the event the motor fails. Chains used to operate the door manually shall be of such a length that the door can be easily operated from the floor. An eyebolt will be affixed into the concrete in the area of the chain to allow the use of a high security padlock as an additional security feature. The electric control buttons and the manual override feature will be located so that they cannot be reached by cutting a hole through the door.
 8. Physical Segregation Within the Vault. The vault must be segmented into High Risk vs. Low Risk. High Risk must further be segmented into Drugs vs. Currency and Monetary Instruments vs. all other High Risk Seizures. Finally Drugs must be segmented into Hard vs. Soft. Although not mandated, many vaults have included a staging segment for contraband that is to be destroyed. Each storage segment must have a separate zone in the IDS. The method of physical segregation will be accomplished with the use of metal cage structures with the caging running true-floor to true-ceiling with sliding cage doors. Cages are to be constructed of 9-gauge mesh. The mesh opening must be small enough to preclude anyone reaching in with a hand or even a finger and manipulating the lock or removing stored material. The color of the mesh will be in accordance with industry standard. All anchoring bolts to the floor, wall(s) and ceiling must be torqued down in keeping with the manufacturer's specifications and spot welded so that the anchoring bolts cannot easily be removed. Each cage door will be secured by a lock meeting UL-437. As stated earlier the placing of the

[RETURN TO TOP](#)

steel plates to accommodate the keypads is acceptable. Additionally, there will be sufficient CCTV coverage for each storage area (e.g. in the aisles between shelving). CCTV coverage will depend on the configuration and layout of the vault.

(a) Storage Cage Construction: Separate storage areas in the room must be provided for hard narcotics (heroin and similar drugs), soft narcotics (vegetative drugs such as marijuana) and items of value (currency, jewelry and weapons). Separate 9 gauge expanded metal cages must be used for narcotics with a separate cage for soft and hard narcotics each. The cages shall be constructed of 9 gauge expanded metal mesh securely welded to 42 mm (1.75 inch) steel angle structural frame on 450 mm (18 inch) on center, with 3mm (1/8 inch wide) 50 mm (2 inch long) welds at every 400 mm (16 inches) on center at all seams and joints. The partition shall have an integral gate. The gate shall have a single padlock meeting the requirements of Federal Specification FF-P-2827A . The lock shall be protected from tampering by a 6 mm (0.25) metal plate. Gate hinge pins shall be non removable.

(b) Items of value must be stored in a GSA Class VI storage container located inside the permanent seizure storage room. All storage containers must be protected with intrusion detection system. Each cage or cabinet door must have balanced magnetic switches indicating if the door is open and the lock is engaged. Access control system must be provided on storage containers for hard and soft narcotics. The cage or cabinet doors must be under camera video surveillance.

9. Independent Storage Structure. If the permanent seizure storage is located in a separate structure more than 150 meters (500 feet) from other occupied facilities, or is larger than 28 square meters (300 square feet), then the building must be equipped with male and female toilet facilities. Permanent seizure storage located in a separate structure will require mechanical, electrical, telephone and janitor closet space. Physical plant equipment spaces must not open directly into storage areas. Exhaust and air supply vents must be located remote from any direct exhaust from storage areas. Permanent seizure storage located in separate structures must be surrounded by security fences. The fences must be located a minimum of 6 meters (20 feet) from the structure, providing a buffer zone for security monitoring. The fence must be a minimum of 2.4 meters (10 feet) high, and have a sloped top or be topped with concertina wire. The perimeter of the permanent seizure storage must be under camera video surveillance with adequate site lighting.

10. Windows. No newly constructed vaults shall have windows.

11. Closed Circuit Television (CCTV). The entire exterior and interior of the vault must be monitored by the CCTV system. The contractor is responsible to ensure

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

that what CBP requires be monitored by a camera or group of cameras is what results from the installation. Therefore, it is up to the contractor to choose the appropriate camera/lens combinations and to mount the cameras so that the required coverage is provided. If the placement of multiple cameras can provide coverage of more than one for the requirements listed below and the image captured is sufficient to identify any person(s) in the frame, multiple cameras will suffice for both requirements, Cameras must be capable of recording identifiable images of people in darkness.

12. Camera Coverage Requirements:

(a) Vault

- All cameras must provide usable images of the exterior of the entire vault door and its frame. The image captured must be sufficient to identify anyone tampering with or opening the vault door;
- Cameras must provide usable images of the interior of the entire vault door and its frame so that identifiable images of persons entering the vault are captured; and
- Cameras must provide images of the entire interior area of the vault. The images must be of sufficient quality so that person(s) in the area are identifiable and any activity in the area is captured.

(b) Processing Area

- Cameras must provide images of the entire interior of the processing area including the interior of the door. The images must be of sufficient quality so that person(s) in the area are identifiable and any activity in the area is captured. One camera must be positioned to observe someone working at the narcotics scale.

(c) Exterior

- Sufficient cameras are to be placed to provide usable images of the exterior walls, exterior entrance and exterior roof of the vault. Camera placement needs to be coordinated with exterior lighting to maximize quality of images captured during darkness.

13. Ancillary Equipment:

(a) DVR, Multiplexer, Monitor, etc.

- The Digital Video Recorder (DVR), multiplexer and other related equipment are not to be located in the Vault or the processing area. This equipment is to be located in a secure room away from the

[RETURN TO TOP](#)

vault. The equipment is to be housed in a lockable rack type cabinet designed for housing such equipment. The cabinet must also house the Uninterruptible power supply (UPS). A CCTV color monitor with a minimum 21" screen is to be placed in close proximity to this cabinet.

(b) Wiring

- Fiber Optic video transmission cable is preferred if it is compatible with the system components. Copper coaxial cable may be used, however, copper clad aluminum, aluminum, or foil based coaxial cable is not acceptable. All wiring is to be run through metal conduit.

(c) Uninterruptible Power Supply (UPS)

- An Uninterruptible power supply must be a component of the system. Having the CCTV system connected to the generator distribution panel is the ideal.

14. Additional CCTV Camera System Requirements:

(a) Closed Circuit Television System (CCTV) – Performance Requirements (this is an example of performance requirements – you will need to modify to meet the specific needs of the facility you are working on):

- The vault is a six-sided structure (floor walls, roof & floor) that requires full camera coverage. Cameras are to be placed and lenses set so that each camera will produce a usable image of any person inside or in the immediate vicinity of the outside walls or on the roof. The cameras must also provide clear images of operations inside the vault areas and at the overhead and pedestrian entry doors;
- The entire roof area must be covered. Usually this is accomplished using two mast-mounted cameras on opposite corners of the roof using wide-angle lenses. The camera/lens combination is such so that there is an overlap in the coverage;
- All four exterior walls must be covered;
- The exterior of the pedestrian entry door and the overhead door must be covered and the camera must produce clear images of all persons and operations in that area (loading, unloading, etc.) The camera(s) must also provide a clear image of anyone at the pedestrian door so that CBP personnel can identify them before opening the pedestrian door to admit any person who does not have access;
- The entire administration area must be covered and the cameras placed and the lenses adjusted so that clear images of all operations,

[RETURN TO TOP](#)

including weighing and packaging, etc. are produced. The entire vault door and doorjamb must be monitored so that anyone tampering with the door can be identified;

- The entire interior of the vault must be covered. One camera is to be so positioned that it provides a clear picture of the interior of the vault door and doorjamb. The camera shall be positioned so that no one can enter through the vault door that cannot be identified from the image provided by this camera. One camera must also provide the same level of coverage at the entry door to the caged area. Anyone entering the cage should be easily identifiable from the image produced by the camera. One camera must provide usable images system located inside the vault;

NOTE: If a camera can be placed so that it provides coverage for two of the performance requirements noted above, one camera would suffice. For instance if a camera can be placed so that it meets the requirement for capturing the image of a person entering the vault and the same camera provides a usable image of some amount of the storage space, it is not necessary to use another camera to just look at the vault door and jamb.

- All camera wiring is to be run through EMT metal conduit. The size of the conduit is to be determined by the vendor, but is to be of sufficient size so that the wiring will not be chafed or otherwise damaged as it is drawn through the conduit;
- The cameras (shall be whatever model works for space, variable lens) are to be event activated;
- The system shall be placed inside a lockable rack designed for the purpose of securing such equipment. The keys to the rack shall be given to the responsible Officer;
- One color monitor is to be placed with the system equipment to allow authorized personnel the ability to review the images from all the cameras that are stored on the DVR or being played back from the download library; and
- The affected CBP employees should determine how often the DVR is downloaded. The DVR will probably have the capacity to hold up to 30 days in memory. Employees should be cautious in determining the time span because looking for a certain time frame inside a thirty-day period can be time consuming.

- (b) Please note that Seized Property personnel are not to download or administer the CCTV system. The separation of duties must be provided for, generally this is accomplished by having an employee or the CBP Officer manage the system.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

15. Intrusion Detection System (IDS). The purpose of an alarm system is to detect an intrusion or attempted intrusion and to notify appropriate personnel.

(a) General Requirements:

- Equipment shall be UL-2050 approved (certified);
- Balanced Magnetic Switches (BMSs) on all perimeter doors;
- All control units will be located within the area protected by the alarm system;
- All components shall be installed in a manner to prevent access or removal from a location external to the protected zone; and
- All alarm systems shall be capable of operating from commercial AC power. In the event of commercial power failure, provisions will be made for automatic switchover to emergency power, and back to commercial power without causing an alarm. A signal will be presented to the monitoring location indicating when the system has lost power. When batteries are used for emergency power, they will be maintained at full charge by automatic circuits. Emergency power must be capable of operating the system for a minimum of twenty-four hours. For more information on emergency power, see [Appendix 7.15, Loading Docks and Service Access](#).

(b) Volumetric sensors employed in the alarm system must be placed so that the most likely intruder motions are detected.

(c) All perimeter sensors and control units will be equipped with tamper detection.

(d) Depending on facility operations, a duress/panic alarm may be installed. If a duress/panic alarm is used it must be connected to a Class A Central Monitoring Station.

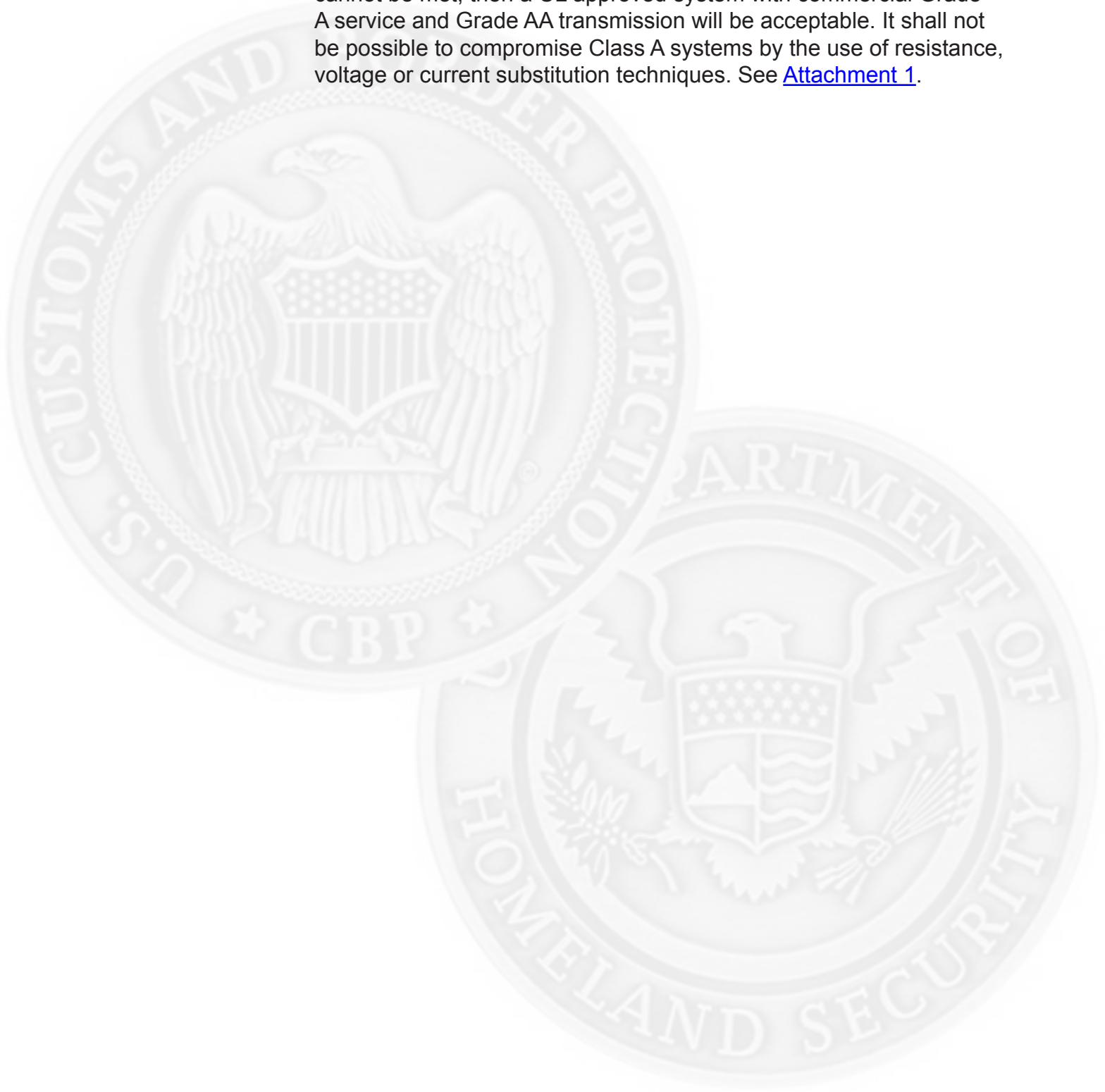
(e) All alarm wiring leaving the controlled area shall be equipped with electronic line supervision.

(f) Class A - Pseudo-Random digital and tone-wire transmitted preferred. Exceeds previous "High Line Security" Requirement.

- These systems will transmit over wire a pseudo-random generated tone or tones or digital type modulation. These systems will use either an interrogation and reply scheme or a synchronization scheme. The signal between the protected premises and the monitor location shall not repeat itself within a six-month period. A line supervision alarm

[RETURN TO TOP](#)

signal shall cause a lock-in condition, which shall be transmitted to the monitor location in not more than 30 seconds. If the above conditions cannot be met, then a UL approved system with commercial Grade A service and Grade AA transmission will be acceptable. It shall not be possible to compromise Class A systems by the use of resistance, voltage or current substitution techniques. See [Attachment 1](#).



II. ATTACHMENT 1

- A. Intrusion detection monitoring requirements and services provided by the Federal Protective Service (FPS) through GSA leases. FPS has designed and built four Mega-Centers located in Suitland, Maryland, Philadelphia, Pennsylvania, Battle Creek, Michigan and Denver, Colorado.
1. Among other tasks, these centers monitor intrusion/duress alarm systems, fire detection systems, environmental systems and elevator emergency telephones for multi-regional areas. In order to take full advantage of the Mega-Centers' Intrusion Detection System (IDS) monitoring capabilities; FPS mandates that all installations and upgrades of the above referenced systems in both leased and government facilities are standardized on a national basis, are fully compatible with the standardized alarm receiving equipment existing in the Mega-Centers, and are capable of being remotely programmed with software from the approved panel manufacturers. A national decision was made that FPS would only recommend and support alarm systems that fully interfaced with the control center's equipment and software. Therefore, FPS requires that only remote-programmable alarm systems are specified when designing or upgrading alarm systems that are monitored at the Mega-Center. Additionally all remote-programmable alarm systems must be able to easily communicate with the Mega-Centers' monitoring equipment.
 2. Currently, the FPS list of approved alarm control panels include those manufactured by ADEMCO, CADDX, DMP, ITI, & Radionics/Bosch. Additionally, approved alarm panels must communicate via the Mega-Centers' alarm receivers using one of the following panel signaling protocols: ADEMCO Contact ID, Radionics/Bosch Modem II, Modem IIE and Modem IIIA; and Security Industry Association (SIA). The Mega-Centers can also accept most digital communicators for Fire Detection Systems that transmit one of the following industry standard formats (communications protocol): ADEMCO Contact ID, Radionics / Bosch Modem II, Modem IIE and Modem IIIA or SIA.
 3. The current standard alarm control panels for Federal buildings and larger leased sites are the ADEMCO model numbers Vista 50PUL, Vista 128FB or FBP & 250 FB or FBP; the CADDX model number NX8E; the DMP model number XR200; and the Radionics/Bosch model number 9412G. These alarm control panels are commercial UL, compatible with Fire Detection and most Access Control Systems. For smaller leased space and office applications contact your local Mega-Center for acceptable alternatives supplied by approved manufacturers. All alarm systems must have tampered devices, cabinets and junction boxes. All devices will report as one point as a zone description that can be used when reporting an alarm condition to the responding authority. FPS cannot monitor any alarm system that does not fully comply with the above referenced criteria. If a system does not meet these criteria, either the customer or GSA will have to

[RETURN TO TOP](#)

assume the cost of commercial monitoring.

III. ADDITIONAL GUIDANCE

- A. Concrete compressive strength. Concrete shall have a minimum 28 day compressive strength of 3000 psi. when tested in accordance with the applicable sections of the American Concrete Institute Standard ACI318 – (Building Code Requirement for Reinforced Concrete).
- B. Additional Specifications - Vault area will be equipped with one of the following:
 - 1. An emergency escape which meets applicable building and safety codes. The escape device will be designed and installed so that it will not be activated by the exterior locking device nor actuated by drilling or rapping on the door from the outside.
 - 2. A decal containing procedures to be followed in an emergency and for operating the escape device will be permanently affixed to the inside of the door.
 - 3. Communications facilities and an alarm system or other signaling device which will permit a person in the vault area to communicate with someone on the outside to obtain release.
 - 4. An emergency light.
 - 5. At least one approved fire extinguisher installed near the door.
- C. For additional IDS guidance refer to [Appendix 8.9. IDS](#).





APPENDIX 8.8: STRONGROOMS

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

I. GENERAL

- A. A strongroom is an enclosed space constructed of solid building materials. Strongrooms are normally used for the storage of classified or sensitive materials, such as firearms. Protection is supplemented by guards and or Intrusion Detection Systems (IDS). Rooms that have false ceilings and walls constructed of fibrous materials, or other modular or lightweight materials, do not qualify as strongrooms.
- B. Construction of strongrooms may be necessary for bulk storage or where use of GSA-approved security containers are not adequate or not practical. Possible applications for strongrooms are:
1. Open storage of classified National Security Information (NSI);
 2. Closed storage of NSI in a non-controlled facility;
 3. Weapons and ammunition rooms;
 4. Evidence storage rooms/Temporary seized property held less than 72 hours;
 5. Mail rooms;
 6. Rooms used to store high value tools and equipment;
 7. Funds and valuables storage;
 8. LAN/TELCOM; and
 9. Other sensitive assets.

II. CONSTRUCTION STANDARDS

- A. Heavy-duty builder's hardware shall be used in construction. All screws, nuts, bolts, hasps, clamps, bars hinges, and pins should be securely fastened to preclude unwanted entry. Hardware accessible from outside the strongroom must be peened, pinned, or spot-welded to preclude removal.
- B. Walls:
1. The perimeter walls, floors, and ceiling will be permanently constructed using slab to slab construction. Slab to slab construction (true floor to the true ceiling) is defined as walls that extend from the solid concrete floor to the underside of the roof slab above. All construction must be done in a manner as to provide visual evidence of unauthorized penetration.
 2. Walls will be constructed using reinforced Concrete Masonry Units (CMU) not less than 8 inches thick.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- (a) Masonry units will be solid brick or hollow type block and filled with concrete and metal reinforcement bars.
 - When using hollow type blocks, they will be filled with concrete and reinforced with #5 rebar, a minimum of 5/8 inches in diameter. The reinforcing is to be anchored into the ceiling and floor to a minimum depth of one-half the thickness of the adjoining member.

3. Where a CMU wall is not feasible, the following alternate method can be used:

- (a) The inside walls will be constructed of 5/8-inch fire rated gypsum board and the outside walls with standard 5/8-inch gypsum board and a layer of 9-gauge expanded metal on the inside of the area.
- (b) The expanded metal shall be in a 1½-inch x 2-inch diamond pattern, attached to metal studs and spot welded at 6-inch intervals. If wooden studs are used to attach the expanded metal, the studs shall be no less than 2 inches x 4 inches; otherwise it shall securely anchored to the stud with stainless steel screws and washers. The screws shall be no less than 3 inches in length and installed at no more than 6-inch intervals. The expanded metal shall be affixed in a manner to prevent tampering and to show evidence of attempts at removal. Although less expensive to build this is not the preferred method for securing arms and ammunition. See [Figure 1](#).
- (c) To view the specifications for expanded metal mesh, see [Section VII, Construction Standards: Expanded Metal Mesh Specifications](#).

C. Ceilings:

1. When walls are being constructed using the CMU method described above in II.B.2, and they do not extend to the true ceiling and a suspended (false) ceiling is created, the suspended (false) ceiling must be reinforced with a 9-gauge expanded metal to serve as the true ceiling. When expanded metal is used, it must overlap the adjoining walls and be secured in such a manner that removal will show evidence of tampering.
2. When constructing walls using the alternate method described above in paragraph II.B.3 and the walls do not extend from slab to slab and a suspended (false) ceiling is created, the suspended (false) ceiling must be reinforced with a 9-gauge expanded metal to serve as the true ceiling.
 - (a) When metal studs are used to construct the walls, the expanded metal must be spot welded at 6-inch intervals to the framing of the side panels so that any attempted removal will show evidence of tampering.

[RETURN TO TOP](#)

(b) When wooden studs are used to construct the walls, the expanded metal must be securely anchored to the stud with stainless steel screws and washers. The screws shall be no less than 3 inches in length and installed at no more than 6-inch intervals.

3. When the walls of an area do extend from slab to slab and a false ceiling is added it is not necessary to reinforce the false ceiling.

D. Floors:

1. For new construction, floors will consist of reinforced concrete with a minimum thickness of 8 inches. The concrete mixture will have a minimum compressive strength of at least 3,000 psi. Reinforcement will be accomplished with 2 grids of #5 rebar, a minimum of 5/8-inch diameter, positioned centrally and spaced horizontally and vertically 6 inches on center; rods will be tied or welded at intersections.
2. Existing floors will consist of reinforced concrete based on structural/floor loading.

E. Doors/Door Hardware:

1. Doors must be constructed of 12-gauge steel clad hollow core metal or of single solid core wood, 1 ¾ inches thick, and hung in 12-gauge hollow metal frames.
2. All doors to unclassified area(s) will be equipped as a minimum with a card reader/keypad and a Commercial Grade 1 – GSA approved High Security Lockset. Doors to classified areas must be equipped as a minimum with a Kaba Mas CDX-09 High Security Electromechanical Lock and a Commercial Grade 1 – Mortise High Security Lever Lockset. Keys must be off the building master in facilities that are not solely occupied by CBP.
3. Double doors must have one door secured with flush mount bolts at the top and the bottom. Astragals (overlapping molding, preferably metal) must be used to inhibit access to lock bolts.
4. Perimeter door hinge pins that are located outside the office area must be non-removable (peened, pinned, or spot welded). If the door swings outward, hinge side protection in the form of a dowel-pin and socket is required. Refer to [Figure 2 of Appendix 7.6: Doors and Door Hardware](#) for details. All perimeter doors must have a commercial grade pneumatic door closer and an anti-pry strip installed to prevent the door from being pried open.
5. All door hardware (e.g., hinges, lock hardware) must be secured to door frame with stainless steel screws at least 3 inches long.
6. For additional information on Doors and Door Hardware, refer to [Appendix 7.6](#).

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

F. Windows:

1. Strongrooms shall have no exterior windows.
2. Interior vision panels may be approved on a case-by-case basis.

G. Miscellaneous Openings:

1. Where vents, ducts, registers, sewers, tunnels and other miscellaneous openings are of such size and shape (in excess of 96 inches square) and enter or pass through the area as to permit unauthorized entry, they should be protected with either steel bars or wire mesh grills. If bars are used, they should be at least 3/8-inch diameter hardened steel, welded vertically and horizontally, six inches on center. If grilles are used, they must be of 9-gauge woven wire mesh.
2. For additional information on Miscellaneous Openings, refer to [Appendix 7.8, Openings](#).

III. INTRUSION DETECTION SYSTEM (IDS)

- A. All strongrooms shall include an IDS and it shall be connected to a Class A Central Monitoring Station. At a minimum the IDS should include a balanced magnetic switch (BMS) on the door, motion detection sensors inside the room and a card reader/keypad to track users. There should be a backup method of communication set up with the Central Monitoring Station (e.g. a wireless phone link, such as cellular or an extra analog/digital telephone line), so that if a telephone line is cut or otherwise interrupted, an alarm is activated at the Central Monitoring Station. Acknowledgement of an alarm condition by the Central Monitoring Station must take place within 30 seconds of the alarm. The Central Monitoring Station must dispatch the correct response (law enforcement, duty agent, etc.).
- B. For additional information on IDS, refer to [Appendix 8.9, Intrusion Detection Systems](#).

IV. CLOSED-CIRCUIT TELEVISION (CCTV)

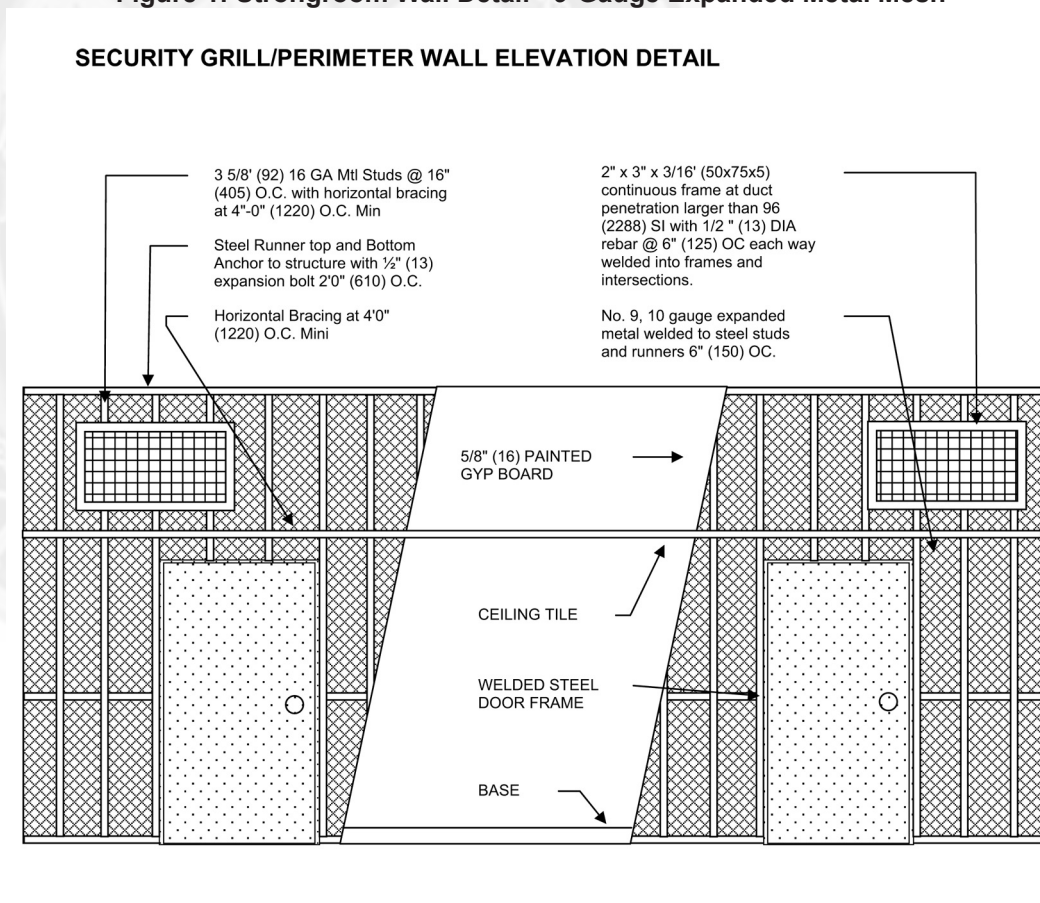
- A. All strongrooms will use CCTV. At a minimum, CCTV will monitor the entrance and perimeter areas. The minimum components that the system must have is one color monitor and one high resolution digital video recorder (DVR), capable of recording a minimum of 30 days and playing back any camera view. All camera views associated with an alarm must be automatically recorded. CCTV images must be retrievable and operable over weekends and holidays.
- B. For additional information on CCTV, refer to [Appendix 8.12, CCTV](#).

V. REFERENCES

- Expanded Metal Manufacturers Association, [EMMA 557-99](#), Standards for Expanded Metals
- [National Concrete Masonry Association](#)
- Customs and Border Protection Lock Hardware Requirements
- [GSA Advantage \(Manufacturers\)](#)
- [GSA Schedule](#)

VI. GRAPHICS

Figure 1: Strongroom Wall Detail - 9-Gauge Expanded Metal Mesh



VII. CONSTRUCTION STANDARDS

A. Expanded Metal Mesh Specifications

1. Expanded metal mesh shall meet ASTM F1267-89 type, Class 1 standard and shall have the following characteristics:
 - (a) Strand thickness: No. 9 - 10-gauge minimum (flattened);
 - (b) Weight: 195 lbs/csf minimum;

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- (c) Material: Carbon Steel;
 - (d) Shape: Flattened;
 - (e) Pattern: Diamond;
 - (f) Dimensions: 3.20 inch maximum (long opening) (LWD) and 1.33 inch maximum (short opening) (SWD); and
 - (g) Recommended mesh: 3/4" #9 (10 ga).
- B. Mesh shall be fastened to steel stud and top and bottom runners using either screw or weld attachment. Screws or weld shall be spaced at 6" on center maximum, with all corners fastened to the framing. Mesh splice shall occur at studs only. Splice between supports is not permitted unless: a) such splice is welded continuously top to bottom; b) mesh is overlapped three inches, and fastened or welded every six inches.
- C. Steel framing receiving metal mesh shall be 16 gauge minimum.
- D. Screws shall be self-drilling #8 shank minimum (1/4" minimum penetration into steel framing.) Fasteners must be used from the secure side of the mesh. 1/2-inch washers must be installed when using screws to deter ability to pull mesh over tops of screw heads.
- E. Welds shall be 1/8" x 1/2" long fillet type excepting at unsupported splices where the weld must be continuous.
- F. There can be no gap in coverage. Gaps may be closed with steel studding or flat metal welded (or fasted where welding is not permitted) to the secure side of the expanded metal.







APPENDIX 8.9: INTRUSION DETECTION SYSTEMS

I. INTRUSION DETECTION SYSTEMS

A. General

1. The Intrusion Detection System (IDS) is an essential part of the physical security system. As defined in the United Facilities Criteria (UFC) [UFC 4-021-02NE](#), an IDS consists of the combination of electronic components, including sensors, control units, transmission lines, and monitoring units integrated to be capable of detecting one or more types of intrusion into a protected area.

B. Uses of IDS

1. IDS can include both interior and exterior systems. These are utilized to provide:
 - (a) The earliest practical warning of any attempted penetration into protected areas;
 - (b) A greater defense capability to detect and defeat intruder attacks;
 - (c) Additional controls at critical areas or points;
 - (d) Insurance against human error;
 - (e) A substitute for other physical security measures that cannot be used because of safety issues, operational requirements, building layout, cost or similar issues.

- C. The primary function of an IDS is to detect intruders. The detection of an intruder is the first of a four-phase process. This detection phase starts the clock on the “Detect, Assess, Delay and Respond” timeline. To be effective these actions must be less than the time it would take an aggressor to cause damage or to complete his mission.

- D. To maximize the effectiveness of an IDS, the design should utilize both the “Protection In-Depth” (tiered defensive system) principle and the concept of complementary devices. Protection In-Depth first identifies an asset requiring protection and then configures layers of unbroken defensive rings protecting that item. The first detection layer is located at the outermost defensive rings necessary to provide the required delay needed to timely stop the aggressor.

II. ALARM COMPONENTS

A. Components of an alarm system

1. An alarm system is composed of four main parts:
 - (a) A control unit used to arm/disarm the system as well as edit system

[RETURN TO TOP](#)

capabilities and responses;

- (b) One or more sensors to detect the presence or actions of an intruder;
- (c) A central processing unit (CPU), or remote monitoring station dedicated to constantly monitoring the sensors and transmits an alarm signal when a sensor detects an intruder; and
- (d) The alarm annunciator, which signals an activation of the system.

III. ALARM INSTALLATION

A. Planning Alarm Installations

1. Alarms are used to detect approach or intrusion. Some are intended for exterior protection, and some are suitable only for indoor installations. The following should be addressed in determining the need for an alarm system:
 - (a) Sensitivity or criticality of the operation;
 - (b) Facility vulnerability to damage, interruption, alteration or other harm;
 - (c) Sensitivity or value of the information or property stored at the facility;
 - (d) Location of facility and accessibility to intruders;
 - (e) Other forms of protection in place or available;
 - (f) Guard or law enforcement response capability.

B. Tiered Defensive System Concept

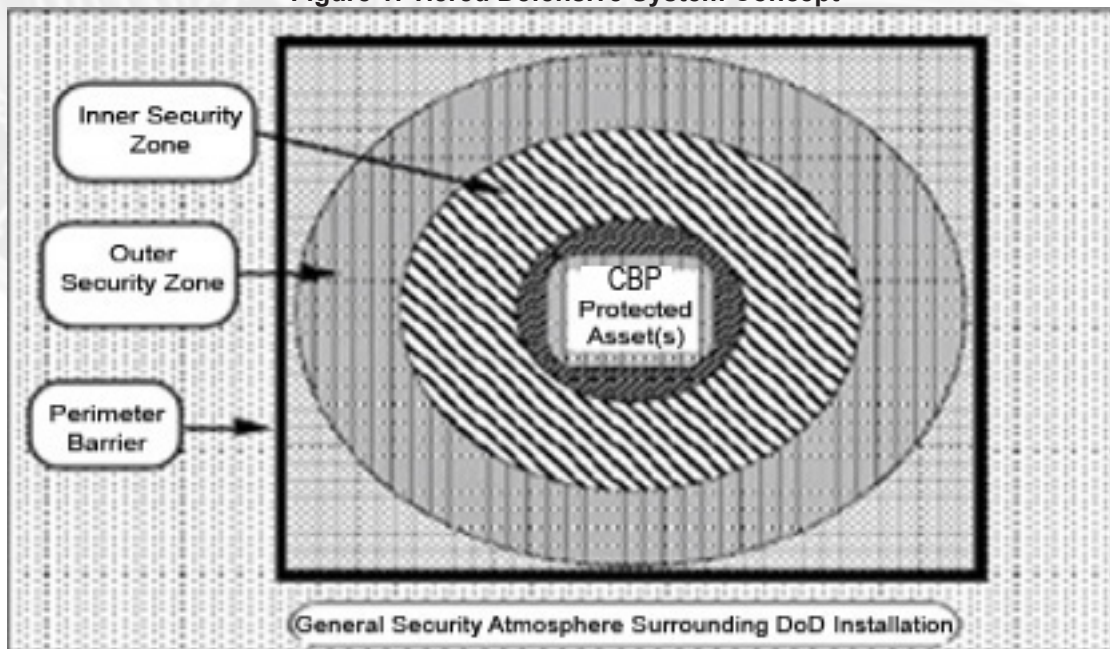
1. As shown in [Figure 1](#) the Protection in-Depth principle has one potential weakness. Once an asset has been identified for protection, the methods selected to protect that asset have to be similar or identical to an aggressor's method of attack. This requires that every possible method of attack be taken into consideration.
2. Combining a "Line" device such as a vibration activated fence, with a volumetric device such as an exterior bistatic microwave detector is a good example of complementary protection. Each device provides protection assistance to the other type of device in the overall coverage of that area. Bridging over a fence still subjects the aggressor to the capabilities of the microwave system.
 - (a) It is important to remember that this technique is not infallible. Each type of device still retains its inherent weakness. A determined intruder with the proper intelligence, resources and capabilities can still bypass/defeat

[RETURN TO TOP](#)

this type of setup by analyzing the composition of the total system and then developing a response to each individual device. In this example the intruder bridges the fence without touching it, landing as closely as possible to the microwave transmitter where the cone of protection is the smallest. Then, depending upon the construction of the microwave, the intruder can either climb onto and over the transmitter or crawl underneath its cone of protection.

3. Choosing the proper system, installing it correctly, and routine maintenance are also very important issues concerning the effectiveness of the IDS.
4. Laziness, lack of knowledge, programming weaknesses, confusion, and improper placement of sensors system can be exploited by the knowledgeable intruder. Improper maintenance procedures resulting in multiple false alarms and causing a lack of confidence in the system are also pathways for bypassing the system. This is especially true of exterior sensors where environmental conditions mandate that devices be maintained regularly for their proper function.

Figure 1: Tiered Defensive System Concept



C. Sensors

1. The three basic types of sensors are perimeter, volumetric, and proximity. The following are general definitions and each will be covered more in depth in attached interior and exterior use sections.
 - (a) Perimeter. Perimeter protection is the first line of defense. The most common points for sensors are doors, windows, vents and skylights. These may be protected, with detectors sensing their opening or breaking.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

The major advantages of perimeter-protection sensors are their simple design and reliability. The major disadvantage is that they protect only openings such as doors or windows. If intrusion occurs through a wall or ceiling, these devices are bypassed and the intrusion goes undetected.

- Switches. These devices are usually magnetic operated switches affixed to a door or window in such a way that opening the door or window removes the magnetic field causing an alarm. High security switches are normally balanced or biased magnetic switches. Another type of switch is the plunger or roller switch which is compressed when the door or window is closed. Once the door or window is opened pressure on the device is released, the alarm circuit is broken and an alarm results;
- Screens. Openings such as vents, ducts, skylights, and similar openings can be alarmed by thin wire filaments that signal an alarm if the screen is cut or broken. Often the wire filaments are placed in a frame of wooden rods and require little maintenance; and
- Glass Breakage. Electronic sensing devices used to detect high-frequency sound patterns within the glass when it is broken, or the shock wave a substantial impact makes against the surface.

(b) Volumetric. Volume protection sensors are designed to detect the presence or actions of an intruder almost anywhere within an entire room from floor to ceiling. A variety of volumetric devices are available. Each kind of detector has some advantages and limitations. Therefore, a device must be selected for a specific environment. A major advantage of volumetric devices is that they provide a highly sensitive and invisible means of detection in high-risk areas. The major disadvantage is that an improper application can result in frequent false alarms.

- Infrared. Passive infrared sensors are part of the motion-detection group. They sense the rapid change in temperature caused by body heat of an intruder compared to the room's normally stable environment as the intruder passes through the protected area. Infrared detectors are relatively free of false alarms; however, items moved by air currents within the protected area can activate the alarm. Passive Infrared Detectors are most effective when deployed in a manner where the intruder's movement crosses in front of the device;
- Ultrasonic. Ultrasonic motion detectors generate a high frequency of sound that is out of the normal range of human hearing. An intruder disrupting the ultrasonic wave pattern initiates the alarm. Ultrasonic devices are prone to false alarms, due to excessive air currents or ultrasonic noise from mechanical equipment. Ultrasonic devices

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

are most effective in detecting movements towards or away from the device;

- Microwave. This kind of motion detector uses high-frequency radio waves, or microwaves, to detect movement. Because microwaves penetrate materials such as glass, and metal objects reflect them, they can detect motion outside the protection area causing false alarm problems if not properly installed; and
- Photoelectric. Photoelectric devices transmit a beam across a protected area. When an intruder interrupts this beam, the circuit is disrupted causing an alarm. Today's photoelectric devices use diodes that emit an invisible infrared light and usually pulses rapidly to prevent compromise by substitution. A disadvantage is that they can be defeated relatively easily; the beams are narrow and may be discovered or avoided. They can be utilized effectively at "choke points" where the intruder is forced to pass.

(c) Proximity. Object protection provides direct security for individual items.

- Capacitance. A capacitance device is used to protect specific objects such as security containers and safes. The capacitance alarm uses the metal construction of the container and causes it to act as a capacitor or condenser. When a change occurs in the electromagnetic field surrounding the metal object the balance is disturbed and the alarm is activated. The system can only be applied to ungrounded equipment and accidental alarms can occur if the container is carelessly touched when the alarm is activated;
- These seismic sensing devices use a piezoelectric crystal or microphone to detect the sound pattern that a hammer-like impact on a rigid surface would generate. These devices are attached directly to safes and filing cabinets, or to the walls, ceiling, and floor of vaults. False alarms may occur with these devices by passing vehicles or falling objects.

IV. EXTERIOR SENSORS

A. Planning

1. Exterior sensors without frequent and proper maintenance are prone to false/ nuisance alarms which can result in a lack of confidence in these devices. In addition, because of the harsh environmental conditions in which they function, they generally are more expensive than comparable interior sensors. These same environmental conditions can influence the detection capabilities of these

[RETURN TO TOP](#)

devices in two different manners:

- (a) Rain and snow can reduce the viewing distances of CCTV cameras and can potentially create a gap in coverage. Conversely, these same environmental conditions can increase the likelihood of intruder detection by having the rain or snow impact raise the “irritation” factor of the device close to the threshold alarm level. The result is a reduced window of opportunity for the intruder to exploit.
2. One advantage exterior sensors have over interior sensors is that the exterior devices are left in the secure mode at all times offering no opportunity for the intruder to disable the device when the system is disarmed.

V. EXTERIOR FENCES

A. Planning

1. Studies have shown that fences and walls provide less than 15 seconds of penetration resistance. They do serve to accomplish one or more of the following functions. They serve the purpose of being a demarcation line indicating the perimeter dimensions of the protected area. They also serve as a debris catcher, especially in a two-fence system, minimizing the potential of false alarms caused by stray animals, blowing branches, papers, etc. (In a two fence system, the interior fence is used for detection purposes and to provide some delay.) This barrier also causes an intruder to overtly declare his intentions to violate the protected area. The exterior fence line can also serve as a platform for CCTV cameras and can with the proper adjustments have IDS devices attached.

B. Installation

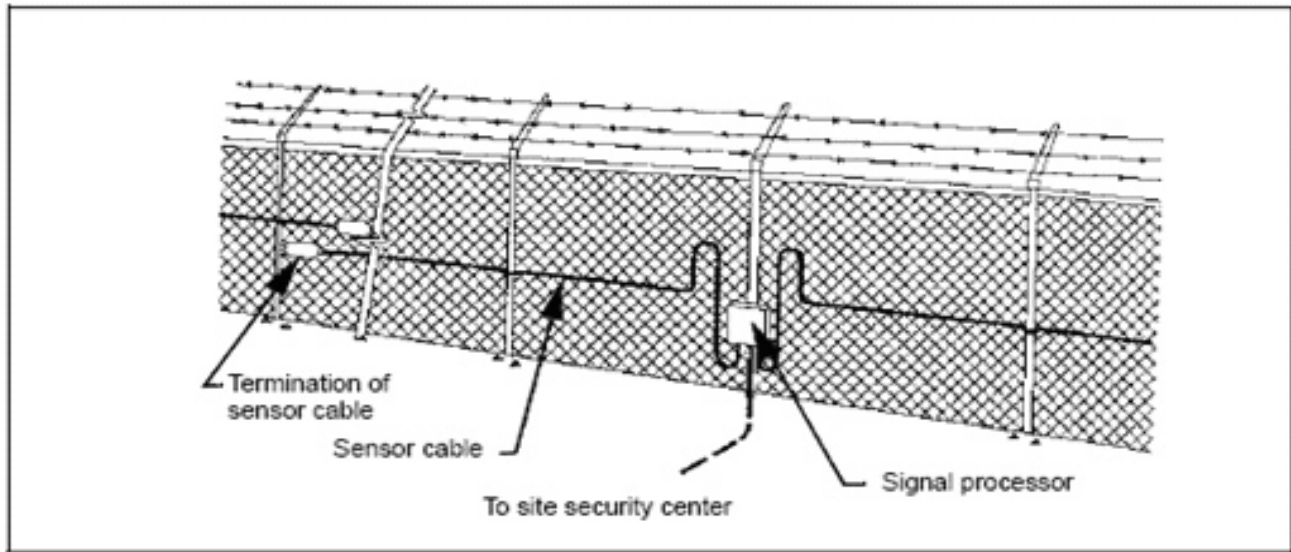
1. Perimeter sensors are normally installed directly on the fences, walls, or gates. Penetration attempts (such as climbing, cutting, or lifting) generate mechanical vibrations and stresses in fence fabric and posts that are usually different than those caused by natural phenomena like wind and rain. In general, if the fence is part of the IDS system it is activated in one of two ways -by touch, or a threshold change in the fence’s electric field or capacitance. The emanation field projects approximately 6 feet (3 feet on each side of the fence) from the fence.
2. For further information, see:
 - (a) The U.S. Navy’s [Interim Technical Guidance \(ITG\) 03-3, Entry Control Facilities](#).
 - (b) [Chapter 7.3, Fencing](#).

C. Types of Fence Sensors

1. Strain-Sensitive Cable

- (a) Strain-sensitive cables are transducers that are uniformly sensitive along their entire length. They generate an analog voltage when subject to mechanical distortions or stress resulting from fence motion. Strain-sensitive cables are sensitive to both low and high frequencies. The signal processor usually has a band-pass filter that passes only those signals characteristic of fence-penetration actions. An alarm is initiated when the signal's frequency, amplitude, and duration characteristics satisfy the processor's criteria.
- (b) Strain-sensitive cable acts like a microphone; some manufacturers offer an option that allows the operator to listen to fence noises causing the alarm. Operators can then determine whether the noises are naturally occurring sounds from wind or rain or are from an actual intrusion attempt. This feature is relatively costly to implement because it requires additional cable from each signal processor to the security center and, if CCTV is being used, it may be of limited benefit. Strain-sensitive cable is attached to a chain-link fence about halfway between the bottom and top of the fence fabric with plastic ties. One end of the cable is terminated at the signal processor and the other end with a resistive load. The DC through the cable provides line supervision against cutting or electrically shorting the cable or disconnecting it from the processor.
- (c) A typical installation is shown in [Figure 2](#).

Figure 2: Typical Strain-Sensor Cable



2. Taut-Wire Sensor

(a) A taut-wire sensor combines a physically taut-wire barrier with an intrusion-detection sensor network. The taut-wire sensor consists of a column of uniformly spaced horizontal wires up to several hundred feet in length and securely anchored at each end. Typically, the wires are spaced 4-8 inches apart. Each is individually tensioned and attached to a detector located in a sensor post. Two types of detectors are commonly used: mechanical switches and strain gauges:

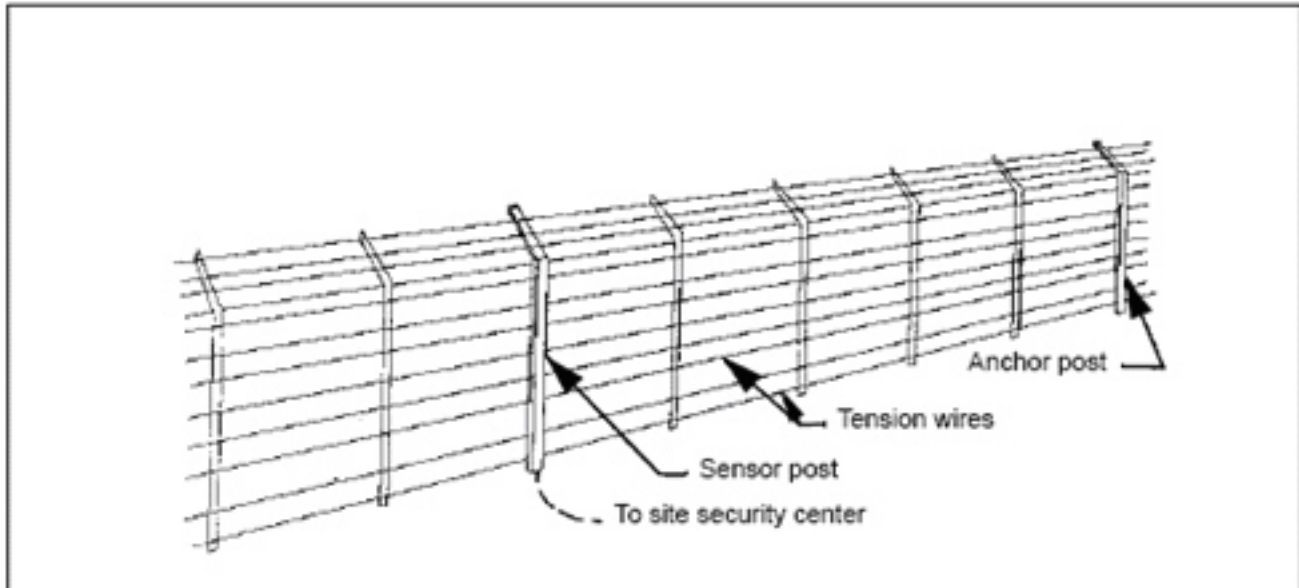
- The mechanical switch consists of a specially designed switch mechanism that is normally open. The tensioned wires are mechanically attached to the switch and movement of the wire beyond a preset limit causes the switch to close. To counteract small gradual movements of a wire (such as that caused by settling of the fence or by freezing or thawing of soil) switches are usually supported in their housing by a soft plastic material. This material allows the switch to self-adjust when acted upon by gradual external forces and wire effects or contraction.
- Strain-gauge detectors are attached to the taut wire with a nut on a threaded stud. When a force is applied to the taut wire, the resulting deflection is converted by the strain gauge into a change in electrical output that is monitored by a signal processor.

3. With sensors that use mechanical switches as detectors, the switches in a single sensor-post assembly are wired in parallel and are connected directly to the alarm-annunciation system. Pulse-count circuitry is not used because a single

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- switch closure, such as that caused by an intruder moving or cutting one wire, is indicative of an intrusion attempt. Strain-gauge detectors in a sensor post are monitored by a signal processor. When the signal from one or more strain gauges satisfies the processor's criteria, an alarm is triggered.
- The taut-wire sensor can be installed as a freestanding fence or can be mounted on an existing fence or wall. [Figure 3](#) shows a freestanding configuration.

Figure 3: Typical Taut-Wire Installation

5. Fiber-Optic Cable Sensors

- Fiber-optic cable sensors are functionally equivalent to the strain sensitive cable sensors previously discussed. However, rather than electrical signals, modulated light is transmitted down the cable and the resulting received signals are processed to determine whether an alarm should be initiated. Since the cable contains no metal and no electrical signal is present, fiber-optic sensors are generally less susceptible to electrical interference from lightning or other sources.

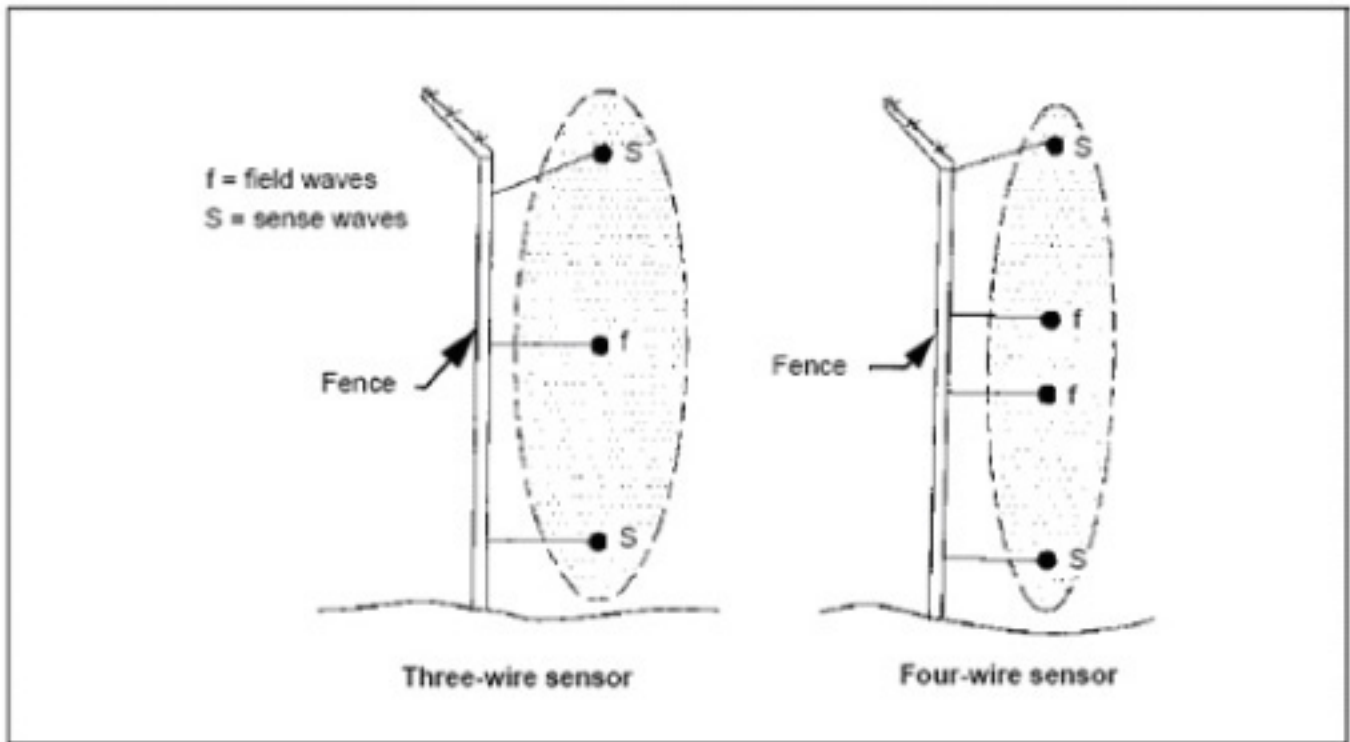
6. Electric-Field Sensors

- Electric-field sensors consist of an alternating-current (AC) field generator, one or more field wires, one or more sense wires, and a signal processor. The generator excites the field wires around which an electrostatic field pattern is created. The electrostatic field induces electrical signals in the sensor cable sense wires, which are monitored by the signal processor. Under normal operating conditions, the induced signals are constant. However, when an intruder approaches the sensor, the induced electrical signals are altered, causing the signal processor to generate an alarm.

[RETURN TO TOP](#)

- (b) Several different field- and sense-wire configurations are available. They range from one field wire and one sense wire to as many as four field wires and one sense wire or four field wires and four sense wires. [Figure 4](#) shows the detection pattern produced by vertical three-wire (one field and two sense wires) configurations. The three-wire system has a wider detection envelope and is less costly (one less field wire and associated hardware). However, because of the tighter coupling between wires, the four-wire system is less susceptible to nuisance alarms caused by extraneous noise along the length of the zone.
- (c) A signal processor monitors the signals produced by the sense wires. The processor usually contains a band-pass filter that rejects high-frequency signals such as those caused by objects striking the wires. Additional criteria that must be satisfied before the processor initiates an alarm include signal amplitude and signal duration. By requiring the signal to be present for a preset amount of time, false alarms (such as those caused by birds flying through the detection pattern) can be minimized.
- (d) As with taut-wire sensors, electric-field sensors can be freestanding (mounted on their own posts) or attached by standoffs to an existing fence. They can also be configured to follow contours of the ground. The area under the sensor must be clear of vegetation, since vegetation near or touching sense wires can cause false alarms. These sensors can also be installed on the walls and roof of a building.

Figure 4: Typical Electric-Field-Sensor Detection Patterns



7. Capacitance Proximity Sensors

- (a) Capacitance proximity sensors measure the electrical capacitance between the ground and an array of sense wires. Any variations in capacitance, such as that caused by an intruder approaching or touching one of the sense wires, initiates an alarm. These sensors usually consist of two or three wires attached to outriggers along the top of an existing fence, wall, or roof edge. To minimize environmental alarms, the capacitance sensor is divided into two arrays of equal length. The signal processor monitors the capacitance of each array. Changes in capacitance common to both arrays (such as produced by wind, rain, ice, fog, and lightning) are canceled within the processor. However, when changes occur in one array and not the other because of an intruder, the processor initiates an alarm.

8. Buried-Line Sensors

- (a) A buried-line sensor system consists of detection probes or cable buried in the ground, typically between two fences that form an isolation zone. These devices are wired to an electronic processing unit. The processing unit generates an alarm if an intruder passes through the detection field. Buried line sensors have several significant features:

- They are hidden, making them difficult to detect and circumvent.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

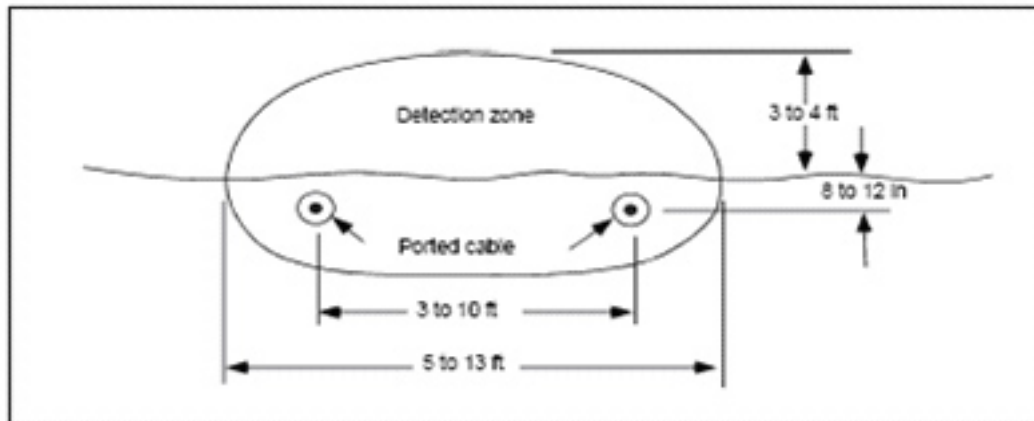
- They follow the terrain's natural contour.
- They do not physically interfere with human activity, such as grass mowing or snow removal.
- They are affected by certain environmental conditions, such as running water and ground freeze/thaw cycles. (Seismic, seismic/magnetic, magnetic, and balanced pressure sensors are seldom used and will not be discussed here.)

(b) The ported-coax cable sensor consists of two coax cables buried in the ground parallel to each other. A radio frequency (RF) transmitter is connected to one cable and a receiver to the other. The outer conductor of each cable is ported (fabricated with small holes or gaps in the shield). The transmitter cable radiates RF energy into the medium surrounding the cables. A portion of this energy is coupled into the receiver cable through its ported shield. (Because of the ported shields, these cables are frequently referred to as leaky cables.) When an intruder enters the RF field, the coupling is disturbed, resulting in a change of signal monitored by the receiver, which then generates an alarm.

(c) Two basic types of ported-coax sensors are available: pulse and continuous wave.

- Pulse-type sensors transmit a pulse of RF energy down one cable and monitor the received signal on the other. The cables can be up to 10,000 feet long. The signal processor initiates an alarm when the electromagnetic field created by the pulse is disturbed and identifies the disturbance's approximate location.
- Continuous-wave sensors apply continuous RF energy to one cable. The signal received on the other cable is monitored for electromagnetic-field disturbances that indicate an intruder's presence. Cable lengths are limited to 300 to 500 feet. Additionally, the sensor is available in a single-cable configuration as well as two separate cables. The pattern typically extends 2-4 feet above the ground and can be 5-13 feet wide, depending on cable spacing and soil composition. [Figure 5](#) represents a typical cross-section of a detection pattern created by a ported-cable sensor.

Figure 5: Typical Ported-Cable Detection Pattern



- (d) Sensor performance depends on properties of the medium surrounding the cables. Velocity and attenuation of the RF wave that propagates along the cables and the coupling between the cables are functions of the dielectric constant of the soil and its conductivity which, in turn, depends on its moisture content. For example, the velocity is greater and the attenuation is less for cables buried in dry, low-loss soil than in wet, conductive soil. Freeze/ thaw cycles in the soil also affect the sensor's performance. When wet soil freezes, the wave velocity and the cable coupling increase and the attenuation decreases, resulting in greater detection sensitivity. Seasonal sensitivity adjustments may be necessary to compensate for changing ground conditions.
- (e) Although usually buried in soil, ported cables can also be used with asphalt and concrete. If the asphalt or concrete pavement area is relatively small and only a few inches thick (such as a pedestrian pavement crossing the perimeter), the ported cables can be routed under the pavement. However, for the large and deep pavements, slots must be cut into the asphalt or concrete to accept the cable.
- (f) A portable ported-coax sensor can be rapidly deployed and removed. The cables are placed on the surface of the ground rather than buried. This sensor is useful for temporary perimeter detection coverage for small areas or objects (such as vehicles or aircraft). They are affected by certain environmental conditions, such as running water and ground freeze/thaw cycles (seismic, seismic/magnetic, magnetic, and balanced pressure sensors are seldom used and will not be discussed here).

9. Line Of Sight (LOS) Sensors

- (a) The LOS sensors, which are mounted above ground, can be either active or passive. Active sensors generate a beam of energy and detect changes

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

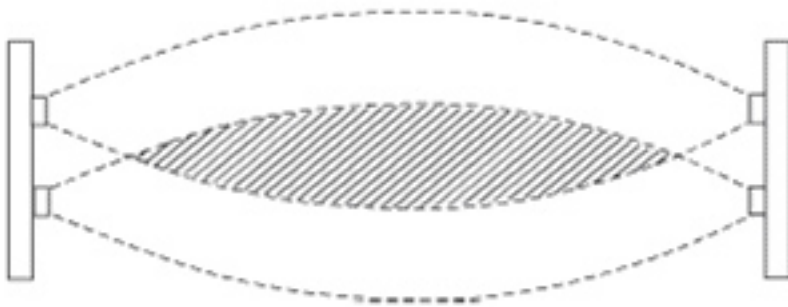
in the received energy that an intruder causes by penetrating the beam. Each sensor consists of a transmitter and a receiver and can be in a monostatic or bistatic configuration. Passive sensors generate no beam of energy; they simply look for changes in the thermal characteristics of their field of view. For effective detection, the terrain within the detection zone must be flat and free of obstacles and vegetation.

10. Microwave Sensors

- (a) Microwave intrusion-detection sensors are categorized as bistatic or monostatic. Bistatic sensors use transmitting and receiving antennas located at opposite ends of the microwave link, whereas monostatic sensors use the same antenna.
- (b) A bistatic system uses a transmitter and a receiver that are typically separated by 100 to 1,200 feet and that are within direct LOS with each other. The signal picked up by the receiver is the vector sum of the directly transmitted signal and signals that are reflected from the ground and nearby structures. Detection occurs when an object (intruder) moving within the beam pattern causes a change in net vector summation of the received signals, resulting in variations of signal strength. The same frequency bands allocated by the Federal Communications Commission (FCC) for interior microwave sensors are also used for exterior sensors. Because high-frequency microwave beams are more directive than low-frequency beams and the beam pattern is less affected by blowing grass in the area between the transmitter and the receiver, most exterior sensors operate at the next to highest allowable frequency, 10.525 gigahertz (GHz). The shape of the microwave beam and the maximum separation between the transmitter and the receiver are functions of antenna size and configuration. Various antenna configurations are available, including parabolic-dish arrays, strip-line arrays, and slotted arrays.
 - The parabolic antenna uses a microwave-feed assembly located at the focal point of a metallic parabolic reflector. A conical beam pattern is produced (see [Figure 6](#)). A strip-line antenna configuration produces a nonsymmetrical beam that is higher than its height. Larger antenna configurations generally produce narrower beam patterns.

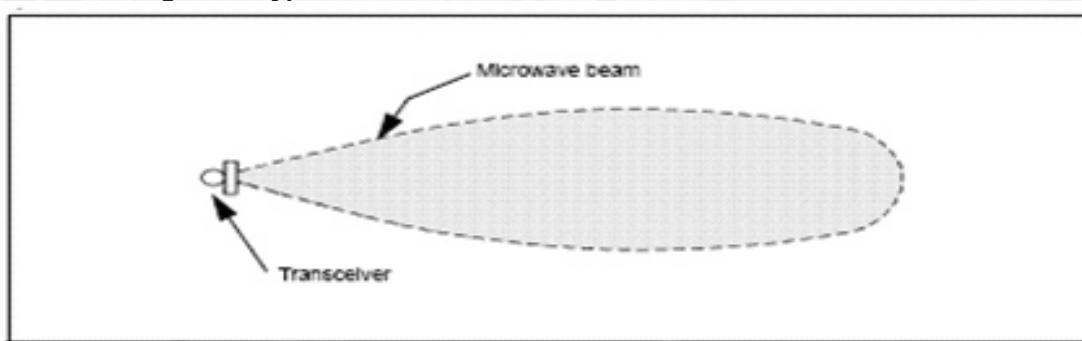
[RETURN TO TOP](#)

Figure 6: Stacked Microwave Configuration



- (c) Monostatic microwave sensors use the same antenna or virtually coincident antenna arrays for the transmitter and receiver, which are usually combined into a single package. Two types of monostatic sensors are available. Amplitude-modulated (AM) sensors detect changes in the net-vector summation of reflected signals similar to bistatic sensors. Frequency-modulated (FM) sensors operate on the Doppler principle similar to interior microwave sensors. The detection pattern is typically shaped like a teardrop (see [Figure 7](#)). Monostatic sensors can provide volumetric coverage of localized areas, such as in corners or around the base of critical equipment.

Figure 7: Typical Monostatic-Microwave-Sensor Detection Pattern



11. Infra-Red Sensors

- (a) Infra-red (IR) sensors are available in both active and passive models. An active sensor generates one or more near-IR beams that generate an alarm when interrupted. A passive sensor detects changes in thermal IR radiation from objects located within its field of view.
- (b) Active sensors consist of transmitter/receiver pairs. The transmitter contains an IR light source such as a gallium arsenide light-emitting diode (LED) that generates an IR beam. The light source is usually modulated to reduce the sensor's susceptibility to unwanted alarms resulting from

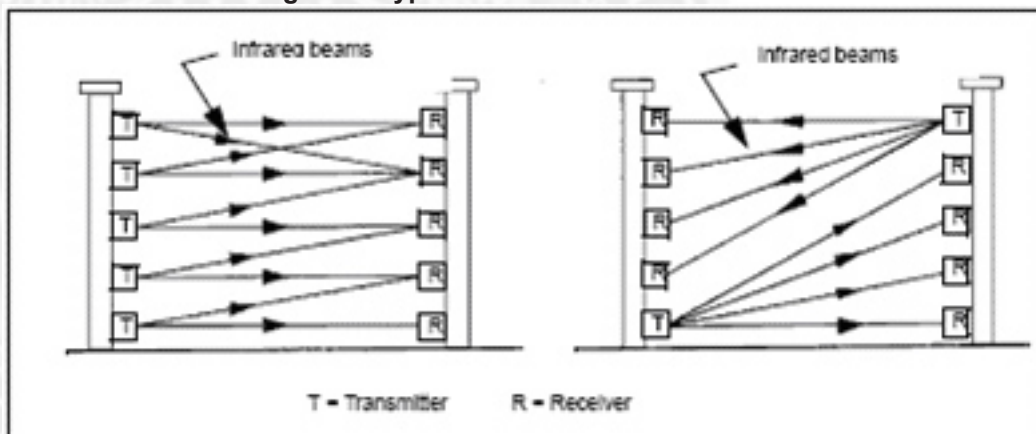
[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

sunlight or other IR light sources. The receiver detects changes in the signal power of the received beam. To minimize nuisance alarms from birds or blowing debris, the alarm criteria usually require that a high percentage of the beam be blocked for a specific interval of time.

- (c) Active sensors can be single- or multiple-beam systems. Because single-beam sensors can be easily bypassed, multiple-beam systems are generally used in perimeter applications. There are two basic types of multiple-beam configurations. One type uses all transmitters on one post and all receivers on the other post; the second type uses one transmitter and several receivers on each post. Both types are illustrated in [Figure 8](#).

Figure 8: Typical IR-Sensor Beam Patterns



- (d) The spacing between transmitters and receivers can be as great as 1,000 feet when operation is under good weather conditions. However, conditions such as heavy rain, fog, snow, or blowing dust particles attenuate the IR energy, reducing its effective range to 100 to 200 feet or less.

12. Video Motion Sensors - Exterior

- (a) A video motion sensor generates an alarm whenever an intruder enters a selected portion of a CCTV camera's field of view. The sensor processes and compares successive images from the camera and generates an alarm if differences between the images satisfy predefined criteria. Digital devices convert selected portions of the analog video signal into digital data that are compared with data converted previously; if differences exceed preset limits, an alarm is generated.
- (b) The signal processor usually provides an adjustable window that can be positioned anywhere on the video image. Available adjustments permit changing the window's horizontal and vertical sizes, its position, and its sensitivity. More sophisticated units provide several adjustable windows

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

that can be individually sized and positioned. Multiple windows permit concentrating on several specific areas of an image while ignoring others. For example, in a scene that contains several critical assets and multiple sources of nuisance alarms (such as large bushes or trees), the sensor can be adjusted to monitor only the assets and ignore the areas that contain the nuisance alarm sources.

- (c) The use of video motion-detection systems for exterior applications has been limited, primarily because of difficulties with uncontrolled exterior environments. Lighting variations caused by cloud movement and shadows of slow-moving objects, birds and animals moving within the camera's field of view, camera motion and moving vegetation during windy conditions, and severe weather conditions have traditionally caused a multitude of unwanted alarms in this type of system. Systems using more advanced signal-processing algorithms have improved motion-detection capability and nuisance-alarm rejection; however, they are still subject to high unwanted-alarm rates under certain conditions and should be used with due caution and extreme care.
- (d) For further information, see [Appendix 8.12, CCTV](#).

VI. INTERIOR INTRUSION DETECTION SENSORS

A. Planning

1. Interior intrusion-detection sensors are devices used to detect unauthorized entry into specific areas or volumetric spaces within a building.
2. These sensors are usually not designed to be weatherproof or rugged enough to survive an outdoor environment. Therefore, this type of sensor should not be used outdoors unless described by the manufacturer as suitable for outdoor use.
3. Interior intrusion-detection sensors generally perform one of three detection functions—detection of an intruder penetrating the boundary of a protected area, detection of intruder motion within a protected area, and detection of an intruder touching or lifting an asset within a protected area.
4. Interior sensors are commonly classified as boundary-penetration sensors, volumetric motion sensors, and point sensors. Although duress switches are not intrusion-detection sensors, they are included in this discussion because they are usually wired to the same equipment that monitors the interior intrusion-detection sensors.

B. Boundary Penetration Sensors

1. Boundary penetration sensors are designed to detect penetration or attempted

[RETURN TO TOP](#)

penetration through perimeter barriers. These barriers include walls, ceilings, duct openings, doors, and windows.

C. Structural-Vibration Sensors

1. Structural-vibration sensors detect low-frequency energy generated in an attempted penetration of a physical barrier (such as a wall or a ceiling) by hammering, drilling, cutting, detonating explosives or employing other forcible methods of entry. A piezoelectric transducer senses mechanical energy and converts it into electrical signals proportional in magnitude to the vibrations. To reduce false alarms from single accidental impacts on the barrier, most vibration sensors use a signal processor that has an adjustable pulse-counting accumulator in conjunction with a manual sensitivity adjustment. The count circuit can be set to count a specific number of pulses of specific magnitude within a predefined time interval before an alarm is generated. However, the circuitry is usually designed to respond immediately to large pulses, such as those caused by an explosion. The sensitivity adjustment is used to compensate for the type of barrier and the distance between transducers. Typically, several transducers can be connected together and monitored by one signal processor. [Figure 9](#) shows an example of wall-mounted, structural-vibration sensors.

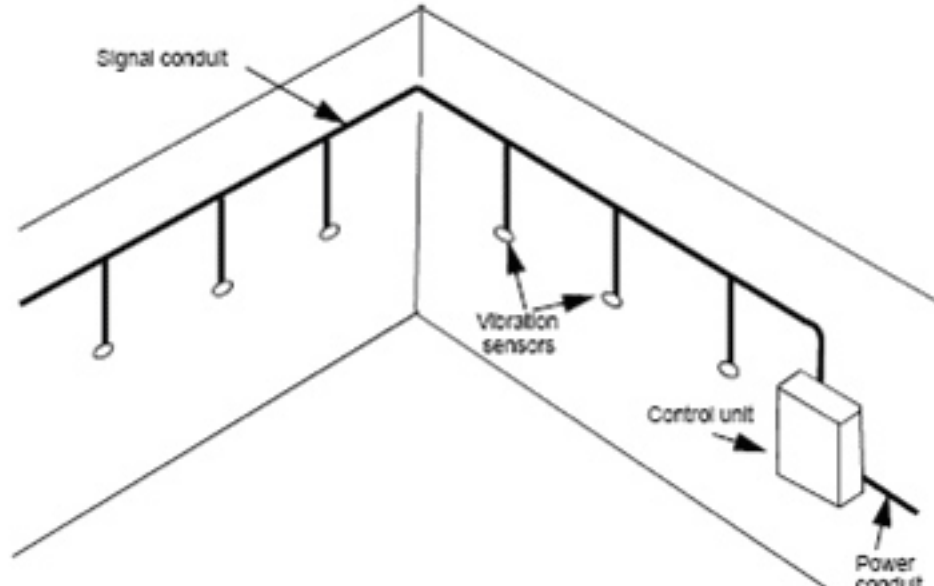
D. Glass-Breakage Sensors

1. Glass-breakage sensors detect the breaking of glass. The noise from breaking glass consists of frequencies in both the audible and ultrasonic range. Glass-breakage sensors use microphone transducers to detect the glass breakage. The sensors are designed to respond to specific frequencies only, thus minimizing such false alarms as may be caused by banging on the glass.

E. Passive Ultrasonic Sensors

1. Passive ultrasonic sensors detect acoustical energy in the ultrasonic frequency range, typically between 20-30 kilohertz (kHz). They are used to detect an attempted penetration through rigid barriers (such as metal or masonry walls, ceilings, and floors). They also detect penetration through windows and vents covered by metal grilles, shutters, or bars if these openings are properly sealed against outside sounds.

Figure 9: Wall-Mounted, Structural-Vibration Sensors



F. Detection Transducer

1. The detection transducer is a piezoelectric crystal that produces electrical signals proportional to the magnitude of the vibrations. A single transducer provides coverage of an area about 15 by 20 feet in a room with an 8- to 12-foot ceiling. A typical detection pattern is shown in [Figure 10](#). Ten or more transducers can be connected to a signal processor. As with vibration sensors, the signal processor for a passive ultrasonic sensor has manual sensitivity adjustment and an adjustable pulse counting accumulator.

G. Ultrasonic Sensors

1. Passive ultrasonic sensors detect ultrasonic energy that results from the breaking of glass, the snipping of bolt cutters on metal barriers, the hissing of an acetylene torch, and the shattering of brittle materials (such as concrete or cinderblock). However, the sensors will not reliably detect drilling through most material nor attacks against soft material such as wallboard. Their effective detection range depends largely on the barrier material, the method of attempted penetration, and the sensitivity adjustment of the sensor. Examples of maximum detection distances for a typical sensor for different types of attempted penetration are shown in [Table 1](#).

Figure 10: Typical Passive-Ultrasonic-Sensor Detection Pattern

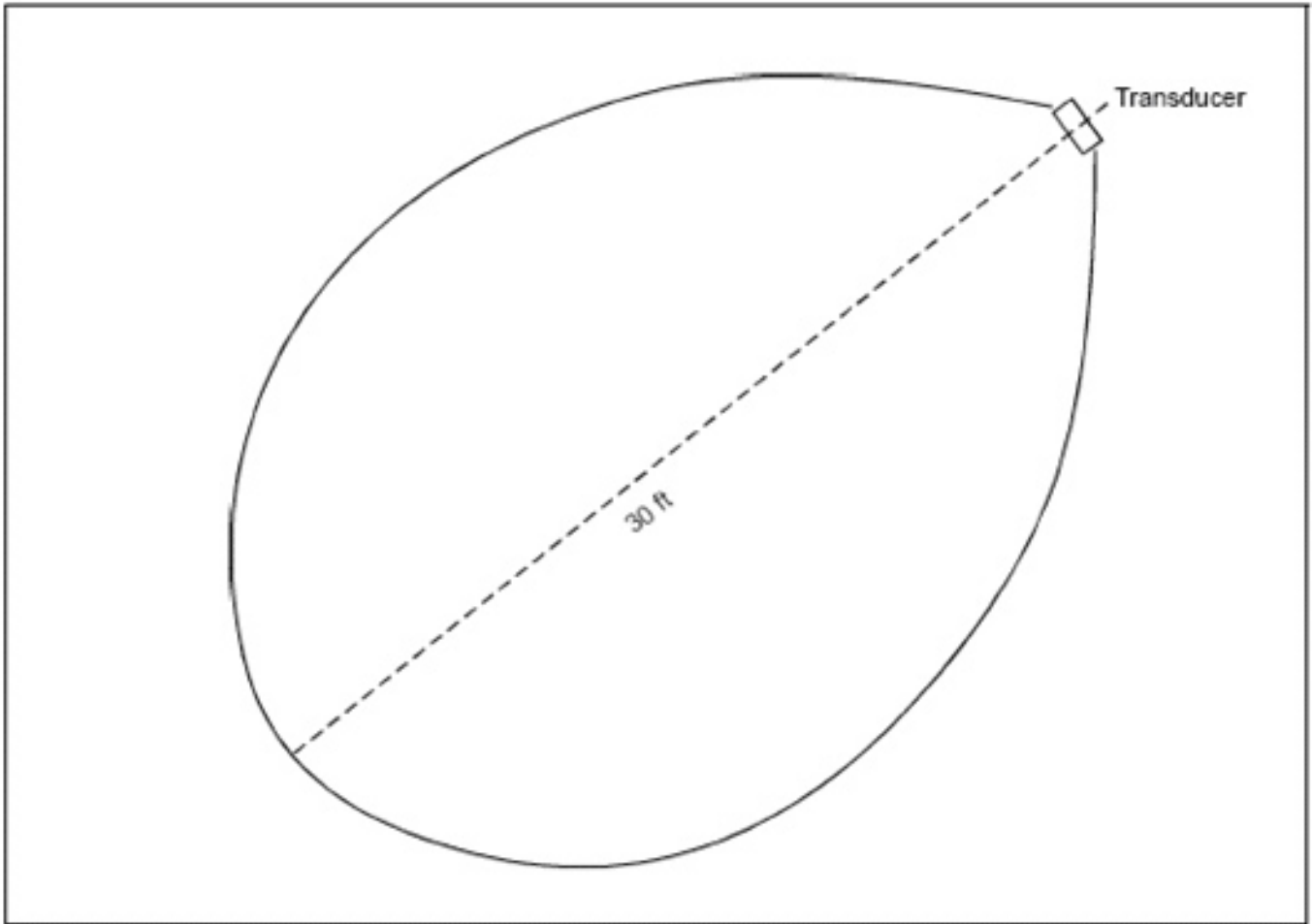


Table 1: Max. Detection Distances for Typical Sensors

Penetration	Distance (in Feet)
Cut 1/4-inch-thick expanded metal with bolt cutters	55
Cut 5/8-inch reinforcing bar with bolt cutters	45
Use acetylene cutting torch	39
Cut wood with circular saw	30
Cut 5/8-inch reinforcing bar with hacksaw	19
Drill through brick	15
Drill through 1/8-inch steel plate	6
Cut 1/8-inch steel plate with hacksaw	4
Drill through cinderblock	3

H. Balanced Magnetic Switches

1. Balanced magnetic switches (BMS) are typically used to detect the opening of a door. These sensors can also be used on windows, hatches, gates, or other

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

structural devices that can be opened to gain entry. When using a BMS, mount the switch mechanism on the door frame and the actuating magnet on the door. Typically, the BMS has a three-position reed switch and an additional magnet (called the bias magnet) located adjacent to the switch. When the door is closed, the reed switch is held in the balanced or center position by interacting magnetic fields. If the door is opened or an external magnet is brought near the sensor in an attempt to defeat it, the switch becomes unbalanced and generates an alarm. A BMS must be mounted so that the magnet receives maximum movement when the door or window is opened. [Figure 11](#) shows several configurations for mounting BMS.

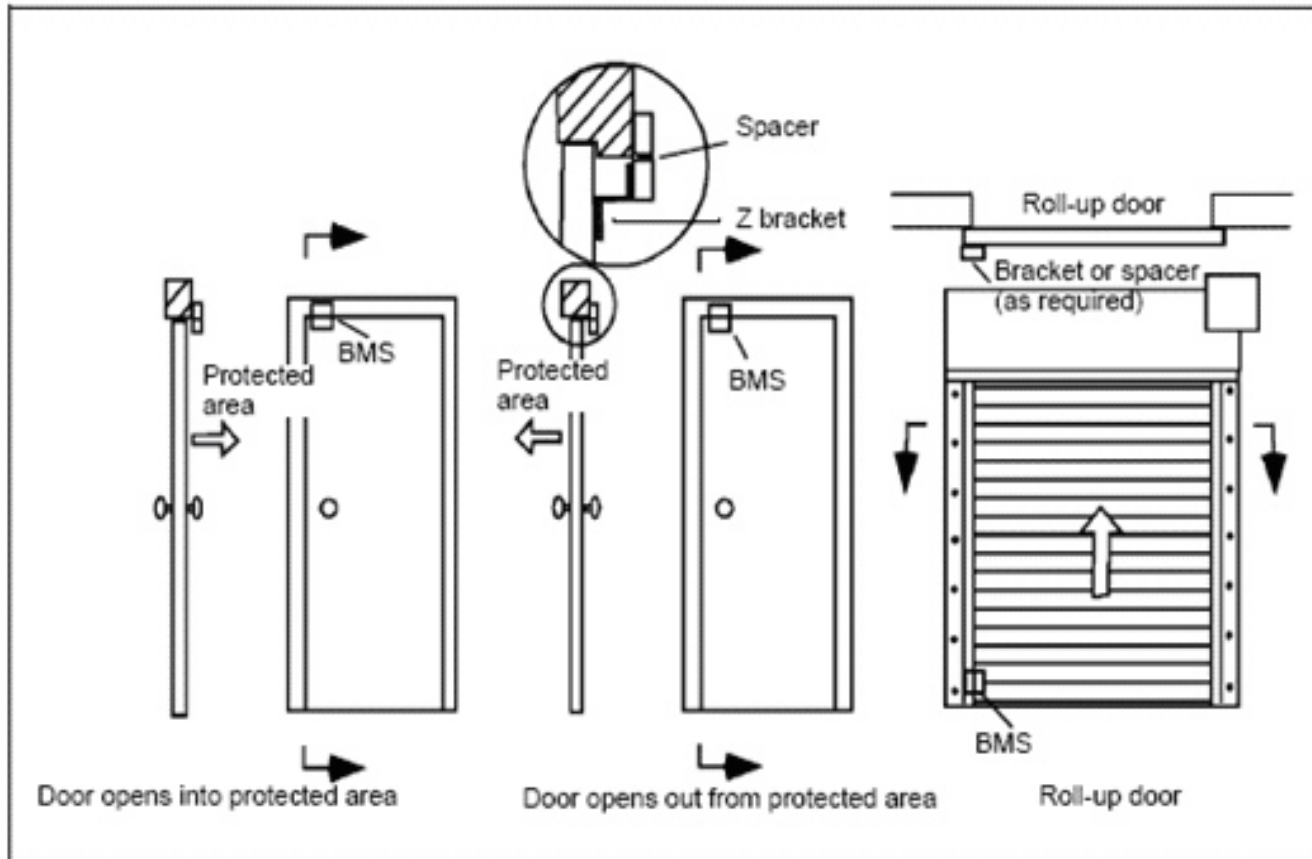
I. Grid-Wire Sensors

1. The grid-wire sensor consists of a continuous electrical wire arranged in a grid pattern. The wire maintains an electrical current. An alarm is generated when the wire is broken. The sensor detects forced entry through walls, floors, ceilings, doors, windows, and other barriers. An enamel-coated Number 24 or 26 American wire gauge (AWG) solid-copper wire typically forms the grid. The grid's maximum size is determined by the spacing between the wires, the wire's resistance, and the electrical characteristics of the source providing the current. The grid wire can be installed directly on the barrier, in a grille or screen that is mounted on the barrier, or over an opening that requires protection. The wire can be stapled directly to barriers made of wood or wallboard. Wood panels should be installed over the grid to protect it from day-to-day abuse and to conceal it. When used on cinder, concrete, and masonry surfaces, these surfaces must first be covered with plywood or other material to which the wire can be stapled. An alternative method is to staple the wire grid to the back side of a panel and install the panel over the surface.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Figure 11: BMS Mounting Configurations



J. Volumetric Motion Sensors

1. Volumetric motion sensors are designed to detect intruder motion within the interior of a protected volume. Volumetric sensors may be active or passive. Active sensors (such as microwave) fill the volume to be protected with an energy pattern and recognize a disturbance in the pattern when anything moves within the detection zone. Whereas active sensors generate their own energy pattern to detect an intruder, passive sensors (such as IR) detect energy generated by an intruder. Some sensors, known as dual technology sensors, use a combination of two different technologies, usually one active and one passive, within the same unit. If CCTV assessment or surveillance cameras are installed, video motion sensors can be used to detect intruder movement within the area. Since ultrasonic motion sensors are seldom used, they will not be discussed here. See [FM 3-19.30, Physical Security](#), for further information.

K. Microwave Motion Sensors

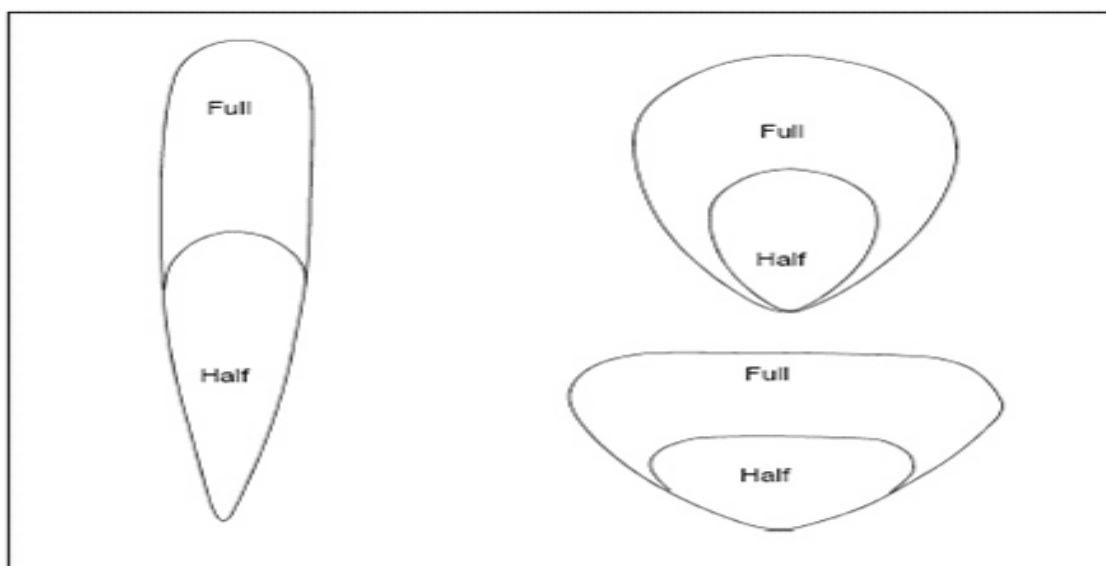
1. With microwave motion sensors, high-frequency electromagnetic energy is used to detect an intruder's motion within the protected area. Interior or sophisticated microwave motion sensors are normally used.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

L. Interior Microwave Motion Sensors

1. Interior microwave motion sensors are typically monostatic; the transmitter and the receiver are housed in the same enclosure (transceiver). They may each be provided with a separate antenna or they may share a common antenna. The high-frequency signals produced by the transmitter are usually generated by a solid-state device, such as a gallium arsenide field-effect transistor. The power generated is usually less than 10 milliwatts, but it is sufficient to transmit the signal for distances up to about 100 feet. The shape of the transmitted beam is a function of the antenna configuration. The range of the transmitted beam can be controlled with a range adjustment. A variety of detection patterns can be generated (see [Figure 12](#)). The frequency of the transmitted signal is compared with the frequency of the signal reflected back from objects in the protected area. If there is no movement within the area, the transmitted and received frequencies will be equal and no alarm will be generated. Movement in the area will generate a Doppler frequency shift in the reflected signal and will produce an alarm if the signal satisfies the sensor's alarm criteria. The Doppler shift for a human intruder is typically between 20 and 120 hertz (Hz). Microwave energy can pass through glass doors and windows as well as lightweight walls or partitions constructed of plywood, plastic, or fiberboard.
2. As a result, false alarms are possible because of the reflection of the microwave signals from the movement of people or vehicles outside of the protected area. The designer can sometimes take advantage of this when the protected area is large and contains a number of partitions.

Figure 12: Typical Detection Patterns for Microwave Motion Sensors[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

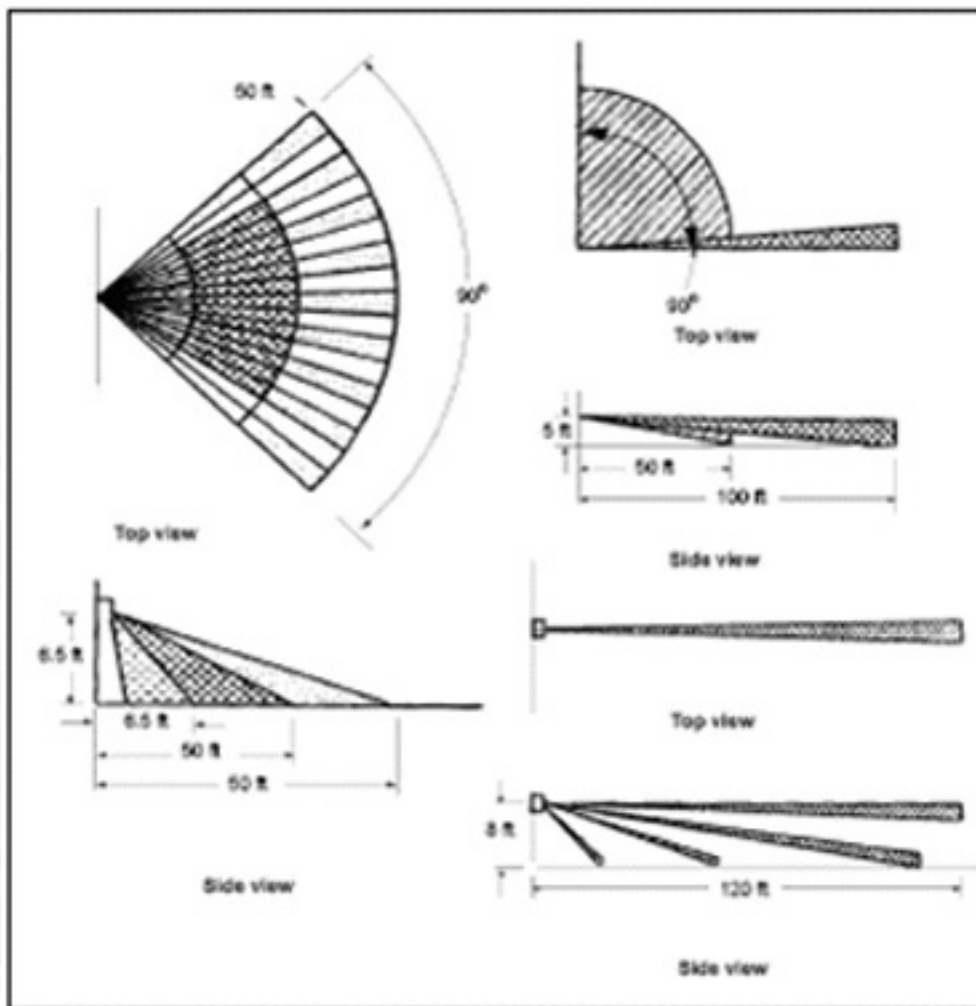
M. Sophisticated Microwave Motion Sensors

1. Sophisticated microwave motion sensors may be equipped with electronic range gating. This feature allows the sensor to ignore the signals reflected beyond the settable detection range. Range gating may be used to effectively minimize unwanted alarms from activity outside the protected area.

N. PIR Motion Sensors

1. Passive Infrared (PIR) motion sensors detect a change in the thermal energy pattern caused by a moving intruder and initiate an alarm when the change in energy satisfies the detector's alarm criteria. These sensors are passive devices because they do not transmit energy; they monitor the energy radiated by the surrounding environment.
2. All objects with temperatures above absolute zero radiate thermal energy. The wavelengths of the IR energy spectrum lie between 1-1,000 microns. Because the human body radiates thermal energy of between 7-14 microns, PIR motion sensors are typically designed to operate in the far IR wavelength range of 4-20 microns.
3. The IR energy must be focused onto a sensing element, somewhat as a camera lens focuses light onto a film. Two techniques are commonly used. One technique uses reflective focusing; parabolic mirrors focus the energy. The other uses an optical lens. Of the various types of optical lenses, Fresnel lenses are preferred because they can achieve short focal lengths with minimal thickness. Because IR energy is severely attenuated by glass, lenses are usually made of plastic.
4. The sensor's detection pattern is determined by the arrangement of lenses or reflectors. The pattern is not continuous but consists of a number of rays or fingers, one for each mirror or lens segment. Numerous detection patterns are available, several of which are shown in [Figure 13](#). The PIR is not provided with a range adjustment, but the range can be adjusted somewhat by manipulating the sensor's position; therefore, careful selection of the appropriate detection pattern is critical to proper sensor performance.

Figure 13 Typical Detection Patterns for a PIR Detector



5. Most manufacturers use a pyroelectric material as the thermal sensing element. This material produces a change in electric charge when exposed to changes in temperature. To minimize false alarms caused by changes in ambient temperature, most manufacturers use a dual-element sensor. The sensing element is split into halves, one that produces a positive voltage pulse and the other a negative pulse when a change in temperature changes. An intruder entering one of the detection fingers produces an imbalance between the two halves, resulting in an alarm condition. Quad-element sensors that combine and compare two dual-element sensors are also in use. Pulse-count activation, a technique in which a predefined number of pulses within a specific interval of time must be produced before an alarm is generated, is also used.

O. Dual-Technology Sensors

1. To minimize the generation of alarms caused by sources other than intruders, dual-technology sensors combine two different technologies in one unit. Ideally, this is achieved by combining two sensors that individually have a high DP and

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

do not respond to common sources of false alarms. Available dual-technology sensors combine an active ultrasonic or microwave sensor with a PIR sensor. The alarms from each sensor are logically combined in an “and” configuration; that is, nearly simultaneous alarms from both active and passive sensors are needed to produce a valid alarm. Although combined technology sensors have a lower false-alarm rate than individual sensors, the DP is also reduced. For example, if each individual sensor has a DP of 0.95, the DP of the combined sensors is the product of individual probabilities (0.9).

2. Also, ultrasonic and microwave motion sensors have the highest probability of detecting movement directly toward or away from the sensor, whereas PIR motion sensors have the highest probability of detecting movement across the detection pattern. Therefore, the DP of sensors combined in a single unit is less than that obtainable if the individual sensors are mounted perpendicular to each other with overlapping detection patterns. Because of the lower false alarm rate, the reduced DP can be somewhat compensated for by increasing the sensitivity or detection criteria of each individual sensor.

P. Interior Video Motion Sensors

1. A video motion sensor generates an alarm when an intruder enters a selected portion of a CCTV camera’s field of view. The sensor processes and compares successive images between the images against predefined alarm criteria. There are two categories of video motion detectors—analog and digital. Analog detectors generate an alarm in response to changes in a picture’s contrast. Digital devices convert selected portions of the analog video signal into digital data that are compared with data converted previously; if differences exceed preset limits, an alarm is generated. The signal processor usually provides an adjustable window that can be positioned anywhere on the video image. Available adjustments permit changing horizontal and vertical window size, window position, and window sensitivity. More sophisticated units provide several adjustable windows that can be individually sized and positioned. Multiple windows permit concentrating on several specific areas of an image while ignoring others. For example, in a scene containing six doorways leading into a long hallway, the sensor can be set to monitor only two critical doorways. For further information, see [Chapter 8.12, CCTV Systems](#)

VII. POINT SENSORS

A. Planning

1. Point sensors are used to protect specific objects within a facility. These sensors (sometimes referred to as proximity sensors) detect an intruder coming in close proximity to, touching, or lifting an object. Several different types are available including capacitance sensors, pressure mats, and pressure switches. Other

[RETURN TO TOP](#)

types of sensors can also be used for object protection.

B. Duress Alarm Devices

1. Duress-alarm devices may be fixed or portable. Operations and security personnel use them to signal a life-threatening emergency. Activation of a duress device will generate an alarm at the alarm-monitoring station. Because of the nature of the alarm, duress devices should never annunciate at the point of threat. These devices are customarily manually operated.
2. Fixed duress devices are mechanical switches permanently mounted in an inconspicuous location, such as under a counter or desk. They can be simple push-button switches activated by the touch of a finger or hand or foot operated switches attached to the floor.
3. Portable duress devices are wireless units consisting of a transmitter and a receiver. The transmitter is portable and small enough to be conveniently carried by a person. The receiver is mounted in a fixed location within the facility. Either ultrasonic or RF energy can be used as the communication medium. When activated, the transmitter generates an alarm that is detected (within range) by the receiver. The receiver then activates a relay that is hardwired to the alarm-monitoring system.

C. Monitoring

1. The Homeland Security Act of 2002 provides the Secretary of Homeland Security with the authority and responsibility to “protect the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government (including any agency instrumentally or wholly owned or mixed-ownership corporations thereof) and the persons on the property.” This responsibility has been delegated to U.S. Immigration and Customs Enforcement’s Federal Protective Service (FPS). As such, FPS also offers IDS monitoring and services through GSA leases.
2. FPS has designed and built four Mega-Centers to provide monitoring and related services. These centers are located in Suitland, Maryland; Philadelphia, Pennsylvania; Battle Creek, Michigan; and Denver, Colorado. Among other tasks, these centers monitor intrusion/duress alarm systems, fire detection systems, environmental systems, and elevator emergency telephones for multi-regional areas. In order to take full advantage of the Mega-Centers’ IDS monitoring capabilities, FPS mandates that all installations and upgrades of the IDS in both leased and government facilities are standardized on a national basis, are fully compatible with the standardized alarm-receiving equipment existing in the Mega-Centers, and are capable of being remotely programmed with software from the approved panel manufacturers.

3. A national decision was made that FPS would only recommend and support alarm systems that fully interfaced with the control center's equipment and software. Therefore, FPS requires that only remote-programmable alarm systems are specified when designing or upgrading alarm systems that are monitored at the Mega-Center. Additionally, all remote-programmable alarm systems must be able to easily communicate with the Mega-Centers' monitoring equipment.
4. Approved alarm panels must communicate via the Mega-Center's alarm receivers. The Mega-Centers can also accept most digital communicators for Fire Detection Systems that transmit one of the standard formats. (communications protocol): ADEMCO Contact ID, Radionics / Bosch Modem II, Modem IIE and Modem IIIA or SIA.
5. All alarm systems/IDS must have tampered devices, cabinets, and junction boxes. All devices will report as one point as a zone description that can be used when reporting an alarm condition to the responding authority.
6. FPS cannot monitor any alarm system that does not fully comply with the above referenced criteria. If a system does not meet these criteria, either the customer or GSA shall assume the cost of commercial monitoring.
7. In order to ensure necessary standardization, full compatibility, and coordination of effort, designs for all installations and upgrades of intrusion / duress alarm systems must be coordinated with the serving Mega-Center.
8. All IDS shall be installed in accordance with UL Guidelines for Burglary Intrusion Detection Systems. The Security System installer/vendor must properly complete and communicate the FPS Mega-Center Alarm Requirements (MAR) Document to the respective FPS Mega-Center. The MAR document includes the following information:
 - (a) A record of the alarm account data
 - (b) A list of all devices and a sketch of the device locations
 - (c) The emergency telephone list
 - (d) User codes
 - (e) A test of the alarm panel and system
9. The Security System installer/vendor must have documented experience installing IDS that are monitored by the Federal Protective Service or the United States Federal government. The Security System installer/vendor is not to be released of their contractual obligations until the CBP Office of Internal Affairs Security Management Division identified personnel have received a minimum of 4 hours training to properly operate, maintain, and troubleshoot the Intrusion

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Detection System, and until the IDS system is 100% operational and being actively monitored by the respective FPS Mega-Center.

10. The installed IDS shall be fully integrated with the Security Management System and be capable of having all alarm situations simultaneously report to both the on site Security Management System and the FPS Mega-Center.
11. FPS cannot monitor any alarm system that does not fully comply with the above referenced criteria or does not have an active dedicated analog phone line for each alarm panel installed. Therefore, it is imperative that there is no deviation from the IDS requirements listed above.

VIII. SYSTEM VALIDATION ASSESSMENT FOR EMERGENCY RESPONDERS (SAVER)

- A. DHS has established the [System Assessment and Validation for Emergency Responders \(SAVER\)](#) program to assist with procurement decisions. The SAVER Program conducts unbiased operational tests on commercial equipment and systems, and provides those results along with other relevant equipment information to the community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the [DHS Authorized Equipment List \(AEL\)](#).
- B. Follow these steps to reach the [SAVER Project Library Index](#).
 1. Go to the [Project Library Index link](#);
 2. Scroll down to, and click on, “14 Physical Security Enhancement Equipment”;
 3. Select “14SW Surveillance, Warning, Access Intrusion Control”;
 4. Click on “14SW-01 General”;
 5. Select “14SW-01-Sensors and Alarms, Alarms”;
 6. Click on “14SW-01-IDS”; and
 7. Chose the appropriate IDS assessment project document.
- C. To request the complete IDS Handbook, follow this link to the [SAVER Document Request Form](#). Enter your e-mail address and choose the format for the document (e-mail, mailed CD, or mailed hard copy). This link leads only to the request form for the full IDS Handbook. To view the project highlights or assessment summary documents, follow the instructions above.







APPENDIX 8.10: HOLD ROOMS

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

I. Hold Rooms

A. General

1. A hold room is a secure facility for the detention of aliens encountered and processed by operational components of CBP.
2. The hold room is used for detainees and is located within the access-controlled secure and violator processing area. All access control equipment will be HSPD-12/FIPS 201 compliant systems and will only be installed by approved GSA Schedule 70 vendors.
3. Hold rooms for detainees must be constructed to hardened construction standards and must be situated in a secure area to ensure the safety of both officers and the traveling public. Hold rooms should be co-located and rectangular in shape with no dividing walls or partitions. All fixtures must meet detention-grade standards.
4. Hold Rooms are located in the following CBP facilities:
 - (a) Border Patrol Stations
 - (b) Border Patrol Sector Headquarters
 - (c) Border Patrol Check Points
 - (d) District Offices
 - (e) Service Processing Centers
 - (f) Ports of Entry (Air, Land, Sea)
 - (g) Anti-Smuggling Units
 - (h) Staging and Alien Detention Removal Facilities
5. The nature and circumstances of detentions are governed by existing CBP policy, including CBP Directives No. 3340-030 and 3340-030B:
6. Minimum square footage per occupant of hold rooms is determined by the following method:
 - (a) 25 sq. ft of common space for wheelchair turnaround circulation as required by ADA
 - (b) 5 sq. ft for toilet and lavatory fixtures

(c) 7 sq. ft of unencumbered for each detainee (Unencumbered is usable space that is not encumbered by fixtures or furnishings)

(d) A single occupant hold room for detainees is therefore a minimum of 37 Sq. ft. Multiple occupancy rooms shall be 37 Sq. ft for the first occupant and 7 sq. ft of unencumbered space for each additional occupant.

7. Other space related requirements include:

(a) 1 toilet per 15 detainees

(b) Males and females must be kept in separate hold rooms (including juveniles)

(c) Young children must remain with their mothers

8. Associated spaces include:

(a) Interview Rooms must be located adjacent to the hold rooms, and either within or outside a secure perimeter zone. They must be under 24X7 surveillance and detainees are required to be secured with handcuffs. If located within the violator processing area, the interview room must have the same construction criteria as the hold room. Asylum seekers must be placed in a separate interview room.

(b) Search Rooms must be located adjacent to hold rooms within a secure perimeter zone. It has the same specifications as a hold room, except there are no windows, toilets and floor drains.

(c) Alien Property Storage Rooms must be located within a security perimeter, securely constructed for high attack resistance and they require a door lock and an Intrusion Detection System.

9. ADA and Toilet Facilities

(a) The Americans with Disabilities Act (ADA) requires that public and common use toilet facilities must be accessible to the disabled. The following provisions apply to hold rooms:

- Hold rooms shall be ADA-Compliant.
- A grab bar must be installed inside the toilet stall designated for the disabled.
- The toilet stall and toilet fixture must have the proper dimensions.
- Where an independent drinking fountain or lavatory is indicated, the

[RETURN TO TOP](#)

top must have the proper height from the floor.

B. Physical Security Requirements of a Hold Room

1. In general, all hold rooms must have the following requirements:

- (a) Located within a security perimeter
- (b) Securely constructed for high attack resistance
- (c) Minimum space as defined above
- (d) No beds; a hold room is not designed for sleeping
- (e) Furniture must be of solid construction and secure to wall or floor

2. According to the Service Processing Center Detention Construction Standards (SPC Detention Construction Standards, Dated 01 November 2004), hold rooms are classified as having a Medium Security Level.

C. "Medium" security walls shall be constructed using one of the following methods:

- 1. Concrete masonry unit walls shall be a minimum nominal 8" (200 mm) wide units reinforced with #4 (No. 13 metric) vertical reinforcing bar at 16" (400 mm) on center. All cells of concrete masonry units shall be fully grouted with 3,000 psi (21 Mpa) grout.
- 2. Pre-cast concrete panel walls shall be a minimum nominal 4" (100 mm) wide, minimum strength of 5,000 psi (35 Mpa) and reinforced with minimum W4 (MW26) welded wire fabric at 4" (100 mm) on center in both directions, conforming to ASTM A185.
- 3. Cast-in-place concrete walls shall be a minimum 6" (150 mm) wide, minimum strength of 3,000 psi (21 Mpa) reinforced with #4 (No. 13 metric) reinforcing bars at 8" (200 mm) on center in one direction. Cast-in-place concrete walls that are less than 6" (150 mm) wide, but no less than 4" (100 mm) wide shall have a minimum strength of 5,000 psi (35 Mpa) reinforced with W4 (MW26) welded wire fabric at 4" (100 mm) on center in both directions.
- 4. Steel wall panels shall be 0.093 in. (12-gauge) minimum thickness A-60 galvaneal steel conforming to ASTM A 653-CS requirements. All structural or stiffening members shall be 0.058 in. (16-gauge) minimum thickness A-60 galvaneal steel conforming to ASTM A 653-LFQ requirements. All structural tubing shall be 0.115 in. (11-gauge) minimum thickness steel conforming to ASTM A 653-CS and ASTM A-525, G-90 galvanized requirements.

[RETURN TO TOP](#)

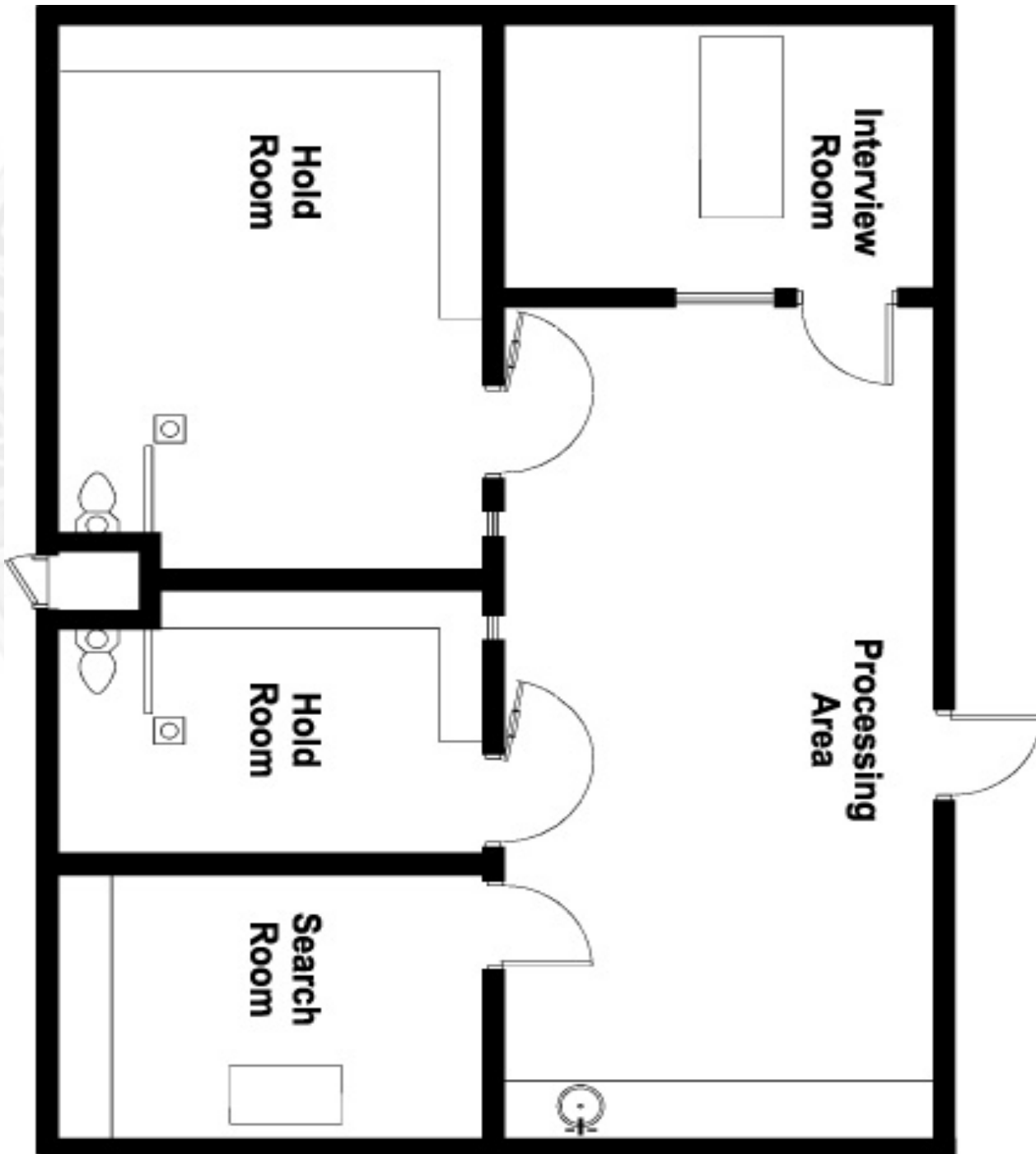
D. "Medium" security roof/ceiling construction shall be constructed of the following:

1. Cast-in-place concrete slabs shall be a minimum of 6" (150 mm) thick, 3,000 psi (21 Mpa) concrete with #4 (No. 13 metric) reinforcing bars at 16" (400 mm) on center in one direction. Cast-in-place concrete slabs that are less than 6" (150 mm) thick, but no less than 4" (100 mm) thick shall have a minimum strength of 5,000 psi (35 Mpa) reinforced with W4 (MW26) welded wire fabric at 4" (100 mm) on center in both directions.
2. Composite metal ceiling shall be a minimum of 4" (100 mm) total depth, 3,000 psi (21 Mpa) concrete, #4 (No. 13 metric) bars 16" (400 mm) on center in one direction.
3. Prestressed concrete tees or hollow core slabs shall have a concrete topping to give adequate cover for #4 (No. 13 metric) bars 16" (400 mm) on center in one direction.
4. Solid concrete planks shall have #4 (No. 13 metric) reinforcing bars at 16" (400 mm) on center in one direction. No concrete topping is required.
5. Metal acoustical ceiling panel shall be maximum security double skin metal 0.125" (3.2 mm) thick with perforations.
6. Metal roof ceilings shall be a minimum of 12-gauge. No additional reinforcing is required, however the ceiling must be securely tied to the "medium" security walls.

[BACK](#)

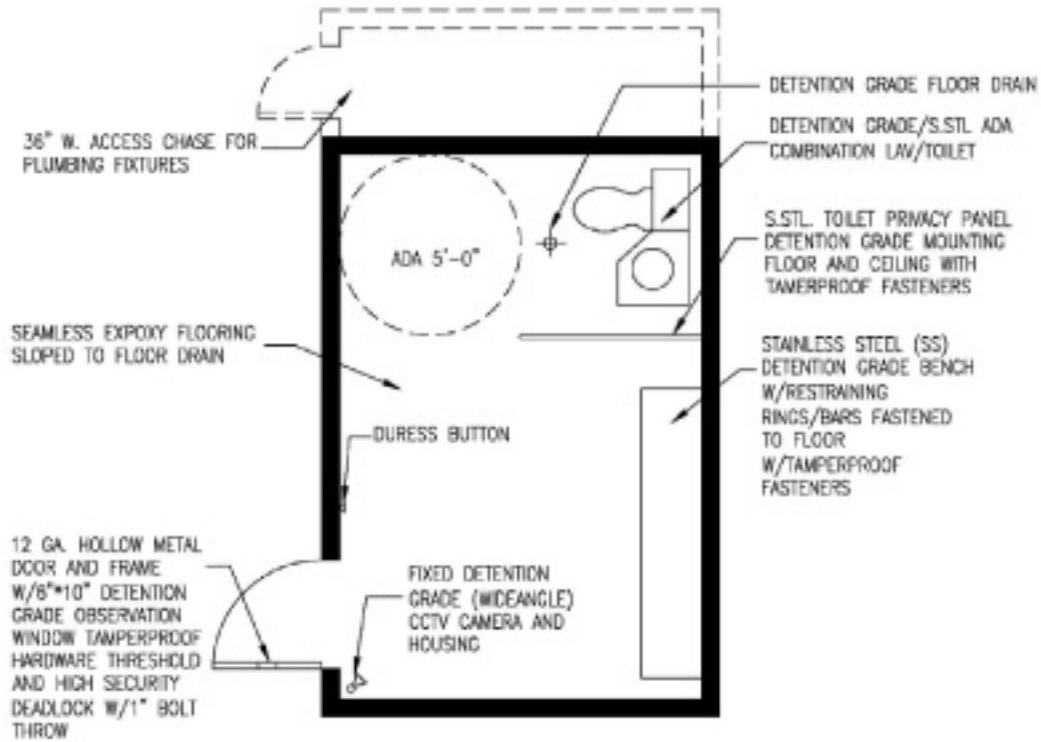
[RETURN TO TABLE OF CONTENTS](#)

II. LAYOUT

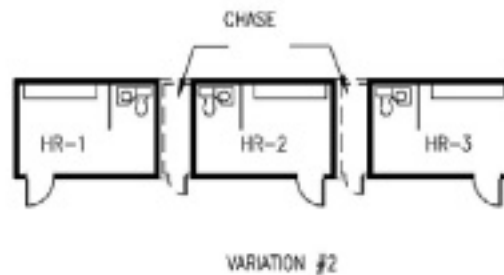
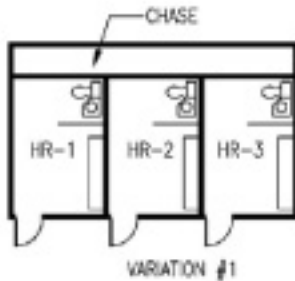


[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.



HOLD ROOM
MALE, FEMALE, JUVENILE



III. INTERSECTIONS OF HORIZONTAL AND VERTICAL SURFACES

- A. Continuity of materials is preferred to facilitate a continuous security enclosure. Where dissimilar materials occur, provide sufficient connections to prevent deflection of materials; or continuously weld ceiling to a steel member anchored to wall or foundation.
- B. Security bars must be continuous at all intersections; the bars must go around the corners and continue into adjacent slabs or secure ceiling construction. When this cannot be accomplished, a continuous #4 (No. 13 metric) reinforcing bar shall be cast no more than 1 ½" (38 mm) from the edge of the concrete unit where it meets other concrete or masonry members. These requirements must be coordinated with masonry horizontal reinforcing, and dissimilar concrete materials; i.e. masonry and cast-in-place concrete.

1. Penetrations

- (a) Security barriers are required on all penetrations in "high" and "medium" secure walls, floors, and ceilings where opening is larger than 8" x 8" (200 mm x 200 mm) or larger than 5" (125 mm) slit. Security barriers are required on all penetrations 5" (125 mm) wide which exceed 24" (600 mm) in length.
- (b) Security barriers shall be constructed of 7/8" (22 mm) diameter round bars or 2" x 2" x 1/4" (50 mm x 50 mm x 6 mm) structural steel tubing. Space between bars or tubing shall not exceed 5" (125 mm). Bars longer than 24" (600 mm) shall be reinforced with an intermediate flat bar, 2 1/2" x 3/8" (63.5 mm x 9.5 mm), welded to the barrier frame and tack welded to each bar. The flat stock is installed perpendicular to the bars and at the midpoint of the bars to prevent spreading.
- (c) Bars on security barriers at central control or housing control must be horizontal (to provide visibility). Bars on all other security barriers must be vertical. Bars on security barriers at central control or housing control are not required to have an intermediate reinforcement at 24" (600 mm).

2. Windows

- (a) The preferred location for hold rooms is an interior space without an exterior window.
- (b) Maximum size required to view detainees for suicide prevention, vandalism and other behaviors. Tinting is allowed with adjustable light levels to control visibility.
- (c) Glazing must be all polycarbonate laminates, glass clad polycarbonates,

[RETURN TO TOP](#)

or all glass laminates in accordance with local building codes.

3. Doors and Frames

- (a) Door frames shall be fabricated from a minimum of 12 or 14-gauge welded steel and have an integral stop and trim. All corners shall be mitered and welded. Fabricate with concealed stiffeners, reinforcement, and edge channels.
- (b) All exposed fasteners shall have countersunk, vandal-proof heads. Three silencers on strike jamb of frame and three wall anchors per jamb at hinge and strike levels.
- (c) Door width – 3 feet 2 inches for masonry opening. The door must be detention hollow metal 2 inches thick in flush panel design. It must be mortised, reinforced, drilled, and tapped to receive mortise hardware. Provide institutional, full mortise hinges with tamper-resistant fasteners and non-removable pins. Provide four hinges for doors 85 inches or more tall and 37 inches wide.
- (d) Doors and frames must have a factory-applied rust-inhibitive primer.
- (e) Vision panel should be polycarbonate laminate, glass-clad polycarbonate or glass laminate. The dimensions should be 4 feet x 10 inches, either square centered or rectangle off-center. Secure glazing stop with tamper-resistant screws.
- (f) Doors should swing out of hold room and a door pull should be placed on the door face outside the hold room.
- (g) Access doors located inside the hold room must meet the security requirements of the trades needing access to concealed equipment. Provide 2 inch exposed flange around the perimeter frames installed in masonry and finished frames with adjustable metal masonry anchors. Install a concealed piano hinge set to open 175 degrees. Furnish two keys per lock. Standard access doors may be used when located outside the hold room.

4. Door Hardware

- (a) Detention –type hardware is required, as indicated below. Finish of visible parts must match finish of other building hardware.
- (b) Hinges: 4 1/2" X 4 1/2", minimum 3 per door, heavy duty ball bearing type with tamper-resistant screws and non-removable pins.

- (c) Locks: Locks shall be detention dead bolt, heavy duty, mortised (MOGUL Key on One Side) mechanical with ADA compliant lever handles; except where suicide resistance is warranted, a substitute cone-shape handle may be used. Locks with interchangeable cores are acceptable (obtain approval from COTR and Using Agency). It must deadlock in both locked and unlocked positions.
- (d) Door Pull: Raised pull on outside of door. Pushplate not required on inside face.
- (e) Door Stops/Wall Bumpers: Dome type 13/8" high or as required to meet applicable conditions.
- (f) Door Closers: No closers or self-closing hinges on hold rooms. Closers are required on doors to a secure perimeter.
- (g) Additional information about specifications for Electro-Mechanical Locks can be found in the following UL Listings: UL1034 listed as Burglary-Resistant Mechanisms, and UL10B listed as Fire Door Accessories.

IV. PLUMBING

A. General

1. When possible, all plumbing fixtures shall be wall-mounted and securely fastened from the rear. This requires an accessible pipe chase in the back of the fixture. Valves and flow controls must be accessible to provide service from the pipe chase without disturbing the connecting piping. Install water service valve in all water lines (hot and cold) to the fixture. Each water closet of each back-to-back pair of water closets shall be provided with an accessible cleanout.
2. Hot water supply to lavatories shall be thermostatically remote controlled to limit water temperature to 110 degrees Fahrenheit.
3. All fixtures must be totally vandal-proof. There can be no attachments to the wall that can be fashioned into weapons.
4. Hold room plumbing requirements shall be coordinated with the building plumbing system, including supply, waste, and vent piping.
5. Drainage from hold rooms shall be isolated from that of other areas until passing through a trash trap.

B. Plumbing Design and Fixture Selection

1. Stainless Steel Combination Water Closet/Lavatory Unit

[RETURN TO TOP](#)

- (a) Within holding rooms a combination water closet and lavatory units shall be a minimum of 12 or 14-gauge, Type 304 stainless steel with satin finish. Construction shall be welded with no seams.
- (b) Toilet shall be blowout jet type with an elongated bowl, self-draining flushing rim, and an integral contoured seat with a sanitary high polish finish.
- (c) Countertop shall have a self-draining soap dish. Fixture shall be “off the floor” type.
- (d) Lavatory shall have pneumatically operated, push-button valve. A roof mounted penal bubbler shall be provided. Integral recessed toilet paper holder shall be provided. Fixture shall withstand 3,000 lb. loadings without permanent damage.
- (e) Where required for handicapped accessibility, special ADA units may be used or separate stainless steel fixtures. Where these fixtures are replacing existing toilets, most manufacturers produce “replacement” fixtures which allow the use of custom floor outlet locations.

2. Stainless Steel Water Closet

- (a) Within holding rooms where combination units are not used, water closets shall be a minimum of 12 or 14-gauge, Type 304 stainless steel with satin finish. Construction shall be seamless welded.
- (b) Toilet shall be blowout jet type with an elongated bowl, self-draining flushing rim, and an integral contoured seat with a sanitary high polish finish.
- (c) Fixture shall be wall mounted at ADA height. Fixtures withstand 3,000 lb. loadings without permanent damage.
- (d) Flush valve shall be concealed and serviced from the rear. Where these fixtures are replacing existing toilets, most manufacturers produce “replacement” fixtures which allow the use of custom floor outlet locations.

3. Stainless Steel Lavatory

- (a) Within holding rooms where combination units are not used, lavatories shall be 14-gauge, Type 304 stainless steel and ADA compliant.
- (b) Lavatory shall be wall hung and totally enclosed.
- (c) Countertop shall have an air-circulating, self-draining soap dish. A separate ceiling mounted bubbler shall be provided with separate push

[RETURN TO TOP](#)

button for drinking water.

- (d) Pneumatic or electronic push button controls shall be used and mounted at ADA compliant height. Where these fixtures are replacing existing lavatories, most manufacturers produce “replacement” fixtures which allow the use of custom drain outlet locations.

4. Floor Drains

- (a) Floor drains shall be cast iron with bronze grates and vandal resistant fasteners. Floor drains shall be not less than 4 inches in diameter.
- (b) The trap shall be equipped with a trap primer.
- (c) Installation of all floor drains shall be closely coordinated with the structural design of the building.
- (d) The floor surface shall slope in all directions toward the floor drain.
- (e) The screws holding the cover shall be ground down and filled with lead.

5. Hose Bibbs

- (a) Provide a recessed, stainless steel hose bibb box with a locking cover, outside the hold room for routine cleaning of the floor.

6. Security Mirrors

- (a) Mirrors shall be 20 gauge chrome-plated steel with 1/2 inch thick fiberboard backing.
- (b) Frame shall be seamless 14-gauge , Type 304 stainless steel.

7. Sprinkler System

- (a) Sprinkler heads in hold rooms shall be coordinated with the building sprinkler system.
- (b) The hold room system shall be isolated from the building system with a shut off valve, clearly labeled, serving the hold room zone.
- (c) Sprinkler heads designed specifically for detention facilities shall be specified.

8. Liquid Soap System

- (a) A centralized, pressurized liquid soap system designed for correctional use shall be used.

V. MECHANICAL SYSTEMS

A. Heating, Ventilation and Air Conditioning

1. Registers and grilles shall be designed and constructed specifically for use in correction and detention facilities. The face shall be fabricated using cold rolled steel, 3/16" thick steel face with 5/16" diameter holes on 7/16" staggered centers. A 3/16" thick steel sleeve shall be stitch welded to the face and along the entire length of all sleeve seams. All shall meet or exceed ANSI or ASTM Standard Specifications for Detention Area Use.
2. Provide barrier grilles within all ducts penetrations in walls of hold rooms where one dimension is larger than 5" (125 mm) and the other dimension is larger than 8" (200 mm). Barrier grilles shall also be placed within all ductwork to and from rooftop air handling equipment.

VI. ELECTRICAL

A. General

1. The electrical system required for hold rooms shall be coordinated with the building's electrical system. The following will be the basis for the electrical system design:
 - (a) Use only tamper resistant detention-type fluorescent light fixtures.
 - (b) Light fixtures are to be controlled from outside the hold rooms with a high-security key-operated switch.
 - (c) Electrical outlets, light switches or thermostats shall not be placed inside hold rooms.
 - (d) Light fixtures shall have emergency power backup

B. Lighting

1. Hold Rooms must have maximum-security type ceiling surface mounted light fixtures. They are described below:
 - (a) Housing, back, and door shall be 14-gauge steel with continuous exterior welds that are ground smooth and reinforced at the corners. The housing shall have a continuous steel piano hinge spot-welded and bolted to door frame for hinged door or spot welded to housing and back for hinged

[RETURN TO TOP](#)

housing. The hinge pin shall be welded to hinge to prevent removal. Grind all welds smooth. Outer lens shall be 0.375" clear polycarbonate backed with an inner lens of 0.125" prismatic polycarbonate. Lens retention to be by means of continuous 14 gauge L-angle along lens for length of lens opening. The inside and outside of housing shall be white polyester powder paint, 1.4 to 1.7 mil thick, with minimum reflectance of 85%. Cell illumination level is to be a minimum of 215 lux (20 foot candle) throughout the entire cell area. Particular attention shall be given to providing the 215-lux illumination level at the desk level and in the personal grooming area.

VII. POWER

1. Emergency Generation

- (a) Emergency power shall be derived from a 480/277 volt, 3-phase, 4-wire diesel engine driven generator sized to carry the required loads, along with a second, equally-sized generator for back-up.
- (b) The generators shall serve distribution panel boards in the main electrical room through a 4-pole automatic transfer switch (ATS). This emergency system shall provide power for the life safety/security systems and other essential loads upon failure of the normal electrical power service for a minimum of 72 hours continuous operation prior to re-fueling.
- (c) Emergency generators shall be located outside the secure perimeter. Items that must be on the emergency generator include:
 - Security equipment
 - Emergency lighting
 - Alarm systems
 - Communications equipment
 - Computer database (UPS system)
 - Ventilation and heating system to maintain habitable conditions during emergency periods
 - Essential food service equipment to allow continued operation during emergency periods

2. Uninterruptible Power Supply

[RETURN TO TOP](#)

- (a) Uninterruptible power supplies (UPS) shall be provided for all security system components. The UPS shall be sized to provide backup power for the full load of the security system for a minimum period of ten (10) minutes.
- (b) This system is designed to handle all security systems in the event of a primary power loss until such time as the emergency generator takes over.

3. Power Outlets

- (a) Electrical outlets shall not be provided in areas generally accessible to groups of detainees. Holding rooms shall not have electrical or special systems outlets (except for group holding cells equipped with TV in a security enclosure where the outlet will not be exposed to the detainee).
- (b) For cleaning and other activities, cords can be run in from the corridors.

4. Lighting Protection/Surge Protection

- (a) All communication, video, and data equipment shall be protected against surges induced on all control, communication, video, sensor and data cables.
- (b) All cables and conductors that serve as control, audio, video, sensor or data conductors that leave the building (including devices mounted on building exterior) shall have surge protection circuits. Fuses shall not be used for surge protection.
- (c) All systems and components shall be equipped with lightning protection devices. Lightning protection system shall be designed to meet the requirements of [NFPA 780](#).

5. Community Antenna Television (CATV) System

- (a) A complete CATV system shall be provided, which will include all devices, cable, splitters, line taps, equipment, and conduit from each CATV outlet to the location of the CATV interior backboard with extension of conduit to location of satellite dish. CATV system shall be star typology with each outlet connected to head-end equipment with the drop cable. System shall provide high quality TV signals to all outlets with a return path for interactive television and cable modem access. Downstream bandwidth shall be 50 – 750 MHz minimum. Upstream bandwidth shall be 5 – 40 MHz minimum.
- (b) Each termination for a TV receiver must have a minimum signal level of 0 decibel millivolts (dBmV) (1000 microvolt) at 55 MHz and 0 dBmV (100

microvolt) at 750 MHz and a maximum signal of 15 dBmV or a level not to overload the receiver for the entire system bandwidth.

6. Additional Electrical Items

- (a) Provide electric power for door locks, where required by design, by extending a conduit from the control room through the hold room ceiling, extending to a point above the door. Locks must be on battery backup emergency power and emergency generator power.
- (b) Provide panic buttons in hold rooms with a disable high-security key or switch from outside the hold rooms. The button should be a large mushroom design.

VIII. ELECTRONIC SECURITY

A. General Requirements

- 1. The electronic security system shall be a completely integrated system which coordinates with gate operators, electric locks and other detention hardware, detention equipment, fire alarms, and provides electronic door controls, video touch screen controls, intercom and paging, video surveillance/CCTV, staff duress system, and perimeter alarm system.
- 2. Due to the critical nature of these facilities, contractors who perform the electronic security work must be pre-qualified to meet requirements such as:
 - (a) Relevant experience in similar projects
 - (b) Company financial soundness
 - (c) Payment and performance bondable
 - (d) Relevant experience of assigned key personnel
- 3. Security electronic equipment must be coordinated with detention equipment, including but not limited to: security fasteners, security access panels, electric locks.
- 4. Prior to final acceptance of the systems, the electronic security contractor shall provide evidence of system tests, complete documentation manuals, and shall conduct training in the use of the systems.

- B. CCTV: Fixed CCTV camera with motion detection capability, detention grade housing and wide-angle lens. Connect to monitor at secondary waiting / processing counter or in secondary supervisor's office (if included) or other CBP designated

[RETURN TO TOP](#)

location. Position the camera to observe activity in room, but not degrade privacy afforded by toilet area modesty screen. Do not mount over fixtures in room.

- C. Duress System: Provide detention grade duress alarm button interior side adjacent to entry door with keyed reset / disable control outside of room. Connect to CCC (CBP Coordination Center) and / or other CBP designated locations as required.
- D. Access Control: See [Section II.B.3, Doors and Frames](#) for access requirements.
- E. For large detention facilities, refer to the Technical Specifications, Section 13800 of the U.S. Immigration and Customs Enforcement Processing Center Detention Construction Standards, dated 01 November 2004.
- F. The following Legacy Documents were used to develop this Appendix:
 - 1. INS Hold Room Construction Standards 1999
 - 2. U.S. Customs and Border Protection Airport Technical Design Standards 2006
 - 3. U.S. Immigration and Customs Enforcement Service Processing Center Detention Construction Standards (SPC-Detention Construction Stds. 2004)





APPENDIX 8.12: CLOSED CIRCUIT TELEVISION (CCTV)

I. GENERAL

A. The CCTV system is a core subsystem of an overall Electronic Security System (ESS). It is the collection of cameras, recorders, switches, keyboards, and monitors that allow viewing and recording of security events. The CCTV system is normally integrated into the overall ESS and centrally monitored at the Dispatch Center. Uses of CCTV systems for security services include several different functions as described below.

1. Surveillance

(a) CCTV cameras can be used to give a viewer the capability to be made aware of or view visual events at multiple locations from a centralized remote viewing area. CCTV camera technology makes visual information available that would normally only be available through multiple (possibly roving) human resources.

2. Assessment

(a) When alerted by an alarm notification, CCTV cameras allow Dispatch Center operators or other viewers to assess the situation and make a determination as to what type of response may or may not be required. An example would be an intrusion alarm at a remote facility. Visual assessment and other confirmation may indicate an unannounced maintenance crew at work. Symptoms of intrusion would lead to a response.

3. Deterrence

(a) While more effective against unsophisticated burglars as opposed to trained covert agents, CCTV cameras may deter burglary, vandalism, or intrusion due to fear of discovery and prosecution.

4. Evidentiary Archives

5. Retrieval of archived images may be helpful in identification or prosecution of trespassers, vandals, or other intruders.

6. Facial Recognition

(a) Cameras can be used for biometric facial recognition as discussed in [Chapter 11](#).

7. Intrusion Detection

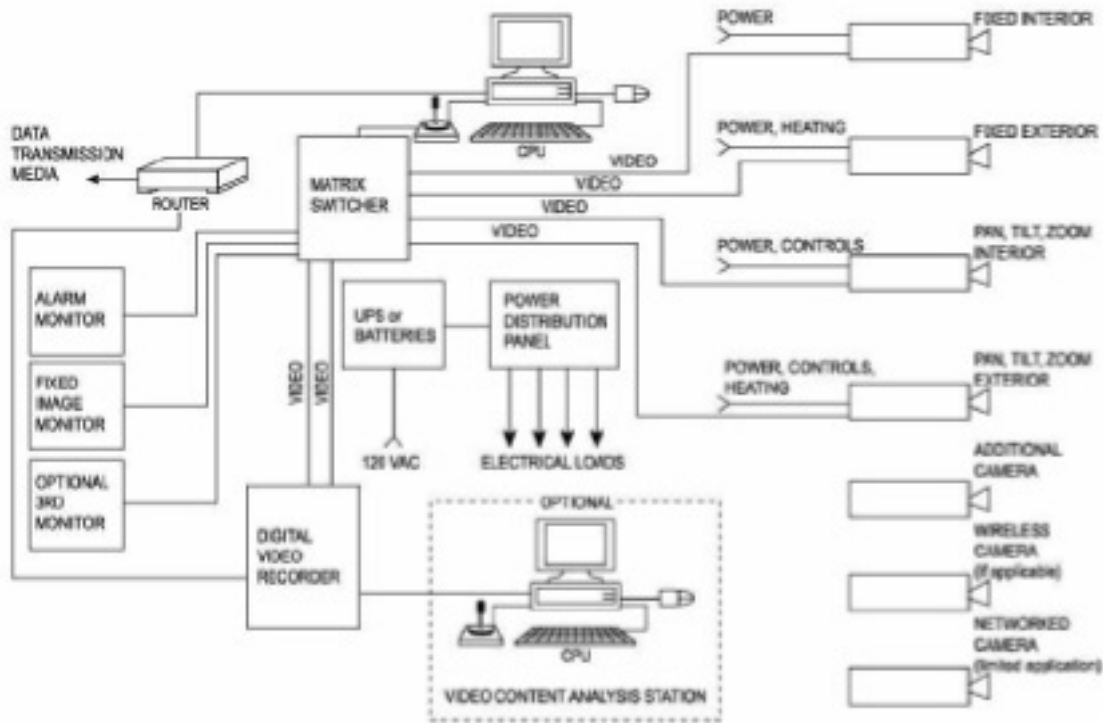
(a) CCTV cameras when employed with video content analysis or motion path analysis software and equipment are increasingly being used as a means

[RETURN TO TOP](#)

for intrusion detection as discussed in [Chapter 11, Access to Facilities](#).



Figure 1: CCTV System



II. SYSTEM OVERALL REQUIREMENTS

A. Requirements

- Major components of the CCTV system must be capable of full color transmission, although day/night cameras are commonly utilized in areas requiring light sensitivity. Pan, tilt, zoom (PTZ) cameras are to be utilized to supplement fixed cameras, permitting more accurate coverage in critical areas. All camera views associated with an alarm must be automatically recorded. A color monitor and high resolution DVR with a minimum 30 day recording capability must be employed to store video footage; the DVR shall also be capable of playing back any camera view. Cameras in hold rooms and interview rooms will have detention-grade housings and, to deter tampering, cannot be mounted over fixtures in the rooms. CCTV cameras will not be installed in search rooms. Questions or concerns about the adequacy of an existing or proposed CCTV system or component should be addressed to CBP/IA/SMD at cbp_security@dhs.gov.
- The system, including all components and appurtenances, shall be configured and installed to yield a mean-time-between-failure (MTBF) of at least 10,000 hours, and shall be calculated based on the configuration specified in the section

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

titled "[Overall System Reliability Calculations.](#)"

B. Power Line Surge Protection

1. Requirements

- (a) All equipment connected to AC power shall be protected from surges. Equipment protection shall withstand surge test waveforms described in IEEE C62.41.1 and IEEE C62.41.2. Fuses shall not be used for surge protection.

C. Video Line Surge Protection

1. Requirements

- (a) All cable, except fiber optic cable, used for sync or video signal transmission shall include protective devices to safeguard the CCTV equipment against surges. The surge suppression device shall not attenuate or reduce the video or sync signal under normal conditions. The surge suppression device shall be capable of dissipating not less than 1500 watts for 1 millisecond, and the response time from zero volts to clamping shall not be greater than 5 nanoseconds. Fuses shall not be used for surge protection.

D. Control Line Surge Protection

1. Requirements

- (a) All cables and conductors, except fiber optic cables, which serve as communication, control, or signal lines shall be protected against surges and shall have surge protection installed at each end. Protection shall be furnished at the equipment and additional triple electrode gas surge protectors rated for the application on each wire line circuit shall be installed within 1 m 3 feet of the building cable entrance. Fuses shall not be used for surge protection.

E. Power Line Conditioners

1. Requirements

- (a) A power line conditioner shall be furnished for the security console CCTV equipment. The power line conditioner used for the CCTV equipment shall be the same one as provided for Intrusion Detection System (IDS) ESS. The power line conditioner shall be of the ferro-resonant design,

with no moving parts and no tap switching, while electrically isolating the secondary from the power line side. The power line conditioner shall be sized for no less than 125 percent of the actual connected kVA load. Characteristics of the power line conditioner shall be as follows:

- At 85-percent load, the output voltage shall not deviate by more than plus or minus 1 percent of nominal when the input voltage fluctuates between minus 20 percent to plus 10 percent of nominal;
- During load changes of zero to full load, the output voltage shall not deviate by more than plus or minus 3 percent of nominal. Full correction of load switching disturbances shall be accomplished within 5 cycles, and 95 percent correction shall be accomplished within 2 cycles of the onset of the disturbance.

F. Environmental Conditions

1. Field Equipment

- (a) The cameras and all other field equipment shall be rated for continuous operation under ambient environmental conditions of minus 10.0 to 55 degrees C 14 to 120 degrees F using no auxiliary heating or cooling equipment. Equipment shall be rated for continuous operation under the ambient environmental temperature, humidity, wind loading, ice loading, and vibration conditions specified or encountered for the installed location.

2. Security Center Equipment

- (a) The Security Center and remote control/monitoring station equipment shall, unless designated otherwise, be rated for continuous operation under ambient environmental conditions of 15.6 to 29.4 degrees C 60 to 85 degrees F and a relative humidity of 20 to 80 percent.

3. Hazardous Environment

- (a) All system components located in areas designated "Hazardous Environment," where fire or explosion hazards may exist because of flammable gases or vapors, flammable liquids, combustible dust, or ignitable fibers or flyings, shall be rated Class II, Division I, Group F, and installed according to Chapter 5 of the NFPA 70 .

4. Electrical Requirements

- (a) Electrically powered IDS equipment shall operate on 120- or 240-volt [60] [50] Hz AC sources as shown. Equipment shall be able to tolerate

variations in the voltage source of plus or minus 10 percent, and variations in the line frequency of plus or minus 2 percent with no degradation of performance.

5. Uninterruptible Power Supply (UPS)

- (a) All electrical and electronic equipment in the console shall be powered from an UPS provided as specified in Section 26 32 33.00 10 Uninterruptible Power Supply (Ups) System Above 15 Kva Capacity. The UPS shall be sized to provide at least 6 hours battery back-up in the event of primary failure. Batteries will be of the sealed non-gassing type.

NOTE: All Security equipment will connect to the emergency backup generator.

See [UFGS 26 32 33.00 10](#) (October 2007)

III. TECHNICAL DATA PACKAGE (SYSTEM DOCUMENTATION)

- A. The contractor shall supply a CCTV system data package. The data package shall include the following:
 - B. Manufacturers' Data
 - 1. The data package shall include manufacturers' data for all materials and equipment and security center equipment provided.
 - C. System Description and Analyses
 - 1. The data package shall include complete system descriptions, analyses and calculations used in sizing the equipment required. Descriptions and calculations shall show how the equipment will operate as a system to meet the performance. The data package shall include the following:
 - (a) Switcher matrix size;
 - (b) Camera call-up response time;
 - (c) System start up and shutdown operations;
 - (d) Switcher programming instructions;
 - (e) Switcher operating and maintenance instructions;
 - (f) Manuals for CCTV equipment; and
 - (g) Data entry forms.
 - D. Software Data

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- (a) The data package shall consist of descriptions of the operation and capability of system and application software as specified.

E. Overall System Reliability Calculations

1. The data package shall include all manufacturer's reliability data and calculations required to show compliance with the specified reliability. The calculations shall be based on all CCTV equipment associated with one camera circuit and the console CCTV equipment, excluding the data transmission media (DTM).

F. Certifications

1. All specified manufacturer's certifications shall be included with the data package. This includes the IT Certification and Accreditations (C&A) via DHS 4300-A and B).

G. Site Conditions

1. The project security consultant shall verify that site conditions are in agreement with the design package. The CBP project manager shall submit redline drawings/report to the project security consultants documenting changes to the site, or conditions that affect performance of the system to be installed. For those changes or conditions which affect system installation or performance, provide (with the report) specification sheets, or written functional requirements to support the findings, and a cost estimate to correct the deficiency.

H. Operation and Maintenance Manuals

1. A draft copy of the operation and maintenance manuals shall be delivered to the Government prior to beginning the performance verification test for use during site testing.

I. Data Entry

1. The contractor shall enter all data needed to make the system operational;
2. The contractor shall deliver the data to the Government on data entry forms, utilizing data from the contract documents, Contractor's field surveys, and all other pertinent information in the contractor's possession required for complete installation of the data base. The contractor shall identify and request from the Government, any additional data needed to provide a complete and operational CCTV system. The completed forms shall be delivered to the Government for review and approval at least 90 days prior to the contractor's scheduled need date.

J. Graphics

The contractor shall create and install all required graphics needed to make the system operational. Graphics shall have sufficient level of detail for the system operator to assess the alarm. The contractor shall supply hard copy, color examples at least 8-by-10 inches in size, of each type of graphic to be used for the completed CCTV system. If the video switcher does not use a monitor for display of system information, the contractor shall provide examples of the video annotation used for camera identification. The graphics examples shall be delivered to the Government for review and approval at least 90 days prior to the contractor's scheduled need date.

K. Technical Data Package

1. Final copies of each of the manufacturer's commercial manuals arranged as specified bound in hardback, loose-leaf binders and as electronic data, shall be delivered to the Government within 30 days after completing the endurance test. The draft copy used during site testing shall be updated prior to final delivery of the manuals. Each manual's contents shall be identified on the cover. The manual shall include names, addresses, and telephone numbers of each subcontractor installing equipment and systems, and nearest service representatives for each item of equipment for each system. The manuals shall have a table of contents and tab sheets. Tab sheets shall be placed at the beginning of each chapter or section and at the beginning of each appendix. The final copies delivered after completion of the endurance test shall include all modifications made during installation, checkout, and acceptance. The number of copies of each manual to be delivered shall be as specified in writing.

L. Functional Design Manual

1. The functional design manual shall identify the operational requirements for the system and explain the theory of operation, design philosophy, and specific functions. A description of hardware and software functions, interfaces, and requirements shall be included for all system operating modes.

M. Hardware Manual

1. The manual shall describe all equipment furnished, including:
 - (a) General hardware description and specifications;
 - (b) Installation and checkout procedures;
 - (c) Equipment electrical schematics and layout drawings;
 - (d) System schematics and wiring lists;
 - (e) System setup procedures;
 - (f) Manufacturer's repair parts list indicating sources of supply; and

(g) Interface definition.

N. Software Manual

1. The software manual shall describe the functions of all software, and shall include all other information necessary to enable proper loading, testing and operation, including:

- (a) Definitions of terms and functions;
- (b) Procedures for system boot-up;
- (c) Description of using the programs;
- (d) Description of required operational sequences;
- (e) Directory of all disk files; and
- (f) Description of all communications protocols, including data formats, command characters, and a sample of each type of data transfer.

2. Operator's Manual

- (a) The operator's manual shall explain all procedures and instructions for operation of the system including:
 - (b) Video switcher;
 - (c) Video multiplexer;
 - (d) Cameras and video recording equipment;
 - (e) Use of the software;
 - (f) Operator commands;
 - (g) System start-up and shut-down procedures; and
 - (h) Recovery and restart procedures.

O. Maintenance Manual

1. The maintenance manual shall describe maintenance for all equipment including inspection, periodic preventive maintenance, fault diagnosis, and repair or replacement of defective components.

P. As-Built Drawings

1. The contractor shall maintain a separate set of drawings, elementary diagrams, and wiring diagrams of the CCTV system to be used for as-built drawings. This set shall be accurately updated by the contractor with all changes and additions to the CCTV system and shall be delivered to the Government with the final endurance test report. In addition to being complete and accurate, this set of drawings shall be kept neat and shall not be used for installation purposes. Upon completion of the final system drawings, the project security consultants will review the final system work with the contractor. If the final system work is not complete, the contractor will be so advised and shall complete the work as required. Final drawings submitted with the endurance test report shall be finished drawings on Mylar or vellum, and created using AutoCAD.

IV. TESTING AND TRAINING

A. Group IV Technical Data Package ---Systems Acceptance Test (SAT)

1. The contractor shall perform pre-delivery testing, site testing, and adjustment of the completed CCTV system. The contractor shall provide all personnel, equipment, instrumentation, and supplies necessary to perform all testing.
 - (a) Written notification of planned testing shall be given to the project security consultants at least 14 days prior to the test and in no case shall notice be given until after the contractor has received written approval of the specific test procedures.
2. Test Procedures and Reports
 - (a) Test procedures shall explain, in detail, step-by-step actions and expected results demonstrating compliance with the requirements. Test reports shall be used to document results of the tests. Reports shall be delivered to the Government within 7 days after completion of each test.

B. Training

1. The contractor will conduct training courses for designated personnel in the maintenance and operation of the procured CCTV system as specified in the procurement contract and in the “owners” manual.
 - (a) The training will be oriented to the specific system procured and installed under the contract;
 - (b) Training manuals will be delivered for each trainee, along with three additional manuals delivered: two (2) manuals for archiving at the project site and one (1) manual for the procurement office;
 - (c) The manuals shall include:

- Class agenda;
 - Class objectives defined for each lesson; and
 - Detailed description of the subject matter for each lesson.
2. The contractor is responsible for:
- (a) Furnishing all audio-visual equipment;
 - (b) All other training materials and supplies.
 - (c) Where the contractor presents portions of the course through the use of audio-visual material, copies of the audio-visual materials will be delivered to the Government, either as a part of the printed training manuals or on the same media as that used during the training sessions.
3. A training day will:
- (a) Take place Monday through Friday;
 - (b) Occur during normal operational hours;
 - (c) Not exceed an 8-hour duty day; and
 - (d) Incorporate breaks and lunch period.
4. Approval for the training content and class scheduled will be obtained from the Government by the vendor no less than 30 days prior to the training.

C. Operator Training

1. Course training:
- (a) The course shall be taught at the project site for five consecutive training days during or after the contractor's field testing and government acceptance of the system;
 - (b) A minimum of 3 personnel will attend the course;
 - (c) No part of the training given during this course will be counted toward completion of the performance verification test;
 - (d) The course shall consist of:
 - Classroom instruction;
 - Hands-on training;

- Instruction on the specific hardware configuration of the installed system; and
 - Specific instructions for operating the installed system.
2. The course shall demonstrate:
- (a) System start-up;
 - (b) System operation;
 - (c) System shutdown;
 - (d) System recovery after a failure;
 - (e) Specific hardware configuration; and
 - (f) Operation of the system and its software.
3. The contractor will:
- (a) Prepare and insert additional training material in the training manuals when the need for additional material becomes apparent during instruction;
 - (b) Prepare a written report after the completion of the course;
 - (c) List in the report the times, dates, attendees and material covered at each training session;
 - (d) Describe the skill level of each student at the end of this course; and
 - (e) Submit the report before the end of the performance verification test.
4. The course shall include:
- (a) General CCTV hardware, installed system architecture and configuration;
 - (b) Functional operation of the installed system and software;
 - (c) Operator commands;
 - (d) Alarm interfaces;
 - (e) Alarm reporting;
 - (f) Fault diagnostics and correction;

- (g) General system maintenance; and
- (h) Replacement of failed components and integration of replacement; components into the operating CCTV system.

D. Training Documentation

- 1. Lesson plans and training manuals for the training phases shall be delivered for approval. These will include type of training to be provided, along with a sample training report and a list of reference material.

V. MAINTENANCE AND SERVICE

A. General Requirements

- 1. The contractor will provide all services required and equipment necessary to maintain the entire CCTV system in an operational state as specified for a period of 1 year after the manufacturer's factory warranty period, and shall provide all necessary material required for the work. Impacts on facility operations shall be minimized when performing scheduled adjustments or other unscheduled work. The vendor will provide a quote for an extended warranty.

B. Description of Work

- 1. The adjustment and repair of the CCTV system includes all computer equipment, software updates, signal transmission equipment, and video equipment. Provide the manufacturer's required adjustments and all other work necessary.

C. Personnel

- 1. Service personnel will be qualified to accomplish all work promptly and satisfactorily. The Government shall be advised in writing of the name of the designated service representative, and of any changes in personnel.

D. Schedule of Work

- 1. The contractor will perform two inspections at 6-month intervals or less;
- 2. This work shall be performed during regular working hours, Monday through Friday, excluding legal holidays;
- 3. During these inspections, the contractor will:
 - (a) Conduct visual checks and operational tests of the CPU, switcher, peripheral equipment, interface panels, recording devices, monitors, video equipment electrical and mechanical controls, and a check of the picture quality from each camera;

(b) Run system software and correct all diagnosed problems; and

(c) Resolve any previous outstanding problems.

E. Emergency Service

1. The Government will initiate service calls when the CCTV system is not functioning properly. Qualified personnel shall be available to provide service to the complete CCTV system. The Government shall be furnished with a telephone number where the service supervisor can be reached at all times. Service personnel shall be at the site within 24 hours after receiving a request for service. The CCTV system shall be restored to proper operating condition within 3 calendar days after receiving a request for service.

F. Operation

1. Performance of scheduled adjustments and repair shall verify operation of the CCTV system as demonstrated by the applicable portions of the performance verification test.

G. Records and Logs

1. The contractor will keep records and logs of each task, and shall organize cumulative records for each major component and for the complete system chronologically. A continuous log will be maintained for all devices.
2. The log shall contain calibration, repair, warranties, serial number, bar code data, installation date, major repair dates, and programming data. Complete logs shall be kept and shall be available for inspection on site, demonstrating that planned and systematic adjustments and repairs have been accomplished for the CCTV system.

3. Work Requests

- (a) The contractor shall separately record each service call request, as received. The form shall include the serial number identifying the component involved, its location, date and time the call was received, nature of trouble, names of the service personnel assigned to the task, instructions describing what has to be done, the amount and nature of the materials to be used, the time and date work started, and the time and date of completion. The contractor shall deliver a record of the work performed within 5 days after work is completed.

H. System Modifications

1. The contractor shall make any recommendations for system modification in writing to the Government. No system modifications, including operating

[RETURN TO TOP](#)

parameters and control settings, shall be made without prior approval of the Government. Any modifications made to the systems shall be incorporated into the operations and maintenance manuals, and other documentation affected.

2. Software

(a) The contractor will recommend all software updates, including middleware if needed to allow multiple processes running on one or more machines to interact across a network, to the Government for approval. Upon approval, updates will be:

- Accomplished in a timely manner;
- Fully coordinated with the CCTV system operators.

3. Operation in the system will be verified and incorporated into the operations and maintenance manuals, and software documentation. There shall be a minimum of one scheduled update near the end of the first year's warranty period, at which time the contractor will install and validate the latest released version of the manufacturer's software.

VI. MATERIALS AND EQUIPMENT

A. All system hardware and software components shall be produced by manufacturers regularly engaged in the production of CCTV equipment. Units of the same type of equipment shall be products of a single manufacturer. All material and equipment shall be new and currently in production. Each major component of equipment shall have the manufacturer's name and address, and the model and serial number in a conspicuous place. Equipment located at the security center or a remote control/monitoring station shall be rack mounted as shown in [Figure 1](#). Both Television and Computing devices shall comply with 47 CFR § 15(B).

B. Soldering

1. All soldering shall be done in accordance with standard industry practices.

C. Enclosures

1. The contractor shall provide metallic enclosures as needed for equipment not housed in racks or supplied with a housing. The enclosures shall be as specified or shown.

D. Interior

1. Enclosures to house equipment in an interior environment shall meet the requirements of NEMA 250 Type 12.

E. Exposed-to-Weather

1. Enclosures to house equipment in an outdoor environment shall meet the requirements of NEMA 250 Type 4X.
2. Corrosion-Resistant
3. Enclosures to house equipment in a corrosive environment shall meet the requirements of NEMA 250 Type 4X.
4. Hazardous Environment Equipment
 - (a) All system electronics to be used in a hazardous environment shall be housed in a metallic enclosure which meets the requirements of paragraph "Hazardous Environment."

F. Wiring

- (a) All wiring will be marked in accordance with industry standards and correlate with the wiring diagram.

VII. LOCKS AND KEY-LOCK OPERATED SWITCHES

A. Locks

1. Locks shall be provided on system enclosures for maintenance purposes;
2. Locks shall be Underwriters Laboratory (UL) listed;
3. Locks shall be either a round-key type, with three dual, one mushroom, and three plain pin tumblers; or conventional key type lock having a combination of five cylinder pin and five-point three position side bar; and
4. Keys shall be stamped "U.S. GOVT. DO NOT DUP." The locks shall be so arranged that the key can only be withdrawn when in the locked position. All maintenance locks shall be keyed alike and only two keys shall be furnished for all of these locks.

B. Key-Lock-Operated Switches

1. All key-lock-operated switches required to be installed on system components shall be UL listed, [with three dual, one mushroom, and three plain pin tumblers] [or] [conventional key type lock having a combination of five cylinder pin and five-point three position side bar]. Keys shall be stamped "U.S. GOVT. DO NOT DUP." Key-lock-operated switches shall be two position, with the key removable in either position. All key-lock-operated switches shall be keyed differently and only two keys shall be furnished for each key-lock-operated-switch.

[RETURN TO TOP](#)

C. System Integration

1. When the CCTV system is installed in conjunction with an IDS, the CCTV system shall be interfaced to the IDS and shall provide automatic, alarm-actuated call-up of the camera associated with the alarm zone. Equipment shall be supplied with all adapters, terminators, cables, mainframes, card cages, power supplies, rack mounts, and appurtenances as needed.

VIII. CAMERAS

A. Solid State Cameras

1. High Resolution Day/Night Camera

- (a) The designer should determine if additional lighting is required;
- (b) Lighting ratios of 5:1 or less (highlight to shadow ratio) will ensure shadow detail in the video picture;
- (c) All electronic components and circuits shall be solid state; and
- (d) Signal-to-noise ratio shall not be less than 48 dB unweighted. The camera shall exhibit no geometric distortion. The lens mount shall be a C or CS-mount, and the camera shall have a back focus adjustment. The camera shall operate from minus 20.0 to plus 55 degrees C minus 4 to 131 degrees F without auxiliary heating or cooling, and with no change in picture quality or resolution. The camera shall operate on [60][50] Hz AC power, and shall be capable of operating at a voltage of 105 to 130/205 to 240/12 Volts DC or 24 Volts AC.

2. Solid State Image Array

- (a) The camera shall have a solid state imager, and the picture produced by the camera shall be free of blemishes. The camera shall provide not less than 550 lines of horizontal resolution, and resolution shall not vary over the life of the camera.

3. Sensitivity

- (a) Camera shall provide full video output with the infrared cut-off filter installed, without camera automatic gain, and a scene reflectance of 75 percent using an f/1.2 lens giving a camera faceplate illumination at 2850K of 1.0 lx 0.1 foot candle.

4. Connectors

- (a) Cameras with lenses having auto iris, manual iris, or zoom and focus functions shall be supplied with connectors and wiring as needed for lens operation. Video signal output connector shall be a Bayonet Neill-Concelman (BNC) connector. Cameras with integral fiber optic video transmitters shall have straight-tip bayonet type fiber optic video output connectors. I.P. cameras may utilize fiber or RJ45 connectors.

5. Automatic Circuits

- (a) The camera shall have circuitry to establish a reference black level, and an automatic white clipper and automatic gain control circuits.

B. Interior Dome PTZ Cameras

1. Interior Dome PTZ Camera System

- (a) An interior dome camera system shall be provided with integral camera installed and integrated into the dome housing;
- (b) The camera shall meet the requirements of paragraph VII Cameras as specified; and
- (c) The dome housing shall be nominally 160 mm 6 inches and shall be furnished in a pendant mount or ceiling mount as shown. The lower dome shall be tinted acrylic and shall have a light attenuation factor of not more than 1 f-stop. The housing shall be equipped with integral pan/tilt complete with wiring, wiring harnesses, connectors, receiver/driver, pan/tilt control system, pre-position cards, or any other hardware and equipment as needed to provide a fully functional pan/tilt dome. The pan/tilt shall be permanently lubricated. The motors shall be thermally or impedance protected against overload damage. Pan movement shall be 360 degrees and tilt movement shall not be less than plus and minus 90 degrees. Pan speed shall not be less than 20 degrees per second, and tilt speed shall not be less than 10 degrees per second. There shall not be less than 64 preset positions, with positioning speeds of at least 360 degrees per second in the automatic mode, and not less than 120 degrees per second in the manual positioning mode, with a positioning accuracy of plus or minus 1/2 degree. Each set of preset position data shall include auto focus, auto iris, pan, tilt, and zoom functions. The system shall be able to automatically scan between any two electronically-set limits, and shall be able to operate in the "tour" mode covering up to all presets in a user defined sequence. The dome system shall withstand temperature ranges from minus 10 to 50 degrees C minus 22 to 122 degrees F over a humidity range of 0 to 90 percent, non-condensing. Pan movement shall be 360 degrees and tilt movement shall not be less than plus and minus 90 degrees. Pan speed shall not be less than 20 degrees per second, and

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

tilt speed shall not be less than 10 degrees per second

2. Exterior PTZ Dome Camera System

- (a) An exterior dome camera system shall be provided with integral camera installed and integrated into the dome housing. The camera shall have a minimum horizontal resolution of 425 lines (color) or 500 lines (monochrome);
- (b) The dome housing shall be nominally 160 mm 6 inches and shall be furnished in a NEMA 4 pendant mount, pole mount, ceiling mount, surface mount, or corner mount as shown. The housing shall be constructed to be dust and water tight, and fully operational in 100 percent condensing humidity. The housing shall be equipped with supplementary camera mounting blocks or supports as needed to position the specified camera and lens to maintain the proper optical centerline. All electrical and signal connections required for operation of the camera and lens shall be supplied. The housing shall protect the internal drives, positioners, and camera from the environment encountered for camera operation;
- (c) The lower dome shall be tinted acrylic and shall have a light attenuation factor of not more than 1 f-stop. An integral heater, sized to maintain the lower dome above the dew point, shall be part of the camera system. The housing shall be equipped with integral pan/tilt complete with wiring, wiring harnesses, connectors, receiver/driver, pan/tilt control system, pre-position cards, or any other hardware and equipment as needed to provide a fully functional pan/tilt dome. The pan/tilt shall be permanently lubricated. The motors shall be thermally or impedance protected against overload damage; and
- (d) Pan movement shall be 360 degrees and tilt movement shall not be less than plus and minus 90 degrees. Pan speed shall not be less than 20 degrees per second, and tilt speed shall not be less than 10 degrees per second. There shall not be less than 99 preset positions, with positioning speeds of at least 360 degrees per second in the automatic mode, and not less than 120 degrees pre second in the manual positioning mode, with a positioning accuracy of plus or minus 1/2 degree. Each set of preset position data shall include auto focus, auto iris, pan, tilt, and zoom functions. The system shall be able to automatically scan between any two electronically-set limits, and shall be able to operate in the "tour" mode covering up to all presets in a user defined sequence. The dome system shall withstand temperature ranges from minus 40 to 50 degrees C minus 40 to 122 degrees F over a humidity range of 0 to 90 percent, non-condensing. When designing CCTV surveillance, consideration needs to be given to lost coverage within the camera sweep field-of-view when the

camera zooms to a fixed location. Refer to [Figure 2](#) below.

C. Camera Lenses

1. Camera lenses shall be all glass with coated optics. The lens mount shall be a C or CS mount, compatible with the cameras selected. The lens shall be supplied with the camera, and shall have a maximum f-stop opening of f/1.2 or the maximum available for the focal length specified. The lens shall be equipped with an auto-iris mechanism unless otherwise specified. Lenses having auto iris, manual iris, or zoom and focus functions shall be supplied with connectors, wiring, receiver/drivers, and controls as needed to operate the lens functions. Lenses shall have sufficient circle of illumination to cover the image sensor evenly. Lenses shall not be used on a camera with an image format larger than the lens is designed to cover. Lens focal lengths shall be as shown or specified in the manufacturer's lens selection tables.

D. Camera Housings And Mounts

1. The camera and lens shall be enclosed in a tamper resistant housing as specified below. Any ancillary housing mounting hardware needed to install the housing at the camera location shall be provided as part of the housing. The camera and lens contained in a camera housing shall be installed on a camera support as shown. Any ancillary mounting hardware needed to install the support and to install the camera on the support shall be provided as part of the support. The camera support shall be capable of supporting the equipment to be mounted on it including wind and ice loading normally encountered at the site.

E. Environmentally Sealed Camera Housing

1. The housing shall be designed to provide a condensation-free environment for camera operation. The housing shall be constructed to be dust and water tight, and fully operational in 100 percent condensing humidity. The housing shall be purged of atmospheric air and pressurized with dry nitrogen, shall be equipped with a fill valve, overpressure valve, and shall have a humidity indicator visible from the exterior. Housing shall not have a leak rate greater than 13.8 kPa 2 psi at sea level within a 90 day period. The housing shall be equipped with supplementary camera mounting blocks or supports as needed to position the specified camera and lens to maintain the proper optical centerline. All electrical and signal connections required for operation of the camera and lens shall be supplied. The housing shall provide the environment needed for camera operation, and shall keep the viewing window free of fog, snow, and ice;
2. The housing shall be equipped with a sunshield, and both the housing and the sunshield shall be white. A mounting bracket which can be adjusted to center

the weight of the housing and camera assembly shall be provided as part of the housing.

F. Indoor Camera Housing

1. The housing shall be designed to provide a tamper resistant enclosure for indoor camera operation. The housing shall be equipped with tamper proof latches, and shall be supplied with the proper mounting brackets for the specified camera and lens. The housing and appurtenances shall be a color that does not conflict with the building interior color scheme.

G. Interior Mount

1. The camera mount shall be suitable for either wall or ceiling mounting and shall have an adjustable head for mounting the camera. The wall mount and head shall be constructed of aluminum or steel with a corrosion-resistant finish. The head shall be adjustable for 360 degrees of pan, and not less than 90 degrees of tilt.

H. Low Profile Ceiling Mount

1. A tamperproof ceiling housing shall be provided for the camera. The housing shall be low profile and shall be suitable for replacement of 610 by 610 mm, 2 by 2 foot ceiling tiles. The housing shall be equipped with a camera mounting bracket and shall allow a 360-degree viewing setup.

I. Interior Dome Housing

1. An interior dome housing shall be provided for each camera as shown. The dome housing shall be a pendant mount, pole mount, ceiling mount, surface mount, or corner mount as shown. The lower dome shall be black opaque acrylic and shall have a light attenuation factor of not more than 1 f-stop. The housing shall be equipped fixed or integral pan/tilt complete with wiring, wiring harnesses, connectors, receiver/driver, pan/tilt control system, pre-position cards, or any other hardware and equipment as needed to provide a fully functional pan/tilt dome. The pan/tilt shall be permanently lubricated. The motors shall be thermally or impedance protected against overload damage. Pan movement shall be 360 degrees and tilt movement shall not be less than plus and minus 90 degrees. Pan speed shall not be less than 20 degrees per second, and tilt speed shall not be less than 10 degrees per second.

J. Exterior Dome Housing

1. An exterior dome housing shall be provided for each camera as shown. The dome housing shall be a pendant mount, pole mount, ceiling mount, surface mount, or corner mount as shown. The housing shall be constructed to be

dust- and water-tight, and fully operational in 100 percent condensing humidity. The housing shall be equipped with supplementary camera mounting blocks or supports as needed to position the specified camera and lens to maintain the proper optical centerline. All electrical and signal connections required for operation of the camera and lens shall be supplied. The housing shall provide the environment needed for camera operation. The lower dome shall be black opaque acrylic and shall have a light attenuation factor of not more than 1 f-stop. The housing shall be equipped with fixed or integral pan/tilt complete with wiring, wiring harnesses, connectors, receiver/driver, pan/tilt control system, pre-position cards, or any other hardware and equipment as needed to provide a fully functional pan/tilt dome. The pan/tilt shall be permanently lubricated. The motors shall be thermally or impedance protected against overload damage. Pan movement shall be 360 degrees and tilt movement shall not be less than plus and minus 90 degrees. Pan speed shall not be less than 20 degrees per second, and tilt speed shall not be less than 10 degrees per second.

K. Exterior Wall Mount

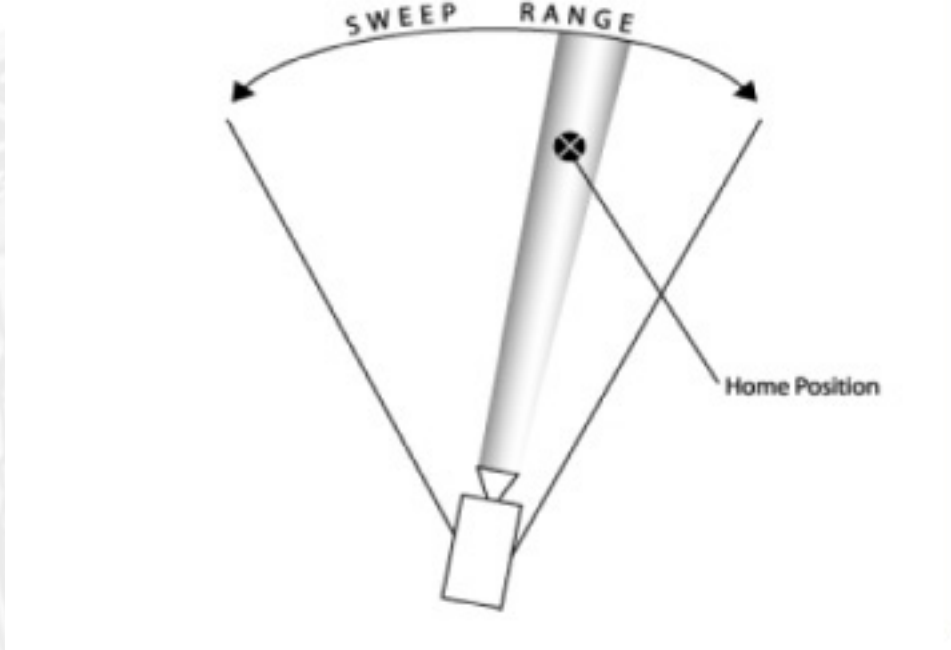
1. There are lengths most commonly used for wall mounts. The exterior camera wall mount will be in the range of 16, 24 or 36 inches long, and shall have an adjustable head for mounting the camera. If another length is required, the person responsible for the installation should review catalogs of CCTV equipment manufacturers to find a mount in current production that will fulfill the requirement. The wall mount and head shall be constructed of aluminum, stainless steel, or steel with a corrosion-resistant finish. The head shall be adjustable for not less than plus and minus 90 degrees of pan, and not less than plus and minus 45 degrees of tilt. If the bracket is to be used in conjunction with a pan/tilt, the bracket shall be supplied without the adjustable mounting head, and shall have a bolt-hole pattern to match the pan/tilt base.

L. Pan/Tilt Mount “non dome system” or “PTZ base mount system”

1. The pan/tilt mount shall be capable of supporting the camera, lens and housing specified. If the pan/tilt is to be mounted outdoors, the pan/tilt shall be weatherproof, and sized to accommodate the camera, lens and housing weight plus maximum wind loading encountered at the installation site. Pan/tilt shall be permanently lubricated. The motors shall be thermally or impedance protected against overload damage. Pan movement shall not be less than 0 to 350 degrees; tilt movement shall not be less than plus and minus 90 degrees. Pan speed shall not be less than 6 degrees per second, and tilt speed shall not be less than 3 degrees per second. The pan/tilt shall be supplied complete with wiring, wiring harnesses, connectors, receiver/driver, pan/tilt control system, pre-position cards, or any other hardware and equipment as needed to provide a fully functional pan/tilt mount to fulfill the site design requirements. Pan movement shall be 360 degrees and tilt movement shall not be less than plus and minus 90

degrees. Pan speed shall not be less than 20 degrees per second, and tilt speed shall not be less than 10 degrees per second.

Figure 2: Fixed-camera field-of-view

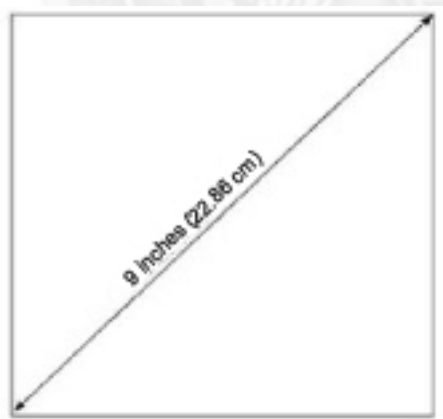


M. Explosion-Proof Housing

1. The explosion-proof housing shall meet the requirements of NEMA 4 for hazardous locations. The housing shall be designed to provide a tamper resistant enclosure and shall be equipped with tamper proof latches. It shall be supplied with the proper mounting brackets for the specified camera and lens.

IX. VIDEO MONITOR

Figure 3: Dimensions of a 9-inch ESS Display



A. Color Video Monitor

1. All electronic components and circuits shall be solid state except for the picture tube. The monitor shall have a stabilized high voltage power supply, and regulated low voltage power supplies. The monitor shall have automatic frequency control (AFC) and horizontal resolution not less than 420 lines at the center of the picture tube. The number of lines in the video produced by the security camera is a measure of picture resolution (sharpness). The larger the number of lines, the better the resolution and hence, overall picture quality. Over 380 Lines is generally considered good resolution while over 700 lines is considered high resolution. The video input shall allow switchable loop-through or 75 ohm termination. The monitor shall have circuitry for automatic degaussing. The monitor shall operate on 50/60 Hz, and shall be capable of operating at a voltage of 105 to 130, 205 to 240 AC Volts;
2. LCD monitor minimums: 1280×720 (720 lines or greater).

B. Controls

1. Front panel controls shall be provided for power on/off, horizontal hold, vertical hold, contrast, and brightness. The monitor shall have switchable DC restoration.

C. Connectors for Video Monitor

1. Video signal input and output shall be by BNC connectors.

D. Video Switcher/Controller

1. The switcher shall conform to CEA 170 specifications, and shall be a vertical interval switcher. Electronic components, subassemblies, and circuits of the switcher shall be solid state. The switcher shall be microprocessor based and software programmable. The switcher shall be a modular system that shall allow for expansion or modification of inputs, outputs, alarm interfaces, and secondary control stations by addition of the appropriate modules. Switcher components shall operate on 120V or 230V, 50/60 Hz. The switcher central processor unit shall be capable of being interfaced to a master security computer for integrated operation and control. The video switcher central processing unit (CPU) shall have the capability of accepting time from a master clock supplied in ASCII format through a TIA-232-F input. All components, modules, cables, power supplies, software, and other items needed for a complete and operable CCTV switching system shall be provided. Switcher equipment shall be rack mounted unless otherwise specified.

E. Switcher Software

1. The switcher shall be software programmable, and the software shall be supplied as part of the switcher. The software shall be installed in the switcher CPU, and shall be configured as required by the site design. Changes or alterations of features under software control shall be accomplished through software programming without changes in hardware or system configuration. The switcher shall retain the current program for at least 6 hours in the event of power loss, and shall not require reprogramming in order to restart the system.

F. Alarm Interface Unit

1. An alarm interface shall be furnished with the switcher. The interface shall be compatible with the [ESS alarm annunciation system](#). The alarm interface shall monitor alarm closures for processing by the switcher CPU or video server. Alarm Inputs may be configured for supervised or unsupervised mode. See [Figure 3](#) for an example of an ESS display dimensions;
2. Alarm inputs to the alarm interface shall be relay contact or through other interface. The alarm interface shall be modular and shall allow for system expansion. The alarm interface to be installed at the site shall be configured to handle 64 alarm points, and shall have an expansion capability of not less than 25 percent. An output shall be provided to actuate a video recorder.

G. Switcher or Video Server Response Time and Alarm Processing

1. The switcher response time shall not be greater than 200 milliseconds from the time the alarm is sensed at the switcher alarm interface, until the picture is displayed on the monitor. The switcher shall continue to process subsequent alarms and shall display or place them in a queue. The operator shall be able to view the alarms in queue by operating an alarm release function which switches the subsequent alarms to the monitor in the order of occurrence.

H. Control Keyboards or Video Monitoring Stations

1. Control and programming keyboards shall be supplied for the video switcher or video server at the security station, and control keyboards shall be supplied for any control/monitoring stations as shown. The control keyboard shall provide the interface between the operator and the CCTV system, and shall relay commands from the operator to the switcher CPU. The keyboard shall provide control of the video switcher functions needed for operation and programming of the video switcher. Controls shall include, but not be limited to: programming the switcher, switcher control, lens function control, pan/tilt/zoom (PTZ) control, control of environmental housing accessories, and annotation programming. If the switcher CPU requires an additional text keyboard for system management functions, the keyboard shall be supplied as part of the video switcher.

I. Accessory Control Equipment

1. The video switcher shall be equipped with signal distribution units, preposition cards, expansion units, cables, software or any other equipment needed to ensure that the CCTV system is complete and fully operational;
2. Connectors for Video Switcher or Video Server
 - (a) Video signal input and output shall be by BNC connectors, fiber connectors, or RJ45 connectors.

J. Video Annotation

1. Video annotation equipment shall be provided for the video switcher. The annotation shall be alphanumeric and programmable for each video source. Annotation to be generated shall include, but not be limited to: individual video source identification number, time (hour, minute, second) in a 24-hour format, date (month, day, year), and a unique, user-defined title with at least 8 characters. The annotation shall be inserted onto the source video so that both shall appear on a monitor or recording. The lines of annotation shall be movable for horizontal and vertical placement on the video picture. The annotation shall be automatically adjusted for date. Programmed annotation information shall be retained in memory for at least 4 hours in the event of power loss.

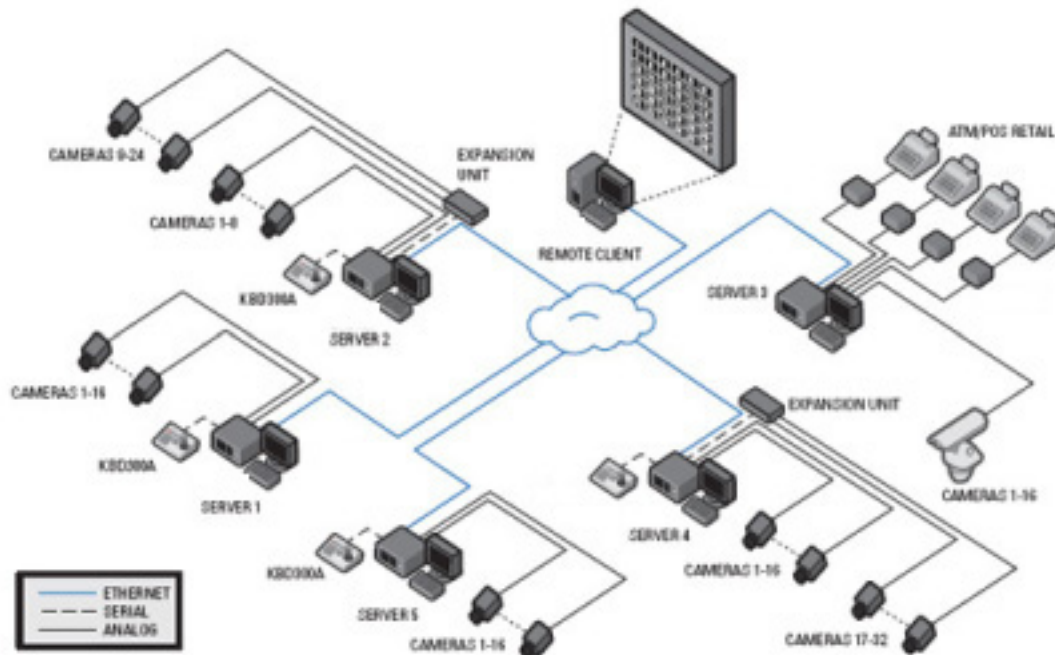
X. DIGITAL VIDEO EQUIPMENT

A. Digital Video Recorder (DVR)

1. A digital video recorder (DVR) is a device that records video in a digital format to a disk drive or other medium. DVR CCTV system provides a multitude of advanced functions over VCR technology including video searches by event, time, date and camera. There is also much more control over quality and frame rate allowing disk space usage to be optimized and the DVR can also be set to overwrite the oldest security footage should the disk become full. In some DVR security systems remote access to security footage using a PC can also be achieved by connecting the DVR to a Local Area Network (LAN) network or the internet;
2. Security DVRs may be categorized as being either PC based or embedded. A PC based DVR's architecture is a classical personal computer with video capture cards designed to capture video images. An embedded type DVR is specifically designed as a digital video recorder with its operating hardware and application software contained in firmware or read only memory. A CCTV system may provide analog or digital video to the DVR. See [Figure 4](#).
 - (a) 16 channels, minimum of 120 ips/fps capture card, to provide no less than 7.5 images per second, per camera;

- (b) Ability to view images directly from the DVR, onto the monitor; if a multiplexer or live display card is needed, it should be included;
- (c) An installed network card in both DVR and Redundant Array of Inexpensive Disks (RAID), to facilitate hook-up to the network;
- (d) Installed server remote software and include remote access software, with unlimited licenses, so it can be viewed in the field via the network;
- (e) Included playback software needed to allow for playback, if not automatically included on the export media when exporting video;
- (f) Rack mount chassis with adequate cooling for both DVR and Raid (locking model with keys if PC based);
- (g) Internal DVD-R/RW and CD-R/RW burner combo drive;
- (h) Enough memory installed to allow for recording, playback, etc. without skipping/delays/errors, etc. due to low memory problems;
- (i) Internal storage with enough capacity to store 2 images per second x 16 cameras x 7 days minimum, with the largest picture size possible, in case of RAID failure;
- (j) External RAID 5 (distributes parity among the drives) storage with enough capacity to store 2 images per second x 16 cameras x 30 days minimum with the largest picture size possible. All hard drives must be rated to withstand continuous use in a RAID environment;
- (k) Include a keyboard, video, mouse (KVM) switch to share the keyboard, monitor, and mouse between the RAID and DVR (if PC based);
- (l) 3-year complete warranty on parts and labor - onsite service included OR advance replacement shipped overnight prior to return of defective unit and a 30 day "no questions asked" return policy.;
- (m)The DVR(s) shall operate on 100-230 VAC \pm 10%, 50/60 Hz. The signal system shall be NTSC/PAL with an adjustable recording resolution from 320x240 to 704x480m; and
- (n) The DVR(s) shall be a high-resolution unit with a minimum of thirty (30) days recording capability of all channels.

Figure 4: DVR CCTV System Combining Serial, Analog and Ethernet/Internet Capabilities



XI. VIDEO SIGNAL EQUIPMENT

A. The following video signal equipment shall conform to CEA 170. Electrically powered equipment shall operate on 120 Volts 60 Hz AC power. All video signal inputs and outputs shall be by BNC connectors.

1. Ground Loop Corrector

(a) The ground loop corrector shall eliminate the measured ground loop interference (common mode voltage) in wire line or coaxial video transmission lines. The ground loop corrector shall pass the full transmitted video bandwidth with no signal attenuation or loss. Clamping ground loop correctors shall be capable of rejecting at least an 8 volt peak-to-peak 60 Hz common mode signal. Ground isolation transformers shall be capable of rejecting at least a 10-volt peak-to-peak 60-Hz common mode signal. Ground isolation amplifiers shall be capable of rejecting at least a 30-volt peak-to-peak 60-Hz common mode signal. Differential ground loop correctors shall be capable of rejecting at least a 100-volt peak-to-peak 60-Hz common mode signal.

2. Video Distribution Amplifier

(a) The video distribution amplifier shall have four independent video outputs from a single video input. The video distribution amplifier shall have solid-state circuitry consisting of four identical video amplifiers in parallel provide four equal 75-ohm loads, which allow the video outputs to be viewed

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

without distortion or loss of clarity. The distribution amplifier shall have not less than plus or minus 3 dB of gain adjustment for the video output. Output isolation shall be 40 dB or greater at 5 MHz. Bandwidth shall be 10 MHz or greater, and frequency response to 8 MHz shall be plus or minus 0.5 dB or less. Hum and noise shall be 55 dB below 1 volt peak-to-peak or better. Operating power will be 120 VAC, 50/60 Hz or 230 VAC. The video distribution amplifier will comply with these certification/ratings: CE, Class B (DA104DT/220), UL Listed (DA104DT), FCC, Class B (DA104DT), Meets NEMA Type 1 standards.

B. Best practices for CCTV Camera Poles

1. Cantilever Camera Pole

- (a) The camera mounting pole shall be a [non-hinged] [hinged] cantilever aluminum pole with [counterweights] [and] mounting base. All fittings shall be stainless steel. The camera mounting plate shall locate the camera 4.6 m (180 inches) 180 inches vertically from the base, and 2.7 m 105 inches horizontally from the centerline of the pole to the centerline of the camera. The camera mount shall be adjustable with a minimum of 40 degrees pan away from the pole and 6 degrees pan toward the pole, and plus and minus 90 degrees of tilt. The pole shall have an internal wiring harness that routes [video,] [video, sync,] and power between the pole base and the camera mount. The wiring harness shall be compatible with the model camera to be mounted on the pole and the video DTM. Surge protection shall be provided at the pole between the wiring harness, and the incoming electronic signal lines and AC power line. The pole shall have a weatherproof, AC power service outlet that is surge protected and has a ground fault interruption device. Separate circuit breakers shall be provided for camera AC power and service outlet AC power.

2. Straight Camera Pole

- (a) The camera mounting pole shall be a non-hinged/hinged straight aluminum pole with [counterweights] [and] mounting base. All fittings shall be stainless steel. The camera mounting plate shall locate the camera 4.6 m 180 inches vertically from the base, and 508.0 mm 20 inches horizontally from the centerline of the pole to the centerline of the camera. The camera mount shall be adjustable with a minimum of 40 degrees pan away from the pole and 6 degrees pan toward the pole, and plus and minus 90 degrees of tilt. The pole shall have an internal wiring harness that routes video and power between the pole base and the camera mount. The wiring harness shall be compatible with the camera to be mounted on the pole and the video DTM. Surge protection shall be provided at the pole between the wiring harness, and

the incoming electronic signal lines and AC power line. The pole shall have a weatherproof, AC power service outlet that is surge protected and has a ground fault interruption device. Separate circuit breakers shall be provided for camera AC power and service outlet AC power.

3. Pan/Tilt Mounting Pole

- (a) The pan/tilt mounting pole shall be a straight steel or aluminum pole. The pole shall be (manufactures specifications) m/feet high and shall have a mounting plate at the top for the pan/tilt. The pole and mounting plate shall have a corrosion-resistant finish. The mounting plate shall have a bolt hole pattern to match the base of the pan/tilt to be mounted on the pole. Under maximum loading, the total pole deflection shall not exceed 0.1 of one degree. A cable conduit shall be provided from the base of the pole to the mounting plate of the pan/tilt. The conduit shall be sized to accommodate all wiring needed for the camera and pan/tilt.

XII. ACCESSORIES

- A. The designer will provide a drawing showing the amount of rack space needed for the rack mounted CCTV equipment, and placement of the equipment in the rack. Coordinate the CCTV equipment rack layout in conjunction with the ESS rack mounted equipment. Standard 482.6 mm 19 inch electronic rack cabinets conforming to CEA-310-E shall be provided for the CCTV system at the security center and remote control/monitoring sites as shown.

XIII. WIRE AND CABLE

- A. All wire and cable components shall be able to withstand the environment the wire or cable is installed in for a minimum of 20 years.
- B. CCTV Equipment Video Signal Wiring
 1. The coaxial cable shall have a characteristic impedance of 75 ohms plus or minus 3 ohms. RG 59/U coaxial signal cable shall have shielding which provides a minimum of 95 percent coverage, a solid copper center conductor of not less than 23 AWG. RG 6/U coaxial cable shall have shielding which provides a minimum of 95 percent coverage, with center conductor of 18 AWG;
 2. Category 6 cable, commonly referred to as Cat 6, is a cable standard for Gigabit Ethernet and other network protocols that is backward compatible with the Category 5/5e and Category 3 cable standards. The cable contains four twisted copper wire pairs, just like earlier copper cable standards. Although Cat-6 is sometimes made with 23 gauge wire, this is not a requirement; the ANSI/TIA-568-B.2-1 specification states the cable may be made with 22- to 24- AWG-

gauge wire, so long as the cable meets the specified testing standards. When used as a patch cable, Cat-6 is normally terminated in 8P8C modular connectors. Cat-6 connectors are made to higher standards that help reduce noise caused by crosstalk and system noise installed in metal conduit to preclude damage; the conduit shall be sized to accommodate all wiring.

C. Low Voltage Control Wiring

1. Plenum or riser cables shall be IEEE C2 CL2P certified.

D. Digital Data Interconnection Wiring

1. Interconnecting cables carrying digital data between equipment located at the security center or at a secondary control/monitoring site shall be not less than 20 AWG and shall be stranded copper wire for each conductor. The cable or each individual conductor within the cable shall have a shield that provides 100 percent coverage. Cables with a single overall shield shall have a tinned copper shield drain wire. Plenum or riser cables shall be IEEE C2 CL2P certified.

XIV. LEGACY OFFICES

- A. For CBP Offices that have not upgraded to fully digital CCTV systems, the following will apply.

1. Video Multiplexer

- (a) The [video multiplexer](#) shall be a multi-channel record and playback system with the capability of color real time multi-screen viewing. Electronic components, sub assemblies, and circuits of the multiplexer shall be solid state. The multiplexer, using time division multiplexing, shall permit up to 16 camera inputs to be recorded simultaneously on a single video cassette recorder (VCR). All 16 camera inputs shall be capable of being viewed on a video monitor either live or recorded. The multiplexer shall allow for viewing of either live video or input from the DVR/VCR (Simplex Operation). The multiplexer shall allow for simultaneous viewing, recording playback, and multiplexing (Duplex Operation). The inputs shall be capable of simultaneous viewing on the monitor or full screen individually and in other multi-screen modes such as 2x2, 3x3, 4x4 or other configurations. The viewing format shall also permit 2x dynamic zoom capability, full screen. The multiplexer shall be compatible with EIA/NTSC/PAL video cameras. External camera synchronization shall not be required for proper operation of the video multiplexer. Control of all functions of the multiplexer shall be provided either by a full function keyboard or by push-button selection with on-screen menu driven set-up. The multiplexer shall retain the current program for at least 6 hours in the event of power loss.

The video multiplexer will have a built-in video loss detection that alerts the operators or technicians of camera failure. Logical camera numbering provides the ability to assign any camera number to the physical input. An integral color bar generator allows the user to adjust monitor settings.

2. Predelivery Testing

(a) General

- The contractor shall assemble the test CCTV system as specified, and perform tests to demonstrate that the performance of the system complies with the contract requirements in accordance with the approved pre-delivery test procedures. The tests shall take place during regular daytime working hours on weekdays. Model numbers of equipment tested shall be identical to those to be delivered to the site. Original copies of all data produced during pre-delivery testing, including results of each test procedure, shall be delivered to the Government at the conclusion of pre-delivery testing prior to Government approval of the test. The test report shall be arranged so that all commands, stimuli, and responses are correlated to allow logical interpretation.

(b) Test Setup

- The contractor shall provide the equipment needed for the test setup and shall configure it to provide alarm actuated camera call-up and alarm recording as required to emulate the installed system. The test setup shall consist of at least 4 complete camera circuits. The alarm signal input to the CCTV test setup shall be by the same method that is used in the installed system. The video switcher shall be capable of switching any camera to any monitor and any combination of cameras to any combination of monitors;
- The minimum test setup shall include:
 - i. Four video cameras and lenses, including dome cameras if required for the installed system;
 - ii. Three video monitors;
 - iii. Video recorder/DVR if it is required for the installed system;
 - iv. Video switcher including video input modules, video output modules, and control and applications software;
 - v. Video multiplexer, if required for the installed system;
 - vi. Alarm input panel if required for the installed system;

- vii. Pan/tilt mount and pan/tilt controller if the installed system includes cameras on pan/tilt mounts;
- viii. Any ancillary equipment associated with a camera circuit such as equalizing amplifiers, video loss/presence detectors, terminators, ground loop correctors, surge protectors or other in-line video devices; and
- ix. Cabling for all components.

XV. SYSTEM VALIDATION ASSESSMENT FOR EMERGENCY RESPONDERS (SAVER)

- A. The U.S. Department of Homeland Security (DHS) has established the [System Assessment and Validation for Emergency Responders \(SAVER\)](#) program to assist emergency responders making procurement decisions. The SAVER Program conducts unbiased operational tests on commercial equipment and systems, and provides those results along with other relevant equipment information to the community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the [DHS Authorized Equipment List \(AEL\)](#).
- B. Follow these steps to reach the [SAVER Project Library Index](#).
 - 1. Go to the [Project Library Index site](#);
 - 2. Scroll down to, and click on, “14 Physical Security Enhancement Equipment”;
 - 3. Select “14 SW Surveillance, Warning, Access Intrusion Control”;
 - 4. Click on “14SW-01 General”;
 - 5. 14SW-01-VIDA Systems, Video Assessment, Security”;
 - 6. Click on “14SW-01-VIDA CCTV Technology”;
 - 7. Chose the appropriate IDS assessment project document.
- C. To request the complete CCTV Technology Report, fill out the SAVER Document Request Form. Enter your e-mail address and the format in which you’d prefer to receive the document – e-mail, mailed CD, or mailed hard copy. This link leads only to the request form for the full CCTV Technology Report. To view the project highlights or assessment summary documents, follow the instructions above.

XVI. FURTHER INFORMATION

- A. For more information, see [The United Facilities Guide Specifications for Closed Circuit Television Systems](#)
- B. For questions contact cbp.security@dhs.gov







APPENDIX 10: STORAGE OF WEAPONS AND AMMUNITION (ARMORY)

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

I. GENERAL

- A. Armories provide space within the U.S. Customs and Border Protection (CBP) law enforcement and detention facilities for the storage, issuance, and upkeep of weaponry, ammunition, and chemical agents. Armory spaces can include the issuing area, weapons maintenance area, ammunition storage area, and sensitive equipment storage.
- B. Armories may be constructed as part of new construction or installed in existing facilities. Armory construction will include the structural floor deck, partitions, ceiling, door, door frame and locking mechanism, issuance window shutter system, ventilation openings, lighting, fire detection and suppression, security monitoring intrusion detection systems, storage shelving and racks, counter work surfaces, pneumatic system, and hazardous material storage containers.
- C. Armories will not be used for the storage of classified information.

II. PLACEMENT WITHIN A FACILITY

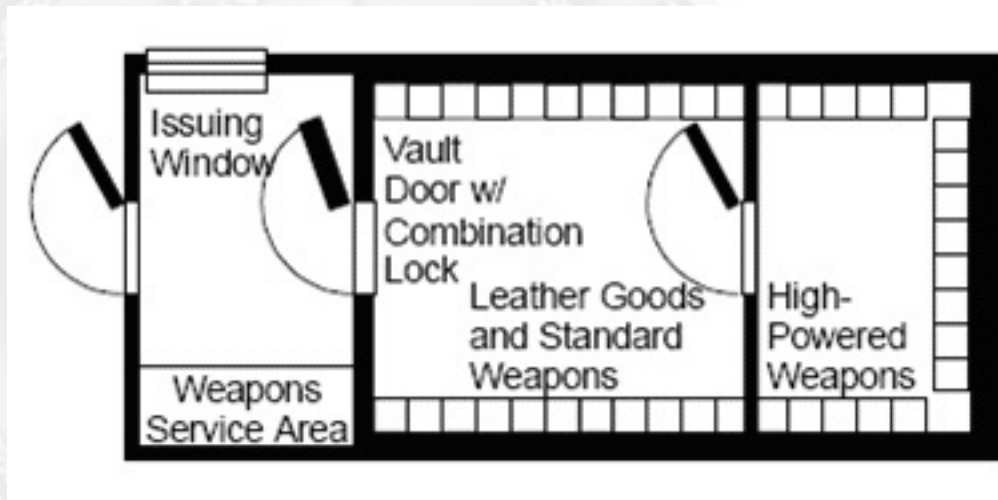
- A. Armories shall be located within the secure perimeter of a building. The public shall not have access to the exterior face of any portion of the armory. The armory shall not be placed contiguous to spaces where individuals can make attempts to compromise the armory without detection such as: equipment rooms, physical plant space, infrequently accessed storage rooms, or shell space.
- B. Armories shall be located where the entrance is under the direct visual control of a manned post with the entrance not being visible to the public. If the armory is located in a facility with secure detention areas, the armory shall be accessible through a secure vestibule or sally port to prevent either detained individuals or individuals from the outside from accessing the armory. Armory doors and issues windows will be monitored by closed-circuit television (CCTV).

III. ARMORY LAYOUT

- A. A clearing barrel shall be located at the staff entrance to the facilities to assure the weapons are void of bullets after they are worn on duty.
- B. The armory needs to be divided into separate areas with a secure area or safes for high-powered and fully automatic weapons. The armory may have a separate space for chemical storage with its own 100% exhaust ventilation. The armory shall also have a separate area for issuing and servicing weapons. This area will be located outside the primary vault perimeter in a vestibule at the front of the armory. Access to the armory shall be through this vestibule by authorized individuals. [Figure 1](#) is an example of an armory layout.

- C. Provide a counter area for cleaning and servicing weapons. Weapons can generate hazardous residue through the lead contaminates from firing. The areas provided for the cleaning and care of weapons shall allow for the proper cleanup and disposal of any materials that become contaminated with lead. Safe storage shall also be provided for the solvents and equipment used in the cleaning process.
- D. Building mechanical rooms and emergency generators shall not be located directly contiguous with armory rooms to avoid any sparks ignition of inventory.

Figure 1: Armory Layout



IV. MINIMUM CONSTRUCTION REQUIREMENTS FOR ARMORIES

A. Walls

1. New construction

- (a) For new construction, armory walls shall be constructed to meet Class M – 15-minute attack resistance as defined in ASTM F 1247 Standard Specifications for Intrusion Resistant Generic Vault Structures.
- (b) Formed concrete walls ([Figure 2](#)) will be a minimum of 8 inches wide and poured with concrete that has compression strength of 3000 psi. Formed concrete walls will extend from slab to slab and will be reinforced with either 2 grids of #5 rebar (5/8-inch) spaced at 4 inches on center or 2 grids of 9 gauge expanded metal. Reinforcing must be firmly anchored to the structural decks.
- (c) Class B Vaults (Minimum Construction) shall conform to Federal Specification AA-V-2737. Class B vaults are GSA approved modular vaults and shall be six (6) sided (floor, ceiling, and four sides) as specified in [AA-V-2737](#).

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

2. Existing Construction

- (a) For existing structures with limited floor loading capability, other wall construction may be considered. For existing walls ([Figure 3](#)), a layer of steel plate of 1/4-inch thickness may be added. The steel plate must be firmly anchored with steel supporting members at 16 inches on center that are secured to building structural members. All seams shall be continuously welded.

Figure 2: Poured Concrete

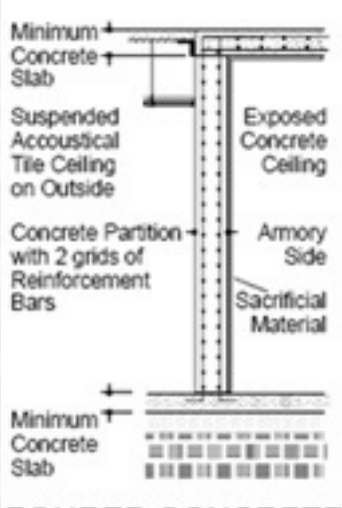
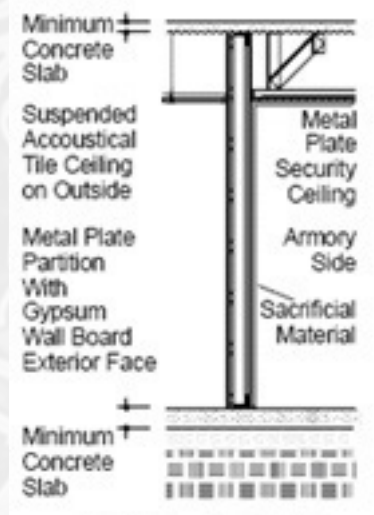


Figure 3: Metal Plate



3. In weapon maintenance areas, provide two layers of 1/2-inch wood surface or other sacrificial material to prevent bullet ricochet on wall and hard ceiling surfaces.
4. Internal areas of armories such as high powered weapons storage can be separated from other armory areas. Use 9-gauge expanded metal mesh securely welded to a 1 3/4-inch steel angle structural frame with vertical supports placed at 18 inches on center. Welds will be 1/8-inch wide by 2-inches long and placed at all seams and joints every 16 inches. The partition shall have an integral gate. The gate will have a single padlock meeting the requirements of Federal Specification FF-P-2827A . The lock shall be protected from tampering by a 1/4-inch metal plate. Gate hinge pins shall be non-removable.

B. Floors

1. Armories may receive inventory for a full year at one time. This can impose a substantial amount of weight on the armory floor. The inventory stored in the armory combined with the armory construction and furnishings, can exceed the allowable structural floor load capacity of existing buildings or the loading limit required by code for business occupancies. The dead (building material weight) and live (imposed weight of storage items) loads must be calculated for

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

each armory installation to assure that the structure is adequate to support the inventory and also meet code requirements.

2. For existing structures that have floor load limitations, careful consideration of armory construction must be taken to reduce, to the most feasible extent possible, the dead loads created by partitions. To control concentrated live loads under these conditions, shelving heights must be limited to that supportable by the structure, and signs must be posted limiting the height that material may be stacked. If possible, the floor and structural frame shall be further reinforced to increase the load capacity.
3. Armory floors must be designed to resist entry from cavities above ceilings and walls.
4. Floors are to be a minimum of 8-inch concrete, reinforced with two grids of #4 rebar placed on 9-inch centers. Concrete shall have compression strength of 3000 psi.
5. For armories installed on existing floors with less than 8 inches of reinforced concrete; an additional layer of 1/4-inch metal plate shall be placed over the floor. (All seams and joints need to be continuously welded.)
6. Floors shall be finished with anti-static material and have an oil- and solvent-resistant finish. Flooring must be resistant to impacts from dropped items or heavy pallets.

C. Ceilings

1. The ceiling shall be designed to thwart entry into the vault area with equivalent protection as provided by the partitions. The armory may either have an exposed ceiling with the structural deck above providing the secure barrier or a constructed ceiling creating a plenum between the ceiling and the structural deck above. When the surrounding armory partitions are secure to the structural deck above, the constructed ceiling does not have to be a secure element and may be a standard suspended acoustical tile ceiling system. For constructed ceilings that form part of the secure enclosure of the armory, ceilings may either be exposed reinforced concrete, pre-cast concrete, reinforced plaster, or a metal ceiling system.
2. Formed concrete ceilings will consist of 8-inch concrete, reinforced with two grids of #4 rebar placed on 4-inch centers or two grids of 9-gauge expanded metal. Concrete shall have compression strength of 3000 psi. Reinforcing must be firmly anchored to the surrounding walls.
3. Pre-cast concrete ceilings may consist of standard concrete "T" members with minimum flange dimensions of 6 inches. Pre-cast concrete members must be

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

securely attached to walls or other building structural members. When pre-cast ceilings are insufficient in depth, 1/4-inch metal plate shall be secured over the ceiling.

4. Plaster ceilings ([Figure 4](#)) shall be constructed of a minimum of 9-gauge expanded metal in 2-inch diamond pattern covered on both sides by 1 ¼ inch cement plaster. The ceiling shall be supported by no less than a 3-inch steel angle at 18 inches on center. The expanded metal must be securely welded to the angle supports.
5. Steel plate ceilings ([Figure 5](#)) shall be constructed of 1/4-inch metal plate securely welded to a metal deck that is supported by a 3-inch steel angle structural frame at 18 inches on center. Welds will be 1/8-inch wide by 2 inches long and placed at all seams and joints every 16 inches. Place epoxy sealant between welds at all seams and joints.
6. In weapon maintenance areas, provide two layers of 1/2-inch wood surface or other sacrificial material to prevent bullet ricochet on wall and hard ceiling surfaces.
7. Provide access panels, with dead bolt keyed locks in constructed ceilings, to plenum space above the ceiling. The access panel must be of 1/4-inch steel plate. Non-removable hinges shall be located on the inside of the armory. Provide a dead bolt lock keyed from the bottom side of the access panel. The lock shall be protected from tampering on the outside by a 1/4-inch metal plate. The access panel frame shall be 1/4-inch steel.

Figure 4: Plaster Security Ceiling

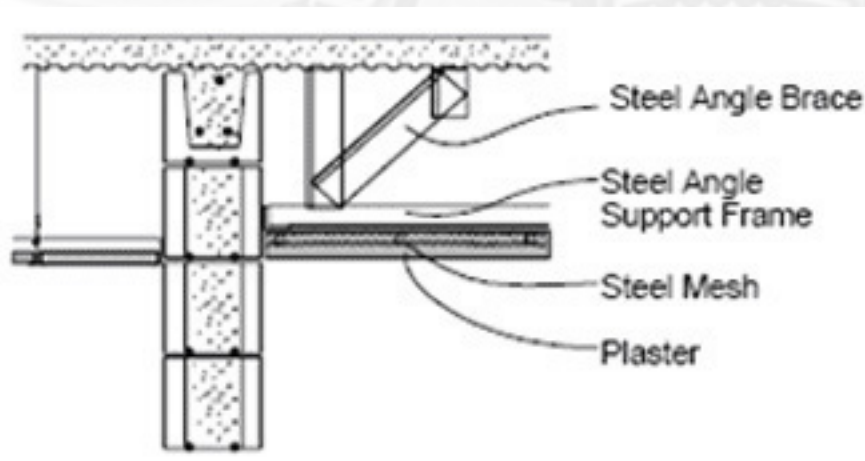
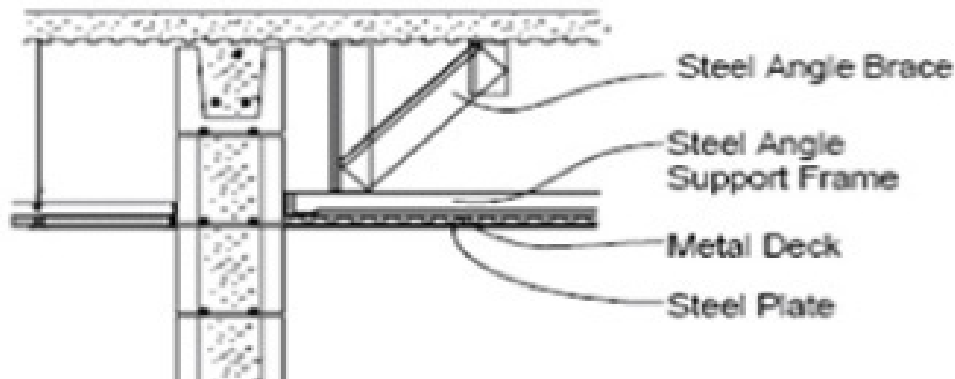


Figure 5: Steel Plate Security Ceiling



D. Doors

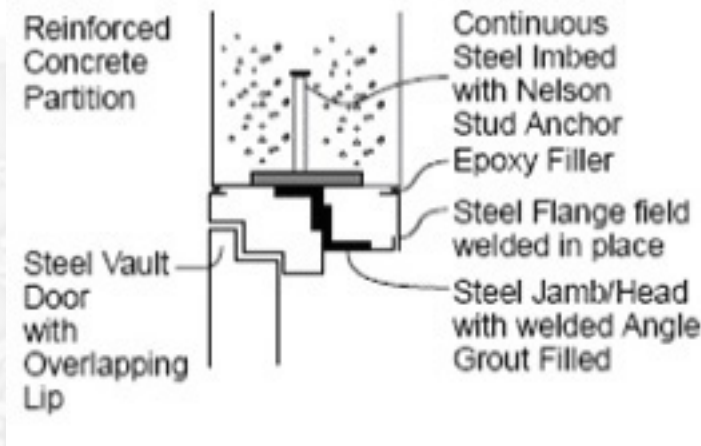
1. Armories will be fitted with GSA Class 5-A vault doors as defined in Federal Specification [AA-D-600D](#).
2. Each vault door furnished by contract or order under Federal Specification AA-D-600D shall bear metallic labels as specified below.
 - (a) General Services Administration label. The General Services Administration Label shall be affixed to the outside of the door. The label shall be silver background and red letters not less than 3mm in height. The label shall show the following:
 - (b) GENERAL SERVICES ADMINISTRATION
 - (c) APPROVED SECURITY VAULT DOOR
 - (d) MANUFACTURER'S NAME
 - (e) Identification label. An identification label shall be affixed to the inside face of the door frame. The label shall show the door model and serial number, date of manufacture, and Government contract number.
 - (f) Certification label. A certification label shall be affixed to the inside face of the door bearing the following certification:
 - (g) This is a U.S. Government Class 5-A vault door which has been tested and approved by the Government under Federal Specification AA-D-600. It affords the following security protection:
 - 30 man-minutes against covert entry;
 - 10 man-minutes against forced entry;

- (h) The protection certified above applies only to the door and not to the vault proper.
 - (i) Number label. All vault doors shall have a number label securely affixed to the front face. Regardless of the method used, the label attachment shall not degrade the door security. The label shall be mounted on the door frame, above or to the left side of the door. The label shall be nominal 0.5 mm thick, satin finished aluminum and shall be 63-65 mm by 17-20 mm. The label numbering system shall be established by the manufacturer to provide non-repetitive numbers. The label numbers shall be not less than 4.5 mm high and shall be embossed.
 - (j) New vault door construction may be 3/8-inch metal front face with a 14-gauge thick back face, and an overlapping lip covering the frame joint ([Figure 6](#)).
3. Large vaults that may receive pallet shipments of ammunition can be equipped with double leaf entrance vault doors. The doors shall be constructed to GSA Class 5-A Standards and an astragal will be provided between the two leafs. The inactive leaf will have dead bolts keyed from the inside of the armory that engage the head and sill of the door frame. The active leaf will be equipped as per a single leaf vault door, with door leaf lips overlapping jamb joints and combination locks.

E. Door Frames

- 1. Door frames shall be a minimum of 1/4-inch metal construction;
- 2. The frame and door shall be mounted so that there will not be more than 3 mm clearance between the door and the door frame. The frame shall be designed so that when attached to the wall, the wall clamping bolts will be exposed only on the inside of the vault. The frame shall have leveling and adjusting screws to compensate for building sag which may occur at any time in the future; and
- 3. The frames and locks will be securely installed to prevent removal of the frame or disengagement of the lock from outside the vault area by welding to a continuous steel imbed with a minimum 6-inch Neilson stud imbedded in a formed concrete partition ([Figure 6](#)).

Figure 6: Vault Door Jamb at Concrete Partition



F. Door Hardware

1. Locks

- (a) Doors shall be equipped with a three-wheel tumbler, key-change combination lock, Group 1R lock as defined by UL 768 Standard for Combination Locks;
- (b) The lock's dial ring shall be mounted so as to be flush to the surface of the door. The attachment of the dial ring shall be firm and secure without movement or side play. The lock case shall be firmly and securely attached to the door by suitable and effective means to prevent movement or side play to the lock case. The lock shall not be modified in any manner from the formation supplied by the lock manufacturer, except that the spindle may be cut to proper length.

- 2. Hinges. The door shall be mounted to the frame by not less than two anti-friction bearing hinges, so designed to allow the door to be opened approximately 180 degrees. The hinges shall be removable from the outside;
- 3. Door stop. A door stop to prevent the door's face hardware from striking wall surfaces will be installed. The stop shall be designed to be wall mounted unless otherwise specified. The stop shall be able to withstand hard usage and shall not scratch or scar the door's painted finish when the door is swung open against it;
- 4. Door striker. The door shall have a striker on both the front and hinged edges to minimize play or shake in the door when in the locked condition. The fit of the door to the striker on both the front and hinged edges shall be such that there is not more than 1 mm play or shake in the door when the bolts are thrown to the locked position;

[RETURN TO TOP](#)

5. Door threshold. The door threshold shall be designed to provide a ramp at the door threshold of approximately 1/4-inch to permit free swing of the door after its installation. If receptive cups, ports, or grooves are used, they shall be recessed not less than 1/2-inch below the bolt in its extended position to prevent dirt or other substances from obstructing the locking mechanism.

G. Windows and Openings

1. For new construction, armories shall have no windows or other access openings directly inside of the armory;
2. For existing construction with windows or openings, they must be protected with Class IV ballistic resistant glazing and a tool resistant barrier grille with screening to prevent direct views into the armory;
3. Any opening directly from the armory larger than 96 sq. in. shall be protected by the following barriers:
 - (a) 1/2-inch steel bars a maximum of 6 inches on center, vertically and horizontally and spot welded at each intersection ([Figure 7](#));
 - (b) All ducts, piping, and wiring conduits passing through the walls, ceiling, or floor of the vault will pass through snug fitting sleeves at the time of construction; and
 - (c) All minor openings between pipes, conduit, and sleeves will be caulked.
4. Issuing windows will have an overhead roll-up metal shutter, coiling grille and stainless steel counter ([Figure 8](#)).
 - (a) Manual operation with overhead counter-balance device. The shutter shall consist of flat slats formed from 14-gauge stainless steel with stainless steel end blocks welded to each end of alternate slats. The bottom of the shutter will be reinforced with a stainless steel angle. (Provide proper mounting members to meet building construction requirements.);
 - (b) The shutter housing shall be formed of 14-gauge steel;
 - (c) The shutter will be equipped with bars that cross the door from jamb to jamb and prevent any movement of the door. The bars shall rest in brackets welded to the jambs and have a locking hasp to prevent unauthorized removal of the bars;
 - (d) Provide slide bolt locks on the coil side of shutters with hasps suitable for a high security padlock;
 - (e) Provide neoprene resilient type seals located along the jamb edges,

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

bottom of shutter, and within the housing; and

- (f) For additional protection, provide a coiling grille which will open from the inside. A pocket will be provided on one side to stack the grilles and on the other side the locking device needs to be concealed, secured, and not accessible to the outside.

Figure 7: Manbar Barrier

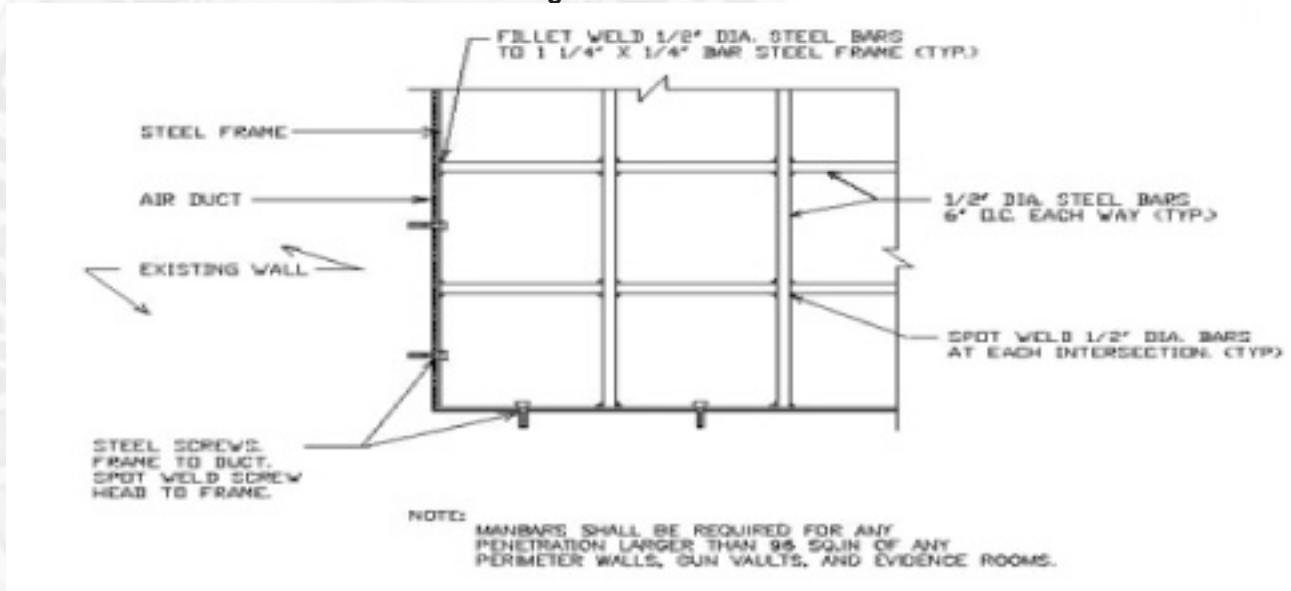
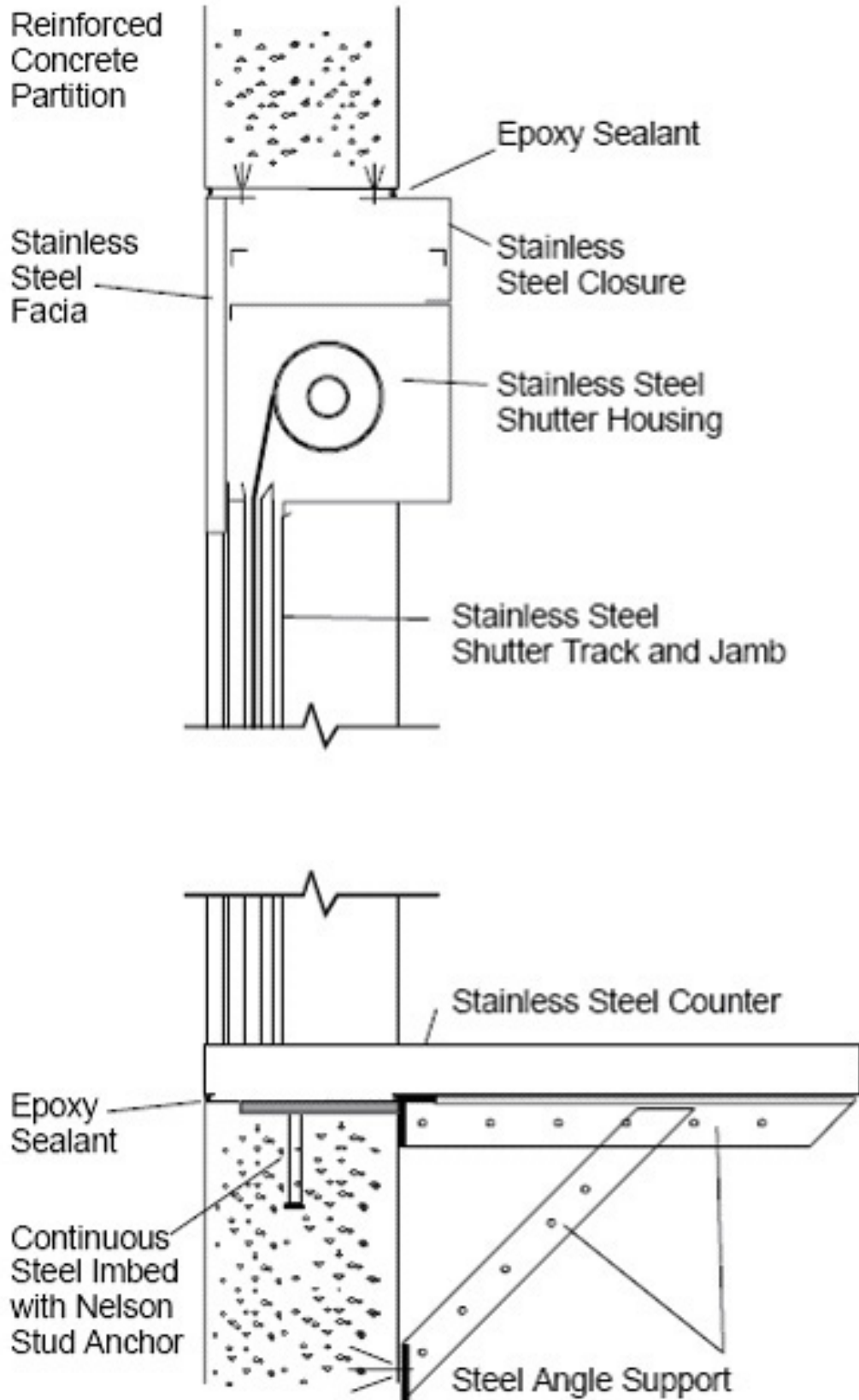


Figure 8: Overhead Counter Shutter



H. Fire and Smoke Detection and Suppression System

1. Armories will be equipped with a minimum of a fire and smoke detection alarm system plus a sprinkler fire suppression system. The fire alarm system will provide notification to emergency response agencies. Specific requirements include the following:
 - (a) Provide and install an enunciator panel to operate in conjunction with the fire alarm system. The panel is to be located in the control room at a location to be selected. Must meet appropriate NFPA codes;
 - (b) Fire and smoke detection sensors must be present in every area of the armory.

I. Intrusion Detection System (IDS)

1. All CBP armory locations will have intrusion detection systems to protect against unauthorized access. These systems will include: sensors; control units; transmission lines; and monitoring units integrated to be capable of detecting all breaches in security;
2. The system shall report directly to an alarm monitoring station, either on-site or off-site for unmanned facilities. Security systems will also activate an audio signal at the armory;
3. The intrusion detection system will include a central control station where alarms will sound and a response force can be dispatched (an alarm bell located at the armory is not acceptable). The intrusion detection system will be designed to cause an alarm to sound at the central control panel and at the armory whenever the system is turned off or malfunctions. On/Off, access, and secure switches not located at a central control station will be located within the alarmed area;
4. Response force shall react to an active alarm as soon as possible, but in no case may arrival at the scene exceed 15 minutes. Unmanned facilities will make arrangements to connect alarms to The Federal Protective Service Mega Center, or comparable Class A Monitoring Station with local police response, In the case of an unmanned station, the alarm system shall have an automatic dialer to alert the patrol agent in charge or the local Port Director or sub-office in case of an intrusion when no one is in the office;
5. A sign shall be placed prominently at the entry to the armory indicating the use of an IDS;
6. The armory will be equipped with a dual technology volumetric motion sensor that detects the presence of individuals within the armory. Separate sensors must be provided for each area of the armory;

7. The intrusion detection system will be equipped with an independent backup power supply that provides a minimum of 4 hours of Uninterruptible power or other duration as determined by a security analysis of the facility; and
8. Transmission lines for the alarm circuits from the armory to the central control station will have either two independent means of alarm signal transmission or line supervision with connecting lines electronically supervised to detect evidence of tampering or malfunction. If two independent means are used, then one must have either a radio or cellular telephone link. The system must be able to seize control of the communication link. All links will be physically and electronically secure. All cable lines need to be encased in metallic conduit. All equipment must be mounted in tamper-resistant enclosures. Key control for the enclosures will be the same as for the armory itself. For more information on IDS, refer to [Appendix 8.9, Intrusion Detection Systems](#).

J. Communication Systems

1. An intercom or telephone link must be provided at the armory entrance connected to the central control station to coordinate status changes;
2. The armory must also have a telephone connection, either in the armory or in the issuing area, which is tied into the facility phone system for use by staff working in the armory.

K. Access Control. At a minimum, all armories will be equipped with door and lock position indicators with magnetic contacts. Automated access control systems may be used. The system shall be capable of maintaining a record of who accessed the armory room. Access control systems may use a keypad, card reader, or a combination of both.

L. Closed-Circuit Television (CCTV). For armories in manned facilities, provide a CCTV system with cameras viewing the exterior entrance and all areas of the interior. The system must be continuously monitored at a staffed central control position. For more information on CCTV refer to [Appendix 8.12, Closed Circuit Television](#).

V. MECHANICAL EQUIPMENT

A. Environment Requirements. Weapons and ammunition shall be kept in a cool, dry environment. Room dehumidifiers need to be installed in the armory. Install small heating elements in the gun vaults.

B. Ventilation

1. Armories must have 15-minute Class M emergency vault ventilators and ventilator ports per UL 680 Emergency Vault Ventilators and Ports (emergency vault ventilators provide fresh air to persons locked in the armory by accident or

[RETURN TO TOP](#)

during robberies).

- (a) The vault ventilating port is intended to be connected to an outside ventilating system that provides circulating air while the vault is open;
 - (b) The port shall not be able to be rendered inoperable from outside of the armory;
 - (c) The port will be equipped with a visual indicator showing the location of the port to a person in the vault, and if the port is in the open or closed position;
 - (d) The ventilator port shall allow for voice communication to someone outside the vault and also allow the passage of small tools and food items to a person inside the vault;
 - (e) The ventilator ports will allow for the supply of 10 cubic feet (0.28 cubic meters) of fresh air per minute per 9 square meters (100 square feet) of area;
 - (f) The ventilator port shall provide a minimum of 2 square inches (1250 square mm) of open area in case of a power failure;
 - (g) The port will be protected as described in paragraph IV.G.3. above; and
 - (h) The ventilator ports shall be placed so that cabinets or equipment cannot be placed to obstruct the opening, both inside and outside the armory.
2. Ductwork for chemical storage room exhausts shall be of stainless steel construction. Supply ducting shall be wrapped or lined to conserve energy, eliminate condensation, and reduce noise;
 3. In the issue vestibule, provide adequate ventilation air exchange of 50 cubic feet (1.4 cubic meters) per minute of outside air in order to ensure the removal of fumes and odors associated with solvents that are used in the cleaning of firearms. Chemical storage rooms shall have 100% exhaust ventilation. Exhaust vents shall be located away from air intake vents or equipment generating sparks.

C. Air Inlets

1. Grilles, registers, and diffusers will be designed and fabricated similar to those used in penal/detention facilities. The face shall be cold-rolled steel 3/16 of an inch thick. Each unit shall be of welded construction and meet the requirements of the American Society for Testing of Materials. Supply units shall be 1-, 2-, 3-, or 4-way directional throw, as required, to provide a uniform air supply free of drafts throughout the area.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

D. Electrical

1. Provide standard fluorescent light fixtures, switched inside the armory with some fixtures circulated to an emergency power source. Place switches immediately inside the armory. Provide continuous light at the exterior of the vault door;
2. Two duplex receptacles must be available inside each area of the armory. Provide duplex electrical outlets at 3 feet on center and at 3.6 feet above the floor at weapon maintenance counters. Provide a dedicated electrical circuit for the pneumatic air cleaning system.

E. Plumbing

1. The equipment service area shall have access to a hand wash sink for use by the staff. The sink area provides: hot and cold running water with lever fixtures, a soap dispenser, mirror, paper towel dispenser, and waste receptacle;
2. If chemical storage is required, then the area will be provided with an emergency eye wash station.

VI. STORAGE

A. The armory will be equipped with housing cabinets for specialized high value equipment, weapons, ammunition, and chemical agents. The type of housing for weapons varies in size, shape, level of security, and material used. Generically, they take the following forms, depending on the type of weapons being used:

1. Cabinet;
2. Lockers;
3. Gun racks; and
4. Lock boxes.

B. Cabinets

1. Provide a 14-gauge welded double wall metal shell or body, with two-coat epoxy finish, vents with flash arrestors, and a leak-proof sill. Provide 14-gauge doors, with continuous piano type hinges, integral key dead bolt lock or hasp for padlock. Locks shall be recessed into the door, with a 1/8-inch protective plate. Provide combination or key operation. If key operation is used, design for armory master key operation. Provide metal or wood shelves, adjustable to 1/2-inch on center. Provide leveling legs and wall anchor to secure cabinet to the wall and prevent cabinet from tipping over or being removed by unauthorized individuals. Install security and safety warning labels as required. If chemical agents are to

[RETURN TO TOP](#)

be housed, provide an anti-static grounding system;

2. Cabinets may be equipped with pull out drawers constructed with slides designed to support a minimum of 150 pounds. Each drawer shall have a combination dead bolt lock. (Provide drawer inserts to accommodate specific weapon and gear inventory.)

C. Lockers

1. Provide a 14-gauge welded double wall metal shell, or body, with two-coat epoxy finish and sloped roof; having 14-gauge doors, continuous piano type hinges, and integral dead bolt lock or hasp for padlock with combination or key operation. If key operation is used, tie in to armory master key. Provide one to two metal shelves and hooks for hanging items. Include leveling legs plus wall anchors to secure locker to the partition to prevent locker from tipping over or being removed by unauthorized individuals. Provide locker numbers and security and safety warning labels as required by type of inventory.

D. Gun Rack

1. Open gun racks must be designed to accommodate rifles, shotguns, and automatic weapons. They should allow for height adjustment up to a minimum of 38 inches;
2. Gun racks need to be constructed of 14-gauge welded steel. They should have felt-cushioned butt support and barrel rests; and
3. Gun racks will be secured to walls and have either a bar that locks the weapons in place, or a cable that can be threaded through the weapons to secure them in place.

E. Ammunition. Ammunition may be stored on open shelf systems within the armory. Shelf units may be constructed of either wood or metal. Shelf units shall be secured to armory partitions to keep the shelf units from falling over.

F. Lock Boxes. Cabinets configured with lock boxes may be used to store restricted inventory in the armory. Lock boxes shall be constructed to comply with the requirements of UL 1037 Anti-theft Alarms and Devices Residential Secure Containers. Lock boxes will be double walled minimum 14-gauge steel construction with a minimum 14-gauge steel door; and secured to the partition or floor. They shall have individual keyed dead bolt locks, and a key for all other locks.

G. Other Storage Devices. The armory shall have coat hooks and pegs for storage of gear and leather goods in the open air or in vented cabinets to allow moisture to

escape. Armory wall surfaces need to have pegboard finishes to allow for hanging inventory.

VII. WEAPONS SERVICE EQUIPMENT

- A. Guns produce lead dust during use. When cleaned, the lead dust can contaminate solvents, rags, and other items used while cleaning the gun; therefore, gun service areas must be designed to control lead contaminates.
- B. Areas for servicing weapons and equipment will include counters at 42 inches above the floor. The counters may be plastic laminate or stainless steel. The counters need to have knee space, and may have equipment drawers, pedestals, and upper cabinets for storage of equipment, cleaning supplies, and solvents. Storage space must also be provided for safety devices, such as goggles and gloves.
- C. A hazardous material storage container shall be provided in the gun service area for disposal of contaminated rags. Signage must be placed on the container indicating the presence of lead contaminates and at the counter instructing that all contaminated materials must be disposed of properly.
- D. The gun service area may also contain power tools and other equipment such as grinders, lathes, milling machines, drill presses, and refinishing equipment.

VIII. INDEPENDENT ARMORY MAGAZINE STRUCTURES

- A. If the armory is located in a separate structure more than 500 feet from other occupied facilities or is larger than 300 square feet, the building housing the function must be equipped with male and female toilet facilities. (These facilities must be accessible for individuals with disabilities.)
 - 1. If the armory is located in a separate structure and will contain large quantities of ammunition on pallets, it shall be equipped with a receiving dock having an elevated platform 4 feet above the vehicle parking surface. The vehicle parking surface shall extend 120 feet beyond the dock edge to accommodate tractor-trailer delivery vehicles. The dock shall have a 50-foot by 12-foot area for unloading of delivery vehicle contents;
 - 2. The armory located in a separate structure may require an office space for range master duties with views to the issue window and receiving dock; and
 - 3. Armories in an independent structure will require mechanical, electrical, telephone, and janitor closet space. Physical plant equipment spaces shall not open directly into armory storage areas. Exhaust and air supply vents need to be located remotely from any direct exhaust from storage areas.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- B. Armories located in separate structures need to have perimeter security fences. The fences shall be located a minimum of 20 feet (6 meters) from the structure, providing a buffer zone for security monitoring. It will be a minimum of 10 feet (2.4 meters) high and have a sloped top or include concertina wire integrated to the top of the fence.

IX. ADDITIONAL CONSIDERATIONS

A. Ready Rooms

1. Requirements. Space may be required for the storage of: clothing articles; fire and medical emergency response equipment; communication equipment; and other gear used by officers to respond to special situations. Ready rooms are not for the storage of weapons, ammunition, or chemical agents. They do not need to be designed to the same level of security as armory rooms;
2. Location. Ready rooms may be placed in public or staff corridor areas where officers can immediately access equipment;
3. Walls. Either core filled concrete masonry unit (CMU) walls, or expanded steel mesh reinforced gypsum wallboard and metal stud partitions may be used. Concrete masonry walls may be constructed with the cores and kerfs filled with concrete. No steel reinforcing is need for security purposes;
4. Gypsum wall board partitions with steel mesh shall be constructed of: one layer of gypsum wall board on each face, over 9-gauge expanded metal mesh under the outside face, on 3 5/8-inch metal studs. The partitions shall extend from structural floor to structural deck above;
5. Ceilings. Ready rooms may have standard suspended acoustical tile ceiling or be exposed to underside of the structure. When existing conditions prevent extension of partitions to the structural deck above, provide a secure ceiling consisting of 1.5 inches of plaster on metal lath or 14-gauge perforated metal pan screwed on metal runners;
6. Doors. Provide 12-gauge hollow metal doors 1 3/4 inches and a 12-gauge hollow metal frame. Non-removable pin hinges must be provided. A keypad or cipher lock will be included in order that officers can access the ready room without having to obtain keys during an emergency. The lockset shall allow emergency egress from inside the ready room;
7. Windows and Openings. Ready rooms in new construction shall not have windows. Existing windows shall be protected with tempered glass, fixed glazing panels, or a wire mesh barrier grille. Exposed openings shall have a 14-gauge steel barrier grille;

8. Security. Ready rooms shall have balanced magnetic door switches and an electric strike connected to a central monitoring station and to audio alarms at the ready room;
9. Fire Detection and Suppression. Ready rooms need fire and smoke detection sensors. The system shall be connected to a central monitoring station and audio alarms at the ready room. Ready rooms shall be provided with sprinklers based on building occupancy requirements;
10. Mechanical System and Ventilation. The ready room shall have standard mechanical service with a minimum supply of 20 cubic feet of fresh air per minute per 9 square 100 square feet;
11. Electrical and Lighting. The ready room shall have standard fluorescent light fixtures switched inside the ready room. Occupancy sensors shall be incorporated that turn the light off after extended periods of time when the room is unoccupied. A duplex electrical outlet needs to be provided on each wall of the ready room where they are not obstructed by cabinets or stored items; and
12. Equipment. The ready rooms shall be equipped with shelving units, cabinets, cabinet drawers, lockers, hooks, and pegboards for storage of equipment with a minimum 20-gauge steel construction. Individual units do not require key or combination locks. These units need to be provided with floor leveling devices, and shall be secured to partitions to prevent tipping over of loaded units.



APPENDIX 11.14: SCREENING PROCEDURES

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

I. PUBLIC ENTRANCES/EXITS

- A. X-ray machines are used to scan bags, briefcases, purses, packages, boxes, mail trails and parcels for the detection of weapons, explosives, narcotics, and flammables using X-ray technology.
- B. Magnetometers are used to scan individuals for the detection of metal using electromagnetic technology.
- C. Facility security standards indicate that the placement of X-ray and magnetometer screening devices at all public entrances for the screening of visitors, contractors, etc., and all of their purses, bags, briefcases, packages, etc., is:
 - 1. Mandatory for Level IV facilities, a standard based on facility evaluation by CBP for Level III facilities;
 - 2. Desirable for Level II facilities;
 - 3. Not applicable for Level I facilities.
 - 4. Additionally, the X-raying of all packages entering the building delivered by contractors, couriers, etc., is mandatory for Level IV facilities, a standard based on facility evaluation by CBP for Level III facilities, desirable for Level II facilities, and not applicable for Level I facilities; and
 - 5. Radiation screening devices are only for use in Level IV facilities based on a facility evaluation and determination made by CBP.

II. RECEIVING AND SHIPPING

- A. Facility security standards require that X-raying all incoming packages and mail is mandatory for Level IV facilities, a standard based on facility evaluation by CBP for Level III facilities, and desirable for Level II and I facilities. At a minimum, appropriate security precautions must be established for all deliveries to include controlled bulk freight arriving at a facility loading dock if it is not X-rayed.

III. LIGHTING REQUIREMENTS

- A. Illumination of 70 foot-candles at minimum must be provided at the workstations and must afford visibility without shadows or glare. Additional task lighting is to be provided directly over these examination work areas.
 - 1. CBP Mobile X-ray Vans/Units (Parcel X-ray and Personal X-ray)
 - 2. Large Commercial Vehicle and Truck Inspection Facilities

- (a) X-ray;
- (b) Ion mobility;
- (c) Spectrometry;
- (d) Gamma ray imaging; and
- (e) Neutron analysis.



Figure 1: Mobile VACIS - Gamma Ray Imaging System



Figure 2: Mobile Search Advanced X-ray Portable Inspection System

IV. UNDER-VEHICLE LIGHTING SYSTEM

- A. These are systems used to illuminate the underside or other areas of a vehicle. In addition to providing a sufficient amount of lighting, the quality of lighting must be good enough to allow thorough screening. The system should aim to eliminate shadows and create contrast.
 - 1. Cargo and Vehicle Inspection Systems;
 - 2. Safety and Regulatory Considerations; and
 - 3. Mobile Vehicle Inspection Systems (Imaging).

Table 1: Sample Power Requirements for Fixed Inspection Systems

Inspection System	Power Requirements	Notes
AS&E Shaped Energy ISO Search X-ray Inspection System	100 kVA site power	Includes power to inspection equipment and power for gantry transport
SAIC Portal VACIS	3 kVA per lane 120/240 VAC	
SAIC VACIS II (track system)	30A , 220-240 VAC	Documentation indicates 5kW of backup power is sufficient for the VACIS II system components, additional power required for operating booth, HVAC, etc.

V. GEOMETRIC DESIGN OF ROADWAYS FACILITIES

- A. Develop facilities in accordance with the guidelines provided above except as modified in the following sections.
- B. X-ray and Magnetometer Screening Devices
- C. Radiation Screening Devices
- D. X-ray Screening Devices
- E. Irradiation Devices
 - 1. Irradiation devices are used to attempt to render safe a biological device that may have been maliciously placed in mail. Irradiation devices are a standard for use in Level IV and III facilities based on a facility evaluation and determination made by CBP. Irradiation devices are desirable in Level II and I facilities.

VI. CONSTRUCTION REQUIREMENTS

- A. Detailed drawings of the Secondary X-ray Processing Workstations are included in the appendix and should be used in conjunction with the provided specifications. Each CBP Secondary X-ray Processing Workstations houses a personal computer (CPU, monitor, and keyboard), a document reader, a printer, and ancillary lighting and equipment.
- B. Specifications and planning guidance must be obtained from CBP. However, the overall design of the Secondary X-ray Processing Workstations must protect the officer from physical assault and provide an immediate means of egress in case of an emergency.

VII. ELECTRONIC VEHICLE ENTRY CONTROL

- A. The function of an entry-control system is to ensure that only authorized personnel are permitted into or out of a controlled area. Entry can be controlled by locked fence gates, locked doors to a building or rooms within a building or specially designed portals.
- B. These means of entry control can be applied manually by guards or automatically by using entry-control devices. In a manual system, guards verify that a person is authorized to enter an area, usually by verifying the photograph and personal characteristics of the individual requesting entry. In an automated system, the entry-control device verifies that a person is authorized to enter or exit. The automated system usually interfaces with locking mechanisms on doors or gates that open momentarily to permit passage. Mechanical hardware (such as locking mechanisms, electric door strikes, and specially designed portal hardware) and equipment used to detect contraband (such as metal detectors, X-ray baggage-search systems, explosives detectors, and special nuclear-material monitors) are described in other documentation.
- C. All entry-control systems control passage by using one or more of three basic techniques: Coded, credential, and biometric.
- D. CBP often stations mobile X-ray equipment at select airports based on operational requirements. These vehicles must be housed in a secure enclosure when not in use.
 - 1. The enclosure should provide shelter from the elements as well as protection from acts of vandalism and theft. A garage or space within the airport terminal building, accessible from the airfield operations area (AOA), is acceptable. Enclose this area with solid walls or floor to ceiling 11-gauge chain link fencing with tension cables top and bottom. Provide vehicle gates with locks keyed individually to a CBP master. The enclosure must have a minimum ceiling height of 9 feet. No special HVAC is required.
- E. For continuous daily operation, the X-ray vans/units will require adequate dedicated electrical service (120VAC 20AMP) from weatherproof outlets or by an onboard gasoline generator if necessary.
- F. A large vehicle inspection facility may be a separate, centralized facility or combined into the functions of a commercial/large vehicle. The following guidelines are intended to provide general considerations in the design of such an inspection facility.
 - 1. An installed large vehicle inspection facility is intended to be the single point of inspection for all large commercial and truck traffic intending to pass through the installation. Once a vehicle is inspected and authorized to access an installation, that vehicle may be tracked and monitored until it enters and exits the installation;

[RETURN TO TOP](#)

2. The design of the large vehicle inspection station should be based on the usage of large vehicle inspection equipment;
3. Since many of these devices are not currently deployed, the design should include space for vehicle inspection equipment and provide utility conduits to the anticipated location for future use. The inspection equipment may be a mobile or stationary. It should be noted that some detection equipment is built-in to a large, drive-through structure. If this type of equipment is anticipated, then this could be coordinated and incorporated into the inspection office and overhead canopy facilities;
4. Installations planning closed-circuit television (CCTV) inspection of the top and underside of vehicles should mount these cameras on the overhead canopy and in the pavement below the vehicle;
5. At a minimum, the inspection facility should possess the infrastructure to support the installation of CCTV inspection equipment, to include adequate lighting to illuminate the underside of the vehicles during inspection; and
6. Some installations may also consider the use of vehicle inspection pits, although this type of facility is not recommended due to commonly encountered soil conditions and anticipated operational safety issues. The following sections contain information on various inspection-related devices in order to facilitate the layout of the truck inspection facility and the determination of the required infrastructure to support inspection equipment.

VIII. CCTV UNDER VEHICLE SEARCH SYSTEMS (UVSS)

- A. The effectiveness of these systems has not been fully assessed and results of initial testing vary. Therefore, the use of CCTV UVSS should be in accordance with Service guidelines.
- B. If a CCTV UVSS is utilized, evaluate the following considerations and guidelines:
 1. Consider maintenance requirements. Is the equipment self-cleaning?
 - (a) If installed below grade, is the enclosure waterproof? Is the vault and equipment designed to support large vehicle loading?
 2. Install the system far enough in advance of the access control point so that the largest vehicle can pass over the equipment without entering the installation;
 3. Drainage should be established such that water drains away from the equipment.
 - (a) When providing drains from the equipment enclosure, provide backflow prevention valves to prevent water from entering the vault. Ensure any

water that may be captured in the vault will not drain through control conduit to the control center.

4. The electrical circuit serving the equipment should be a ground fault interrupt (GFI) circuit;
 5. Monitoring area should be free of glare;
 6. Vehicle speed should be kept below 15 mph (24.1 km/h) to ensure adequate performance; and
 7. Where exposed to freezing temperatures, the equipment installation should include heaters.
- C. There are many types of automated inspection equipment for large vehicle or cargo inspection. Some of those available, including X-ray and gamma ray inspection systems, provide an image of the contents of a vehicle or container. Due to the wide-ranging requirements for the different manufactured systems, it is not possible to provide detailed guidance that will support all types of this equipment. However, this section will identify the important infrastructure considerations associated with both mobile and fixed X-ray/gamma ray inspection systems.
1. These systems offer the ability to inspect vehicles or containers without removing the cargo. The equipment typically consists of a transmitter (X-ray or gamma ray) and a detector on the opposite side of the target vehicle;
 2. Gamma ray systems utilize a low-level, gamma-ray radiation source to generate a beam of gamma rays to penetrate the object. The detectors on the opposite side then measure the amount of gamma ray absorption:
 - (a) This data is then translated into an image of the contents of the vehicle or container. X-ray systems typically utilize electro-mechanical equipment to generate X-rays to penetrate the object. Detectors on the opposite side then record the X-ray transmission, which is then translated into an image. The Mobile Search and Shaped Energy ISO Search systems (discussed below) also include a detector on the transmission side of the unit that detects the X-ray reflections which occur from organic materials, producing a second type of image of the contents.
- D. Due to the use of gamma or X-ray radiation, there are safety and regulatory considerations in the use of these systems. The requirements vary depending on the system. Normally an exclusion zone, an area where personnel are not permitted during operation of the equipment, is established within and around the inspection equipment. The region outside of the exclusion zone is considered safe for personnel during scanning operations. The size of the exclusion zone varies greatly depending on the type of equipment.

- E. Nuclear Regulatory Commission regulations State that radiation dose limits in Public-Uncontrolled areas are 2 mR in any hour or 100 mR in any year. Therefore, depending on the characteristics of the source, the frequency of scans, and the expected occupancies, the exclusion zone can vary. Additionally, a shielding wall can be constructed to reduce the dose substantially. Some X-ray systems have qualified as a “cabinet X-ray system” in accordance with Food and Drug Administration (FDA) regulations or similar standards, meaning minimal shielding is required and the exclusion zone does not extend outside of the footprint of the inspection area. In order to qualify for this designation, FDA regulations require an emission limit of 0.5 mR per hour at 2 in (5 cm) from the surface of the cabinet. Other regulatory considerations are that systems utilizing radioactive sources may require operation under a radiation materials license held and administered by the owner of the equipment (the installation) and a permit for operation may be required.
- F. There are several truck-based, mobile large vehicle or container inspection systems currently available. Two examples are illustrated in [Figure 3](#). These systems utilize a boom type arm to form an inspection tunnel.
- G. In no case are vehicle operators to remain in the vehicle during a scan. The operator is either to exit the vehicle or the vehicle is positioned such that the operator is outside the scan area prior to the scan initiating.
- H. In order to properly plan the required space for this type of equipment, the detailed operational procedures must be reviewed.
- I. The Mobile Search system is designed to acquire images by traveling at a constant velocity past any number of parked vehicles in a line. This is accomplished using an electric secondary drive motor that propels the vehicle at a constant velocity.
- J. The Mobile Search system is capable of scanning only on the “driver’s side” of the Mobile Search vehicle.
- K. The maximum height of the boom is 16 ft 6 in (5.03 m), with a maximum scanned vehicle dimension of 8 ft 6 in (2.59m) wide x 14 ft (4.27 m) high. The width of the equipment with boom and stairs deployed is 25 ft (7.62 m).

Figure 3: Two Truck-Based, Mobile Large Vehicle or Container Inspection System



IX. MOBILE VACIS

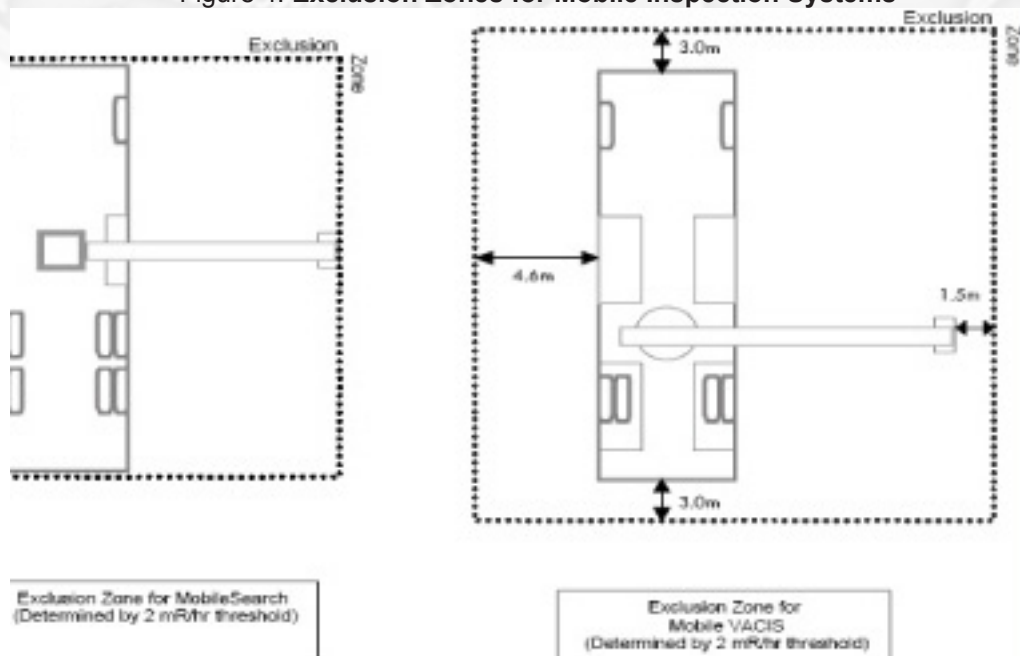
- A. The Mobile Vehicle and Cargo Inspection System (VACIS) is designed to acquire images by either traveling past a stationary vehicle or in a pass-through mode as a moving vehicle passes through the scan area.
- B. The system can conduct operations on either side of the VACIS vehicle.
- C. The vehicle requires a clear height of 20 ft (6.1 m) and a surface grade of less than 5%. The exclusion zone for each system is illustrated in [Figure 4](#).
- D. Exclusion zones are based on the 2mR in any one-hour dose limit. The 100 mR per year limit may govern the location of a permanent facility.
- E. Self-contained portable units require no land based power or other facilities.
- F. If an entry control facility or truck inspection station design is to incorporate a portable vehicle inspection system similar to those illustrated above, but no system specification exists, the following recommendations regarding site development should be followed:
 - 1. Provide a 35-ft (10.7 m) wide x 110-ft (33.5 m) long paved inspection area for use by the portable equipment. This provides enough width for the inspection system

[RETURN TO TOP](#)

and the travel lane for the vehicles to be inspected. The length is sufficient to allow the inspection system to scan a large stationary vehicle and maneuver;

2. To increase throughput, provide a longer inspection lane for operation of a portable system that scans stationary vehicles. This will allow the system to scan several vehicles at one time;
3. Provide no canopy over the inspection area planned or dedicated for use by the portable equipment unless the clear height is a minimum of 22 ft (6.7 m);
4. Site all permanent facilities or guard posts such that they would remain outside of the exclusion zone. A shielding wall may be required if there are occupied buildings or areas near the detector;
5. Situate all permanent facilities such that they are not in the direction of travel of the radiation beam unless the distance between the inspection vehicle and the facility is at least 300 ft (90m.) The intent is to ensure that the 100 mR / year radiation dose limit is not exceeded for personnel who may be in the direction of travel of the radiation. This distance can be reduced to 75.5 ft (23 m) if a 12 in (305 mm) wide x 8 ft (2.4 m) high (minimum) concrete shielding wall is provided between the radiation source and any facility of concern; and
6. The determination of exclusion zones should also consider oblique scan angles, which some inspection systems can implement.

Figure 4: **Exclusion Zones for Mobile Inspection Systems**



- G. There is a wide range of fixed vehicle inspection systems. The systems operate in a manner very similar to the mobile systems. The types of systems can be categorized

as follows:

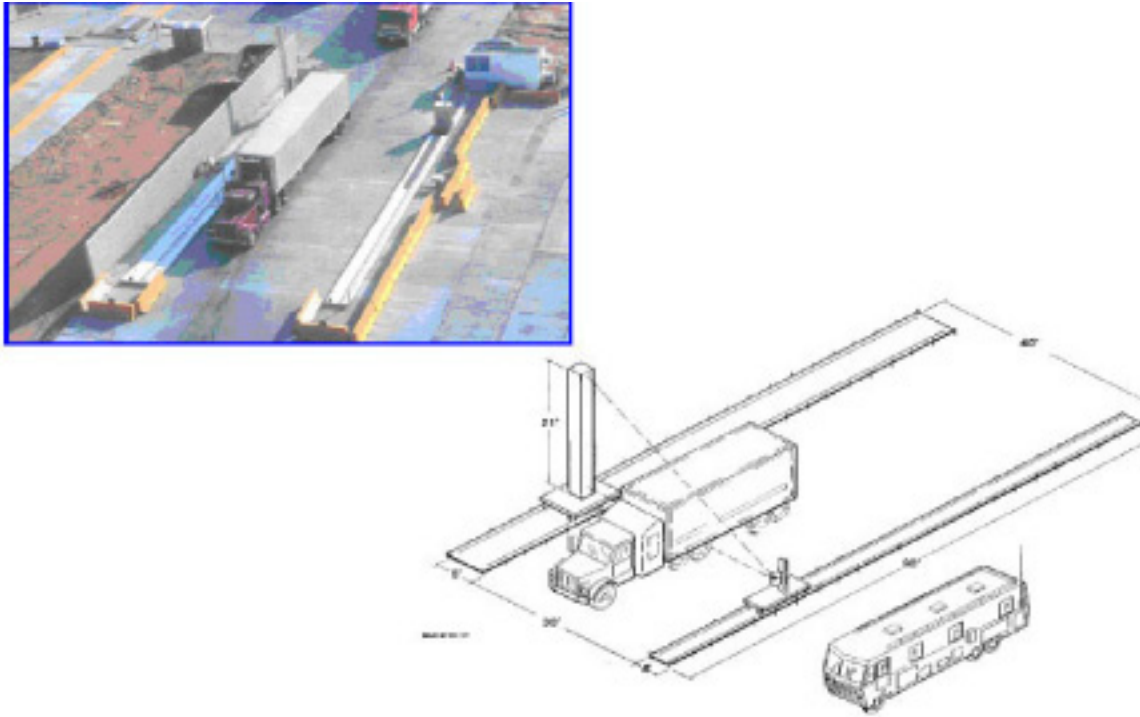
1. Stationary Target Vehicle - transmission source and detector travel past the target on a rail system or similar platform;
 2. Controlled Target Vehicle - vehicle is moved through a fixed inspection system on a platen or gantry transport, on a rail system, or similar device; and
 3. A Portal system - with a fixed inspection system where vehicles pass-through the equipment
- H. Examples of these systems are illustrated in [Figure 5](#), [Figure 6](#), and [Figure 7](#). The space requirements vary from minimal for the portal system to significant for a transport or stationary vehicle system.

Top: Figure 5: Fixed / Portable Vehicle X-ray Inspection Systems (Imaging)



Bottom: Figure 6: Portal VACIS – Gamma Ray Imaging System

Figure 7: VACIS II Gamma Ray Imaging System



- I. As outlined for the mobile inspection systems, exclusion zones may be required for the fixed systems. For illustration purposes, the exclusion zones and/or radiation levels associated with the VACIS II and AS&E Shaped Energy ISO Search systems are provided in [Figures 8-10](#). Note that the VACIS II exclusion zones depend on the type of radioactive isotope used and the presence of a shielding wall. Some systems have no exclusion zone outside of the actual scan area. In no case are the vehicle operators to remain in the vehicle during a scan. The operator is either to exit the vehicle or the vehicle is positioned such that the operator is outside the scan area prior to the scan initiating.

Figure 8: Shaped Energy ISO Search X-ray Inspection System

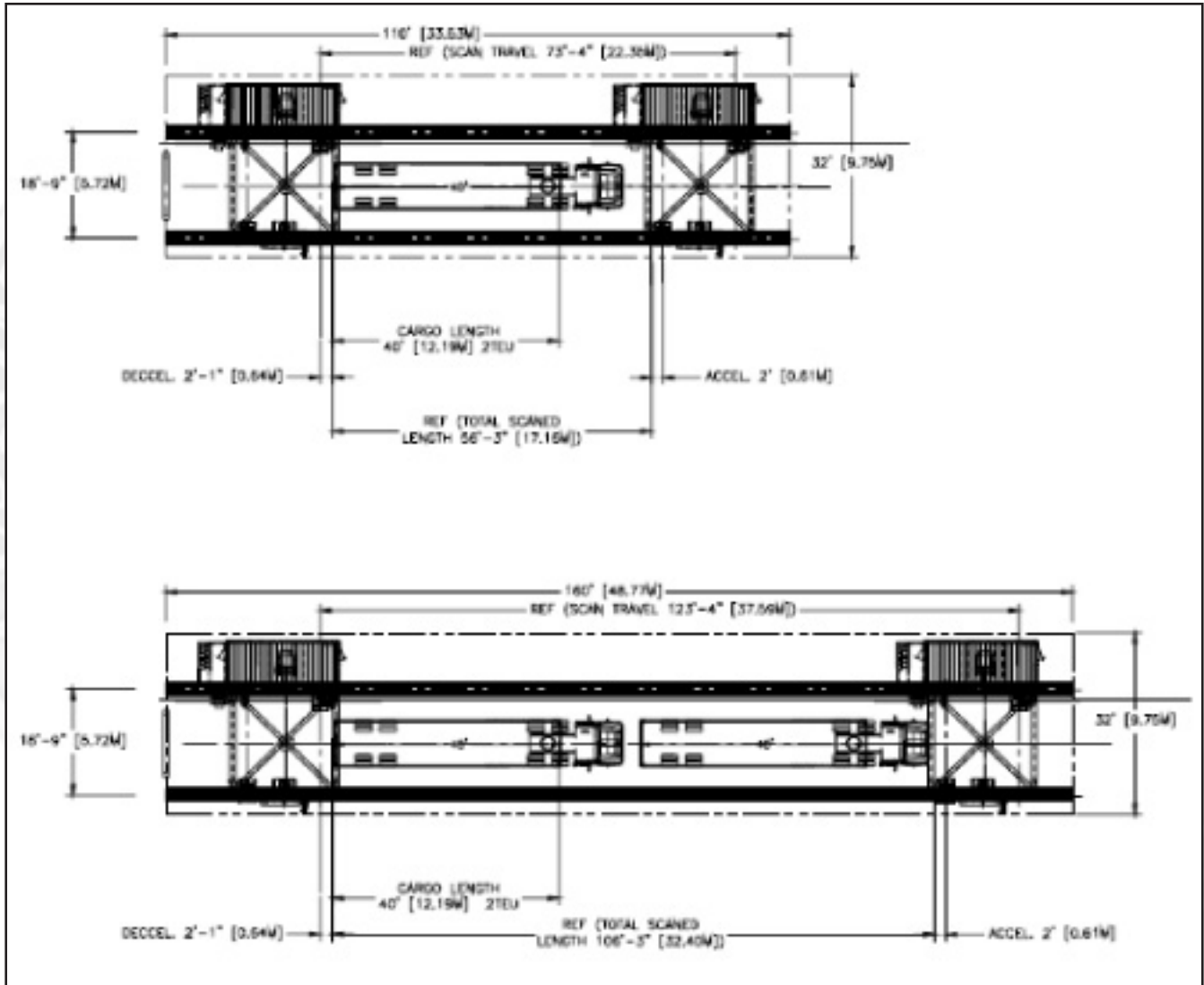
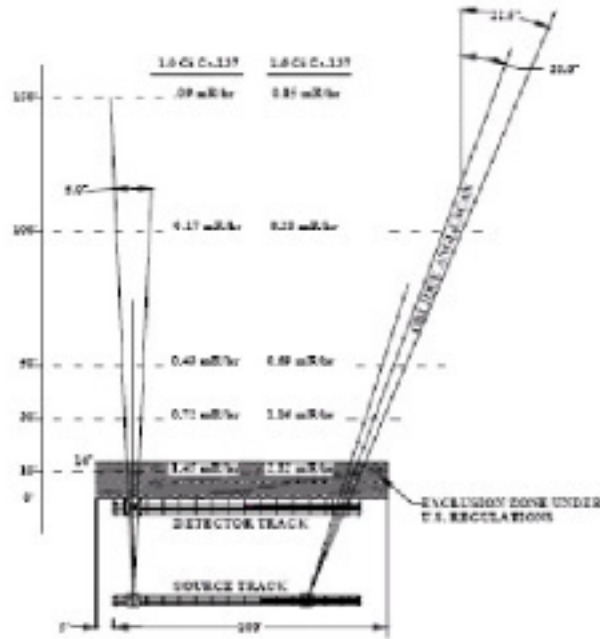
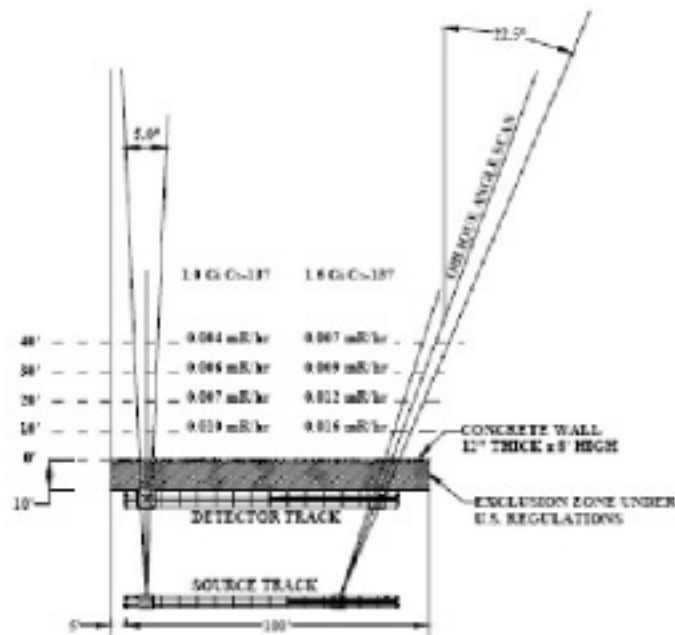


Figure 9: **VACIS II – Gamma Ray Imaging System Exclusion Zones (Cesium Source with and without Shielding Wall)**

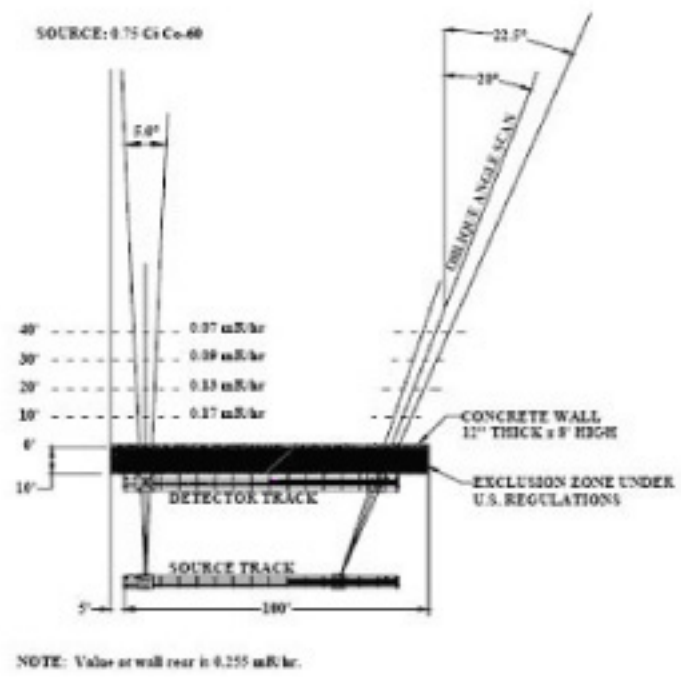
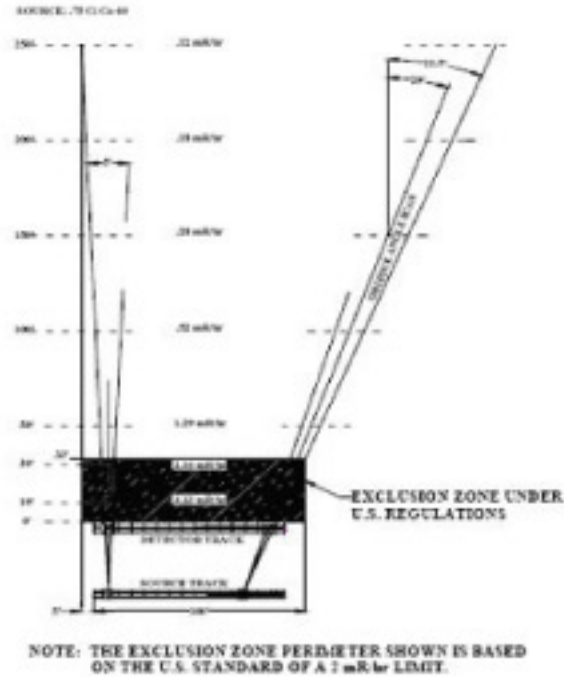


NOTE: EXCLUSION ZONE PERIMETER SHOWN FOR TYPICAL US INSTALLATION FOR 1.8 Ci SOURCE AT 2.0 mR/hr LIMIT.



NOTE: Value at wall rear for 1.8 Ci Cs source is 0.075 mR/hr.
Value at wall rear for 1.8 Ci Cs source is 0.073 mR/hr.

Figure 10: VACIS II – Gamma Ray Imaging System Exclusion Zones (Cobalt Source with and without Shielding Wall)



X. SPACE REQUIREMENTS FOR FIXED/PORTABLE SYSTEM LAYOUT

Figure 11: Large Vehicle Inspection Facility – Mobile Imaging Systems

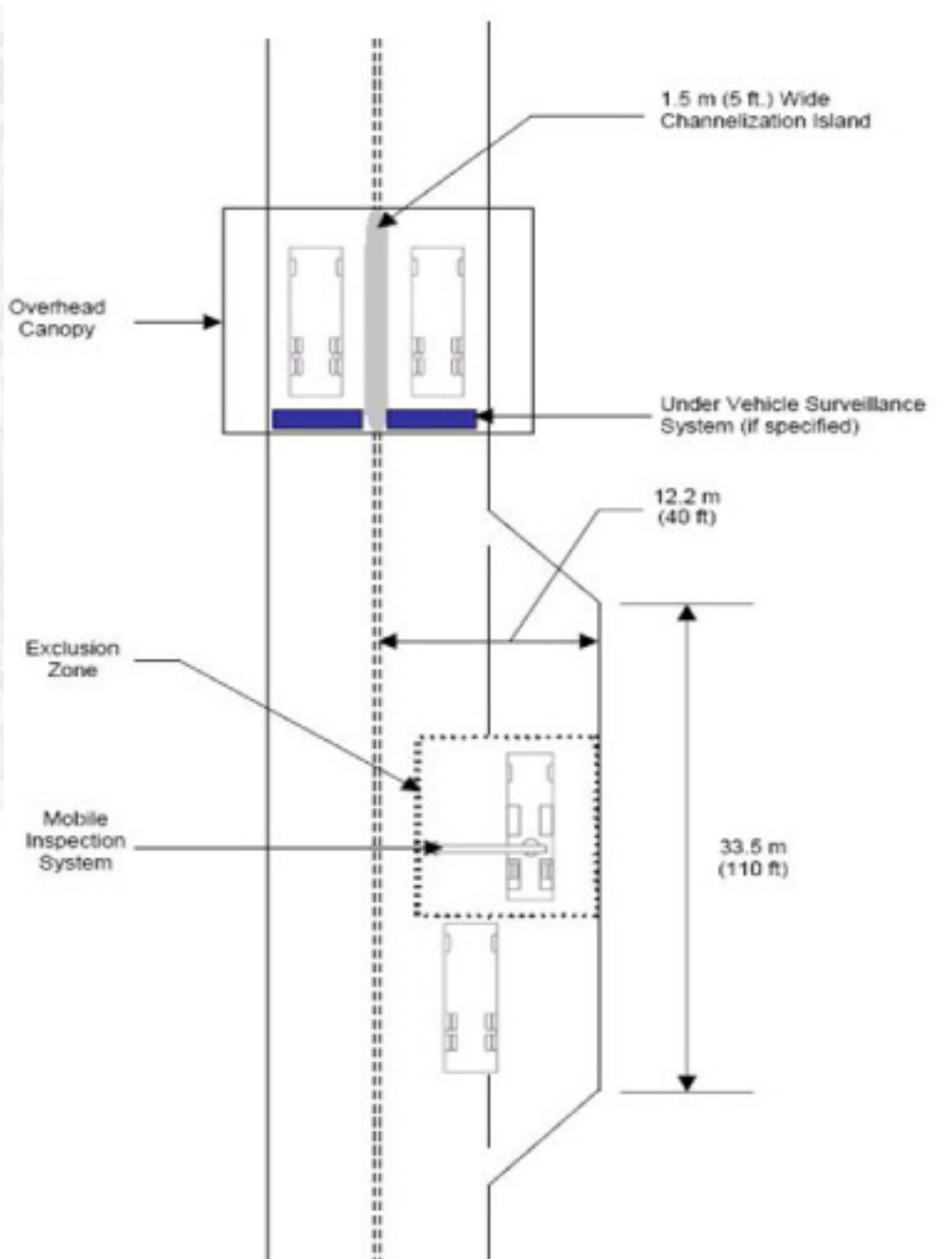
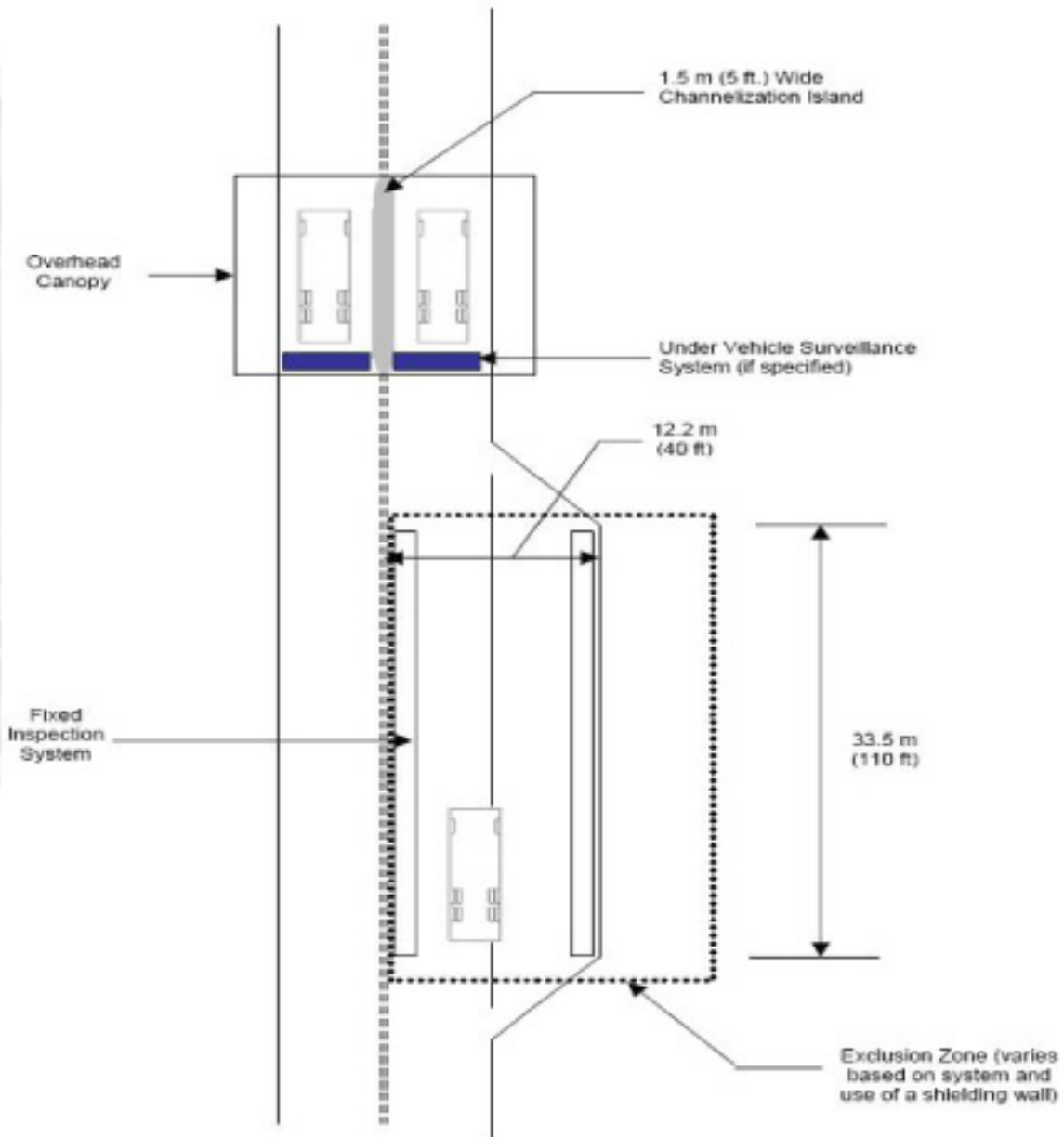


Figure 12: Large Vehicle Assessment Facility – Fixed Imaging System



XI. FIXED/PORTABLE SYSTEMS

- A. The power requirements of fixed/portable systems vary widely depending on the system type. Gamma-ray systems use a radioactive source to generate the transmission rays. This requires less power compared to an X-ray system, which generates the X-ray transmission using electro-mechanical means. [Table 1](#) illustrates the potential power requirements.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- B. If an inspection system is specified, consult with the manufacturer concerning the latest requirements for power. If no inspection system is specified, and the future inclusion of a system is likely, the design of the electrical power system should consider an allowance to provide sufficient site power to support this future requirement.
- C. The space requirements of imaging systems vary greatly.
 - 1. Systems that require a stationary vehicle or move the vehicle on a rail or platen system past fixed detectors require the most space;
 - 2. A portal system requires minimal space.
- D. Design of an entry control facility or truck inspection station is to incorporate a fixed vehicle inspection system similar to those illustrated above.
- E. If the system is unspecified the following recommendations regarding site development should be followed:
 - 1. Provide a 35-ft (10.7-m) wide x 110-ft (33.5-m) long paved inspection area for use by the fixed equipment. This provides enough width for the inspection system and the length of travel for the equipment or a platen/gantry system. The length is sufficient to allow the inspection system to scan a large stationary vehicle and maneuver;
 - 2. Provide a longer inspection lane for operation of a portable system that scans stationary vehicles, allowing the system to scan several vehicles at one time and increasing throughput;
 - 3. A minimum clear height of 22 ft (6.7 m) is required for a canopy over inspection lanes dedicated for use by the fixed equipment. This is conservative since some systems will operate with a clear height of 15 feet (4.57 m) and could be installed under a canopy;
 - 4. Consider provisions for automated inspection equipment to be installed prior to the main inspection area. It is often desirable to complete any automated inspection such as under vehicle screening system (UVSS) or imaging prior to arriving at the main, covered inspection area for identification and further inspection tasks. Therefore these functions should precede the final inspection area. Most inspection systems are designed to be outside and do not require shelter from the weather;
 - 5. Position all permanent facilities or guard posts such that they would remain outside of the exclusion zone. A shielding wall may be required if there are occupied buildings or areas near the detector; and
 - 6. Locate all permanent facilities such that they are not in the direction of travel of

[RETURN TO TOP](#)

the transmission beam unless the distance between the inspection vehicle and the facility is at least 300 ft (90m.) The intent is to ensure that the 100 mR/year radiation dose limit is not exceeded for personnel who may be in the direction of travel of the radiation. This distance can be reduced if a shielding wall meeting manufacturer's guidance is provided between the radiation source and any facility of concern.

- F. Provide channelization islands a minimum of 5 ft (1.5 m) wide to support the future installation of a portal inspection system.
- G. The layout of the large vehicle inspection facility is extremely important to ensure the facility will function properly.
- H. The civil design should consider the turning radius and other operating characteristics of the expected vehicle types.
- I. The facility should have multiple lanes of inspection to support different vehicle types or varying inspection levels.
- J. The design should have adequate stacking distances for the anticipated queue and parking for vehicles to be inspected and security vehicles.
- K. Parking areas should be sized for the range and volume of expected vehicles to be inspected.
- L. Consider providing a sally port in the inspection area:
 - 1. A sally port configuration is created through the use of vehicle barricades or traffic gates;
 - 2. These barriers are intended to confine the vehicle during inspection until it is determined that the vehicle is authorized to proceed or if the vehicle is denied admission to the installation; and
 - 3. The barriers can be used to aid in positioning the vehicle relative to inspection equipment.
- M. Some installations may require screening of the inspection operations from the remaining portions of the Entry Control Facility (ECF).
- N. Screening may increase safety and shields the inspection procedures from public view to prevent visual surveillance from unauthorized personnel.
- O. As discussed above in [Space Requirements for Fixed/Portable System](#), the inspection equipment can have a significant impact on the layout of a truck inspection facility. It is difficult to develop a layout that can support all potential types of automated inspection equipment.

[RETURN TO TOP](#)

- P. If the installation specifies the anticipated inspection systems, then the layout can be customized.
- Q. If the specific system is not identified, but the use of imaging or related inspection equipment is anticipated, the layout should facilitate the future incorporation of this equipment.
- R. [Figures 11](#) and [12](#) illustrate the incorporation of several types of inspection equipment into the layout of a large vehicle inspection facility. As illustrated, it is possible to provide areas for future equipment or as a minimum reserve space for the equipment when developing the site plan for an inspection facility. The following sections provide further detailed design guidance.
 - 1. Design roadways in a Large Vehicle Inspection Facility in accordance with the guidelines provided. Consider following the requirements to support oversized, atypical vehicles such as those frequently encountered during construction operations.

XII. CHANNELIZATION ISLANDS

- A. The minimum raised channelization island should be 5 ft (1.5 m) wide, 6 in (152 mm) high and 50 ft (15.2 m) long. A channelization island should be provided between each incoming traffic lane. These islands provide a safe position for security personnel and a location to mount present/future vehicle inspection devices.

XIII. WIDTH

- A. The minimum lane width should be 16 ft (4.9 m) in the inspection area. A preferred lane width of 18 ft (5.5 m) is recommended. The increased lane widths are required to facilitate manual inspection procedures and to support the potential for future automated inspection technology. Outside of the inspection area, the minimum lane width facilitating the flow of traffic and other operations is 12 ft (3.6 m).
- B. Inspection areas should be a minimum of 18 x 80 ft (5.5 x 24.4 m) x 17 feet 6 in (5.4 m) high that can be enclosed to protect inspection equipment in the event of bad weather.

XIV. VERTICAL CLEARANCES

- A. In order to support potential over height vehicles or future pavement overlays, a minimum vertical clearance of 17 ft (5.2 m) should be maintained throughout the inspection facility. Higher clearance may be desirable for inspection equipment.
- B. Provide a minimum clear height of 17 ft 6 in (5.4 m).

XV. INSPECTION OFFICE

A. The inspection office serves as the central control center for the truck inspection station and provides shelter for security personnel. Every truck inspection station should have an inspection office. As the control center, the inspection office controls the vehicle barricades, traffic control devices, access controls, and lighting. The office should include space for the following equipment and functions:

1. Support 3-5 security personnel;
2. House communications equipment;
3. Contain electronic control panels for all current or anticipated future automated gates or barriers;
4. Monitor stations for CCTV or computer monitors associated with automation controls, UVSS, and imaging systems;
5. Include an electrical room for the main electric panel boards and electronic controls;
6. Include locker storage for traffic control devices, weapons, and personnel equipment including vehicle inspection kits and the pre-positioning of personal protective equipment for CBR exposure;
7. Develop space for storing and charging batteries for communication and/or inspection equipment;
8. House computer servers for future automated identification systems;
9. Provide counter or work space; and
10. Include waiting/processing area for vehicle occupants.

XVI. CARGO HANDLING EQUIPMENT AND STORAGE

A. Although advanced inspection equipment is designed to inspect the contents of a suspect vehicle without opening or removing the cargo, it is anticipated that removal of cargo will be necessary at times for a complete inspection. In addition, current inspection procedures frequently require the removal of all or portions of the cargo in the suspect vehicle. Therefore, the truck inspection station should have cargo handling equipment and storage areas to provide temporary storage of material removed from suspect vehicles. The size of this area should be based on the anticipated demand.

XVII. ELECTRICAL POWER REQUIREMENTS

- A. Electrical design shall consider current power demands as well as the power requirements for future traffic control devices, identification equipment, and other devices associated with potential automation of the inspection station. This includes an allowance for the power demands of future vehicle inspection equipment, such as fixed large vehicle X-ray devices. See the section on [Space Requirements for Fixed/Portable System](#) for additional information concerning vehicle inspection equipment.

XVIII. EXTERIOR LIGHTING

- A. [IESNA HB-9](#) and [TM 5-811-1](#) discuss exterior lighting for general security purposes. The parking and roadway areas of the truck inspection station should have a minimum illumination of 3 footcandle (30 lux). The areas where the actual inspections take place should be illuminated to a minimum of 10 footcandle (100 lux).
1. It may also be necessary to provide additional task lighting in the ID and inspection areas to support adequate identification of vehicle occupants and contents. Lighting may also be mounted at or below pavement level to facilitate under vehicle inspection or associated with under vehicle inspection systems (see the section on [Space Requirements for Fixed/Portable System](#)).

XIX. PERIMETER FENCE AND GATE

1. Ensure that where the inspection facility is part of a Commercial/Large Vehicle Entrance Control Facility (ECF), each ECF has a gate enabling the ECF to be closed at the installation perimeter when not in use;
2. Reinforce gate with cables as indicated in [UFC 4-022-02](#) to increase resistance to a moving vehicle threat;
3. Secure a Type III Barricade to the gate horizontally in accordance with Manual Uniform Traffic Control Devices (MUTCD) (3 per lane). This configuration enables a reduced potential penetration and maximizes stand-off when the ECF is not in use;
4. Secure a centralized truck inspection facility located off installation with a security fence in accordance with service regulations; and
5. Include a gate enabling the inspection facility to be closed at the perimeter of the site when not in use.

BACK



APPENDIX 14: BUILDING-SPECIFIC SECURITY ALERT PLAN

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

I. GENERAL

INSERT BUILDING NUMBER

INSERT BUILDING ADDRESS

A. Purpose and Scope

1. The purpose of this plan is to provide appropriate security countermeasures for _____ BUILDING ADDRESS _____ during heightened security conditions due to emergency situations such as terrorist attack, natural disaster, and civil unrest.
2. During periods of heightened alert, it may be prudent to increase security at this facility over and above day-to-day security countermeasures. In order to ensure rapid escalation of security in the face of an increased threat, it is critical that a measured response be planned in advance. This plan provides five tiered sets of security measures to be taken in case of a change in the Security Alert level.

B. Definitions

1. Designated official. The highest ranking official of the primary customer agency or the alternate highest ranking official or designee selected by mutual agreement by other customer agency officials is responsible for developing, implementing and maintaining a current Occupant Emergency Plan (OEP) for each facility. See [Chapter 15, Occupant Emergency Plan](#), for more information on the OEP.
2. Contingency plans. Detailed plans designed to incorporate all the elements needed in order to direct the implementation of a response to an emergency situation that will ensure the protection of GSA-controlled facilities. Regions are responsible for developing regional specific plans that contain operational guidelines and procedures to address all possible contingencies for emergency situations. These plans should support and not conflict with established OEPs.
3. Continuity of Operations Plans (COOP). Detailed advance plans for the relocation of business services to designed alternate sites based on nature and severity of impact of threat or catastrophic event.
4. Emergency Situation. For the purpose of these guidelines, this will include: bombings, bomb threats, explosions and other hostile or destructive acts, civil disturbances, natural disasters, etc.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

[BACK](#)

5. **Security alert.** A condition, designated by a color, that is declared when an analysis of information gathered or the presence of an existing situation dictates the advisability of increasing the level of security.
6. **Background.** The purpose of the Homeland Security Advisory System (HSAS) is to advise government, industry, and the public of the Nation's current threat alert level. It combines threat information with vulnerability assessments and provides communications to public safety officials and the public to enact appropriate security countermeasures.

(a) Homeland Security Threat Advisories contain actionable information about an incident involving, or a threat targeting, critical national networks or infrastructures or key assets. They could, for example, relay newly developed procedures or protective measures that, when implemented, would significantly improve the current security baseline. They could also suggest a change in readiness posture, protective actions, or response. This category includes products formerly named alerts, advisories, and sector notifications. Advisories are targeted to Federal, State, and local governments, private sector organizations, and international partners.

(b) Homeland Security Information Bulletins communicate information of interest to the Nation's critical infrastructures that do not meet the timeliness, specificity or significance thresholds of warning messages. Such information may include statistical reports, periodic summaries, incident response or reporting guidelines, common vulnerabilities and patches, and configuration standards or tools. It also may include preliminary requests for information. Bulletins are targeted to Federal, State, and local governments, private sector organizations, and international partners.

(c) Color-coded Threat Level System is used to communicate with public safety officials and the public at-large through a threat-based, color-coded system so that protective measures can be implemented to reduce the likelihood or impact of an attack. Raising the threat condition has economic, physical, and psychological effects on the nation; so, the Homeland Security Advisory System can place specific geographic regions or industry sectors on a higher alert status than other regions or industries, based on specific threat information.

C. Implementation

1. This security plan was developed by FPS in conjunction with and approved by the Building Security Committee (BSC). No countermeasures will be implemented as part of these plans without the concurrence of the BSC.
2. Implementation of the plan will be upon:

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

- (a) A change in the HSAS Alert Level nationally, locally or with other respect to the facility (i.e., transportation sector);
 - (b) By the GSA Administrator nationally;
 - (c) By a GSA Regional Administrator for the respective region;
 - (d) By the Director of the FPS nationally; or
 - (e) At a specific facility upon recommendation of FPS and with concurrence of the BSC chairperson or Designated Official upon receipt of specific threat information regarding the building meriting its implementation (i.e., a planned demonstration).
3. The security plan is to be controlled as For Official Use Only, in accordance with DHS policy on Sensitive but Unclassified Information. It is also marked "Law Enforcement Sensitive," which although not a control mechanism indicates the sensitivity and type of information contained herein.
 4. This security plan will be reviewed with the BSC and revised as necessary as part of each recurring BSA or upon request of the BSC Chairperson.

D. Responsibilities

1. Federal Protection Services (FPS)
 - (a) FPS will ensure Plans are developed in conjunction with BSCs and are reviewed and updated at least as often as the periodic BSA is conducted.
 - (b) FPS will notify the BSC of changes to the Homeland Security Alert Level and other conditions that merit a corresponding change in security measures.
 - (c) FPS will coordinate with the BSC and GSA with regard to implementing increased alert levels absent a declaration by the DHS.
 - (d) FPS will notify suppliers of services and equipment to be delivered upon implementation (i.e., notifying guard companies of an increased staffing requirement).
 - (e) FPS will establish appropriate contracting mechanisms to facilitate rapid delivery of services in support of the Plan.
 - (f) FPS will provide other support as agreed to in the plan to implement countermeasures (i.e., increased K-9 patrols, etc.).
 - (g) FPS will verify that countermeasures have been implemented.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

(h) FPS will take appropriate steps for de-escalation once the Alert Level is reduced.

2. Building Security Committee (BSC)

(a) The BSC will work with the Inspector to develop the security plan for the building.

- In signing the plan, the BSC indicates concurrence with the actions to be taken.
- If the plan requires funding to implement such as increased guard presence, the Tenant Agencies will provide funding.

This Plan agreed to by:

FPS Regional Director

date

Building Security Committee Chairperson

date

[RETURN TO TOP](#)

BACK

Green Protective Measures	
General Guidance	Building Specific Actions
At regular intervals, remind customer agency representatives to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for suspicious vehicles on or adjacent to GSA property. Watch for abandoned parcels or suitcases and any unusual activity.	
Ensure the building manager or representative with access to building plans and occupant emergency plans is available at all times.	
Recommend buildings, rooms, and storage areas not in regular use be secured.	
Review all plans and requirements related to introduction of higher security level.	
Require US Government picture identification for Federal employees and a current valid government picture identification (such as a drivers license, state identification card, passport, or immigration card) system for visitors.	
Inspect and search all packages, handbags, and other containers, except those persons displaying US Government credentials. Deny entrance to all persons who refuse this inspection.	
Check basement, engineering spaces, heating and air conditioning ducts, shrubbery, and potential entry points such as roof openings, steam and other utility tunnels, doors and windows.	
Refine and exercise preplanned proactive measures. Ensure personnel receive training on Homeland Security Alert System (HSAS) and department or agency-specific protective measures. Regularly assess facilities for vulnerabilities and take measures to reduce them.	
Consult local authorities on the threat and mutual antiterrorism measures.	
Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.	
After normal duty hours ensure exterior and parking areas floodlights are operating properly to discourage intruders.	

Funding Impact Associated with these measures:

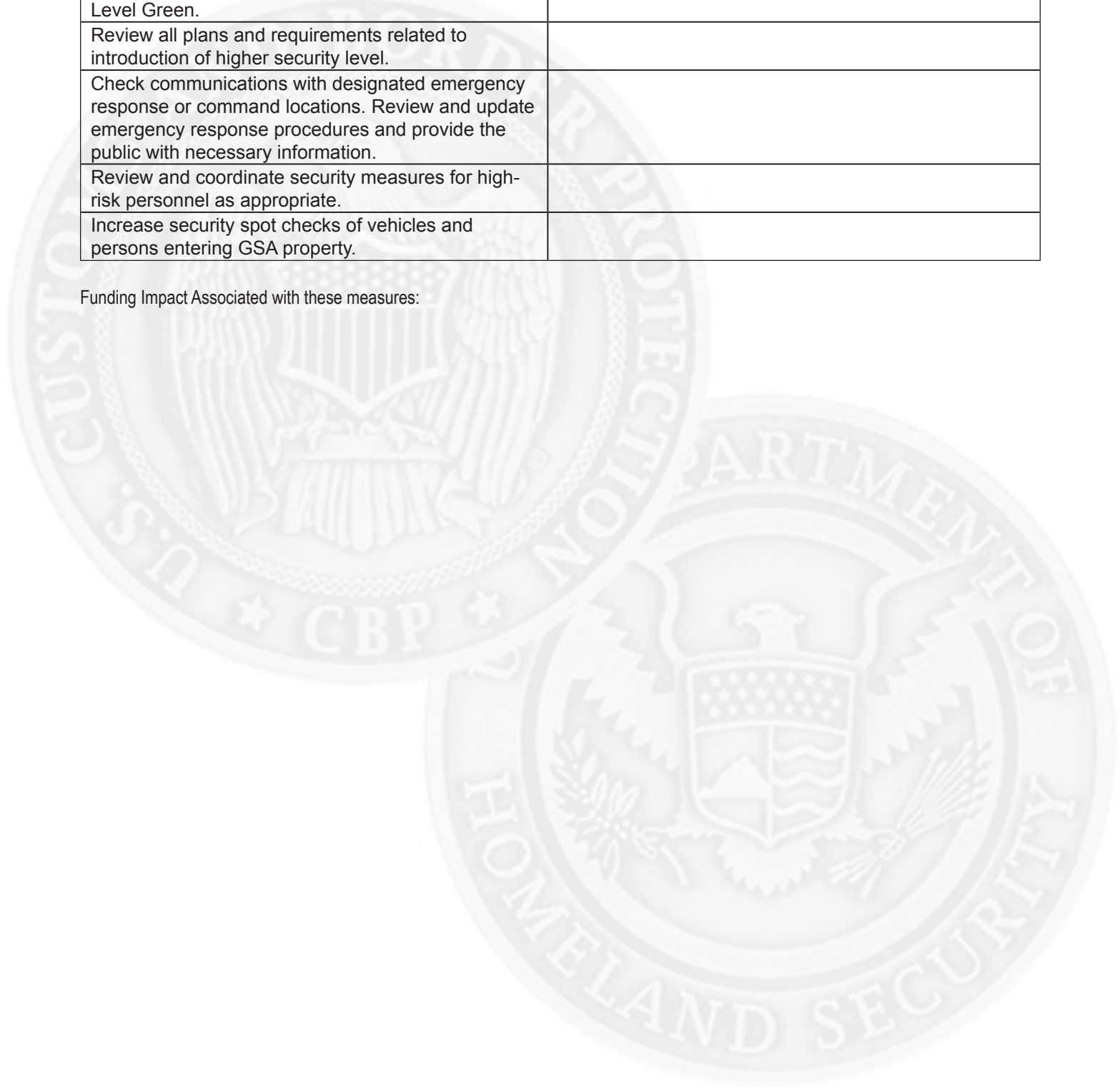
[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

Blue Protective Measures	
General Guidance	Building Specific Actions
Continue, or introduce, all measures listed in Alert Level Green.	
Review all plans and requirements related to introduction of higher security level.	
Check communications with designated emergency response or command locations. Review and update emergency response procedures and provide the public with necessary information.	
Review and coordinate security measures for high-risk personnel as appropriate.	
Increase security spot checks of vehicles and persons entering GSA property.	

Funding Impact Associated with these measures:



[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

Yellow Protective Measures	
General Guidance	Building Specific Actions
Continue, or introduce, all measures listed in Alert Level Blue and warn customers of any other potential form of terrorist attack.	
Keep all personnel involved in implementing antiterrorist contingency plans on call.	
Check plans for implementation of the next alert level.	
At the beginning and end of each workday, as well as at other regular and frequent intervals inspect the interior and exterior of buildings in regular use for suspicious packages.	
In the early stage inform the Building Security Committees of actions to be taken. Explain reasons for actions.	
Increase contacts with individuals responsible for activities such as child care centers, and agencies with a high amount of personal threat reporting, to build confidence among staff.	
Make customers aware of the general situation in order to stop rumors and prevent unnecessary alarm.	
Move unchecked cars and objects (i.e. crates, trash containers) at least 100 feet from buildings. Use other measures where distance cannot be achieved.	
Request personnel who handle mail and deliveries to scrutinize incoming material (above the regular examination process) for letter or parcel bombs.	
Implement additional security measures for high-risk personnel as appropriate.	
Consult local authorities on threat and mutual antiterrorism measures.	
Increase surveillance of critical facilities.	
Implement appropriate contingency and emergency plans.	
After normal duty hours require all employees and visitors sign the building register upon entering and leaving the building.	

Funding Impact Associated with these measures:

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

Orange Protective Measures	
General Guidance	Building Specific Actions
Continue, or introduce, all measures listed in Alert Level Yellow.	
All FPS personnel are subject to emergency recall.	
Limit facility access points to the absolute minimum.	
Protect all designated vulnerable points.	
Strictly enforce control of entry. Randomly search vehicles.	
Increase patrol tempo of security guards, police officers, and Inspectors.	
Erect barriers and obstacles to control traffic flow.	
Consult local authorities about closing public streets that might make facilities more vulnerable to attacks.	
Restrict outside vehicular parking to 300 feet of the facility. Use other measures where distance cannot be achieved.	
Coordinate necessary security efforts with armed forces and other law enforcement agencies.	

Funding Impact Associated with these measures:

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

Red Protective Measures	
General Guidance	Building Specific Actions
Continue, or introduce actions listed in Alert Level Orange.	
Augment security guards as necessary.	
Search all vehicles and their contents before allowing entrance to the building.	
Control access and implement positive identification of all individuals with no exceptions.	
Thoroughly search all suitcases, briefcases, and packages brought into the building.	
Make frequent checks of the exterior of buildings and parking areas under GSA jurisdiction.	
Coordinate the possible closing of public streets and facilities with local authorities.	
Activate the facility OEP.	
FPS should assign emergency response personnel and pre-position specialty trained teams. Monitor, redirect, and/or constrain transportation systems.	
Increase and/or redirect personnel to address critical emergency needs.	
Consider closing of facility.	

Funding Impact Associated with these measures:

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.



Occupant Emergency Plans

Guide for Development, Implementation and Maintenance



U.S. Customs and
Border Protection

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Occupant Emergency Plan (OEP) Guide: Introduction

In the post-911 world, emergency preparedness at work, at home, and in the community is everyone's responsibility. Planning for workplace emergencies is critical to reducing risk to personnel and property. Individuals need to understand what emergencies could occur and what actions to take if something happens. Life safety, communication, efficiency, and roles and responsibilities are critical components to accomplishing facility safety and preparedness. Emergencies can be handled routinely if building occupants are familiar with established procedures and know pertinent emergency contact information.

- Emergency plans are required for virtually all buildings. The Occupational Safety and Health Administration (OSHA) requires that an emergency action plan¹ be developed and implemented if fire extinguishers are required or provided in the workplace and if anyone will be evacuating during a fire or other emergency. The Federal Management Regulations 41 FMR 102-74 requires that all Federal departments and agencies comply with the occupational safety and health standards established in the Occupational Safety and Health Act of 1970 and develop and implement occupant emergency plans.

To be most effective at protecting life and property, all emergency plans should:

- Provide clear instruction on roles and responsibilities for all aspects of the preparedness spectrum from prevention and protection to response and recovery.
- Use an all-hazards approach that includes procedures to handle a wide range of hazards and threats that could affect a building such as medical emergencies, bomb threats, suspicious packages, and natural disasters.
- Meet the specific characteristics, needs, and criteria for each facility². For example, location-specific procedures are added to address unique threats or hazards such as hazardous materials spills or releases of radioactive materials.
- Involve coordination with local emergency responders and law enforcement to address multi-jurisdictional issues regarding mass care, sheltering, and evacuation.

This Occupant Emergency Plan Guide is a tool that should be used in the construction and update of OEPs. It provides assistance in the planning, development, and implementation of facility-specific OEPs. Pairing this OEP Plan Guide with the OEP Template, emergency planners should establish a foundation from which an OEP directly addresses protection goals and objectives.

¹ Refer to OSHA's website for detailed information and instructions for preparation of emergency action plans. <http://www.osha.gov/SLTC/e-tools/evacuation/index.html>

² For small, one-level facilities with fewer than 500 employees, emergency information may be entered on GSA Form 3415, Occupant Emergency Plan (abbreviated).

Table of Contents

- Part 1: Prepare to Write the OEP
 - 1.0 Get Organized
 - 2.0 Gather Information on Threats and Capabilities
 - 3.0 Coordinate with Internal and External Groups
 - 4.0 Address Special Considerations
 - 5.0 Enhanced Protection for Increased Threat
 - 6.0 Post-Incident Recovery
 - 7.0 Completing the OEP

Part 2 Write the OEP

- Part 3 Implement and Maintain the OEP
 - 1.0 Integrate Plan into Facility Operations
 - 2.0 Training, Drills, and Exercises
 - 3.0 Evaluate and Modify OEP

Attachments

- 1. General Responsibilities of the OEO Teams
- 2. Sample Emergency Procedures
- 3. Reviewing OEP Procedures and Identifying Best Practices
- 4. Additional Resources

Acronyms

I. PART 1: PREPARE TO WRITE THE OEP

Before writing an OEP, it is important to get organized by establishing a planning team to encourage participation and personal investment in the process, enhance the visibility and stature of the planning process, and provide for a broad perspective on related issues. The size of the planning team will depend on the facility's operations, requirements and resources.

1.0 Get Organized

The responsibility for managing in emergencies in a Federally owned or leased facility is with the Designated Official, who is the highest ranking official of the primary occupant agency, or a designee selected by mutual agreement of occupant agency officials. The Designated Official must supervise the development of the OEP and the staffing and training of the Occupant Emergency Organization (OEO). The OEO coordinates all emergency response procedures in each facility. The OEO should:

- Be limited in size. Carefully determine how many positions are needed and define their duties clearly. It is important to have enough help in an emergency, but too many people could get in the way and prevent fast, efficient action.
- Consist of, and use, the existing hierarchy of the occupant agencies. Officials heading agencies on a day-to-day basis should assume leadership positions during an emergency since they reflect an agency's greatest leadership, experience, and skill and have ultimate responsibility for the safety and well being of their employees. Members should be accountable, active individuals that will carry out procedures, training, and associated duties for emergency preparedness.
- Consist of members selected by position, not by name. This automatically allows for continuity since positions are typically filled when the incumbent is absent. The acting official assumes the incumbent's role in the emergency organization as well. Selection by position also eliminates the need for assigning alternates.
- Be made up of three primary teams that, together, comprise the building's Emergency Response Team (ERT)³. Each team is discussed in the following sections and general responsibilities for all members of these teams are included in Attachment 1.

OEO personnel should be provided with visual identifiers such as colored safety hats and/or armbands. Occupants should be familiar with these identifiers and their significance.

1.1 Command Center Team

The Command Center Team (CCT) directs all emergency operations from the building's Command Center. CCT members in a large facility, would include:

- Designated Official (DO) – the highest-ranking official of the primary occupant agency; or alternatively, a designee selected by mutual agreement of occupant agency officials. Responsible for activating the plan in all emergencies during normal duty hours.
- Occupant Emergency Coordinator (OEC) – the official appointed by the Designated Official and serves as the primary assistant to the Designated Official to ensure the continued viability of the OEP and its organization. During emergencies the OEC operates the

³The Building Security Council (BSC) is a separate body comprising representatives from each Agency/tenant in a facility. The BSC coordinates with FPS personnel to disseminate security updates and notifications, and to ensure tenant compliance with safety requirements. The BSC is not directly involved with ERT activities, but supports its mission through compliance, as all tenants are required to follow OEP procedures. The DO serves as the linkage, serving on both bodies. Individual BSC members can also serve on both bodies.

Command Center.

- Floor Team Coordinator – supervises and expedites the planned and controlled movement of all building occupants in an emergency.
- Damage Control Team Coordinator – controls dangerous conditions until further help arrives to assess potential and real damage.
- Medical Coordinator – the head of the Health and First Aid Unit and is responsible for training and equipping all employees assigned to perform first aid in an emergency.
- Administrative Officer – records emergency procedures and activities.
- Technical Advisors – occupants familiar with the building’s utilities and mechanical systems or other areas of expertise who advise the DO and OEC.

In a small facility, some positions, such as Administrative Officer, Medical Coordinator, and Floor Team Coordinator, may not be needed or one person could perform several functions.

1.2 Floor Teams

Floor Teams are assigned to each floor of a facility. In a large facility, a typical Floor Team would include:

- Floor Monitors – supervisory personnel selected by the individual Tenant Agency. During a supervisor’s absence, there should be an acting supervisor who should assume the Floor Monitor responsibility. In agencies where the supervisory employee is frequently assigned outside the office, a responsible, conscientious, non-supervisory staff employee may be selected. Floor monitors act in several different capacities, depending on the emergency.
- Floor Area or Wing Monitors – assigned for each major area of the floor.
- Stairwell Monitors – support the Area/Wing Monitors by controlling movement of persons on stairways.
- Elevator Monitors – support the Area/Wing Monitors; one is assigned for each floor where elevators may be captured.
- Exit Monitors – support floor monitors for street and ground level.
- Monitors for Disabled – employees appointed by the floor wardens to assist people with special needs during emergencies. Where possible, two monitors should be assigned to each person. In an emergency, monitors are responsible for remaining with the person throughout the emergency and assisting in their evacuation, following the instructions of the command center and/or the floor warden.

1.3 Damage Control Team

The Damage Control Team consists of the Property Manager and other individuals familiar with the facility’s construction, equipment, and overall operating system. Team members report to the Damage Control Coordinator.

- The Property Manager provides information, guidance, and advice on establishing and maintaining the OEO; assists the Designated Official in recruiting qualified personnel for technical services; and is responsible for designating and supervising the building

[RETURN TO TOP](#)

maintenance supervisor.

- Building maintenance supervisor controls building utilities during an emergency. Under the direction of the Property Manager, the building maintenance supervisor:
 - Establishes a plan to attend mechanical devices; ventilation, water, gas, and steam valves; power switches, elevators, etc., during an emergency.
 - Provides training for emergency situations and coordinates training for bomb searches for building mechanical personnel.
- Ensures that building mechanical personnel know procedures for all emergency situations.

II. PART 2.0: GATHER INFORMATION ON THREATS AND CAPABILITIES

The next step is to become familiar with the security posture of the facility and landscape of its surroundings. Gather and review existing reports and other sources of information on the facility's current security posture, local response capabilities, and possible areas for improvement. [Table 1](#) provides a detailed list of sources of information. Since conditions change within and surrounding a facility, consider the following at a minimum to further validate information:

What are nearby facilities or structures that could add to the threat level of a facility?

Examples include:

- Federal/State/local government offices; post offices, law enforcement stations, fire/rescue, town/city hall, and local mayor/governor's residences; judicial offices and courts.
- Recreation facilities including sports arenas, theaters, malls, and special interest group facilities.
- Military installations.
- Chemical plants, industrial complexes, utilities, nuclear plants, or rail yards that manufacture, use, transport, store, or dispose of large amounts of hazardous materials.
- Road, rail, or water transportation arteries on which hazardous materials are transported within a mile from the facility. For example:
 - Traffic - Roads/tunnels/bridges carry large volumes of traffic; points of congestion that could impede response or place citizens in a vulnerable area and time of day and day of week this activity occurs.
 - Trucking and Transport Activity - Location of hazardous materials cargo loading/unloading facilities; vulnerable areas such as weigh stations and rest areas this cargo may transit.
 - Waterways - Pipelines and process/treatment facilities; berths and ports for cruise ships, roll-on/roll-off cargo vessels, and container ships; international (foreign) flagged vessels (and cargo they carry) that conduct business in the area.
 - Airports - Carriers, flight paths, and airport layout; location of air traffic control tower, runways, passenger terminal, and parking areas.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- Trains/Subways - Location of rails and lines, interchanges, terminals, tunnels, and cargo/passenger terminals; any hazardous material that may be transported by rail.

Does the geographical location (city, state) increase the threat to the facility from natural hazards?

Examples include: Fault lines - earthquakes; coastal locations - hurricanes/tsunamis; tornado alley, etc.

What police, rescue, and hazardous materials response is available to the facility?

Examples include:

- Location and response time of the nearest fire department and hazardous materials team.
- Local rescue, detection, identification, and decontamination capabilities.
- Potential of a chemical, biological, or radiological incident that could affect the facility from internal sources. Examples include: Laboratory areas and storage areas.

Are there services provided within the building that could contribute to overall risk or require specialized considerations? Examples include: Childcare centers and retail space.

What are facility critical products, services, and operations? Examples include:

- Products and services provided by suppliers.
- Services such as electrical power, water, sewer, gas, telecommunications, transportation;
- Operations equipment, and personnel vital to continued functioning of facility.
- Once all the information is gathered and analyzed, assess available resources and ability to respond to each potential emergency:
 - Do we have the needed resources and capabilities to respond?
 - Will external resources be able to respond to use for this emergency as quickly as we may need them, or will they have other priority areas to serve?
- If the answer is no, identify what can be done to correct the problem. Examples include:
 - Develop additional emergency procedures
 - Conduct additional training
 - Acquire additional equipment
 - Establish mutual aid agreements
 - Establish agreements with specialized contractors

Table 1: Sources of Information

Internal Plans and Policies	<ul style="list-style-type: none"> ● Evacuation Plan ● Fire Protection Plan ● Code Adam Activation Procedures ● Safety and Health Program ● Environmental Policies ● Security Procedures ● Insurance Programs ● Finance and Purchasing Procedures 	<ul style="list-style-type: none"> ● Employee Manuals ● Hazardous Materials/WMD Plan ● Process Safety Assessment ● Risk Management Plan ● Capital Improvement Program ● Mutual Aid Agreements ● Facility Closure Policy
Codes and Regulations	<ul style="list-style-type: none"> ● Occupational Safety and Health Regulations ● Environmental Regulations ● Fire Codes 	<ul style="list-style-type: none"> ● Transportation Regulations ● Zoning Regulations ● Tenant Policies ● Seismic Safety Codes
Information to Maintain in the Command Center	Emergency Call Lists – wallet sized if possible, of all persons on and off site who would be involved in responding to an emergency, their responsibilities, and their 24-hour contact numbers.	
	Building and site maps that include:	
	<ul style="list-style-type: none"> ● Location of each building (include name of building, street name, and number) ● Utility shutoffs ● Water hydrants, main valves, lines ● Gas main valves and lines ● Electrical cutoffs and substations ● Storm drains and sewer lines ● Floor plans 	<ul style="list-style-type: none"> ● Alarm and enunciators ● Fire extinguishers and suppression systems ● Exits, stairways, designated escape routes, and restricted areas ● Hazardous materials (including cleaning supplies and chemicals) ● High-value items

III. 3.0 COORDINATE WITH INTERNAL AND EXTERNAL GROUPS

- Government agencies, community organizations, and utilities are all involved with, and affected by, a facility’s OEP program and operations. Communication with these groups is important in orchestrating an effective emergency response strategy.
- There are many external resources that could be needed in an emergency. In some cases, formal agreements may be necessary to define the facility’s relationship. In other cases, it

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

is important to have open lines of communication to share information on possible threats and vulnerabilities.

- **Sample External Groups:**
 - **Community Emergency Management Office**
 - **Mayor or Community Administrator's Office**
 - **Local Emergency Planning Committee (LEPC)**
 - **Fire Department**
 - **Police Department**
 - **Emergency Medical Services/Hospitals**
 - **American Red Cross/Community Services**
 - **HAZMAT Response**
 - **National Weather Service**
 - **Public Works Department/Utilities**
 - **Insurance Carriers**

Discuss coordination and development of the facility OEP with appropriate external groups. While their official approval may not be required, they will likely have valuable insights and information to offer. Some considerations for external coordination include:

- What are their plans and available resources for preparedness and response to potential emergencies?
- What are State and local requirements for reporting emergencies?
- Determine protocols for turning control of a response over to outside agencies. For example:
 - Establish lines of communication with outside responders
 - Decide gate or entrance for responding units use; where they will go and to whom they will report
 - Determine what kind of identification authorities will require from key personnel to allow entrance during an emergency
 - Under the Incident Command System (ICS) and National Incident Management System (NIMS), who becomes the official in charge and when
 - In an Incident of National Significance, what external agency is responsible for emergency support under the National Response Plan (NRP)

Coordination with internal contacts is equally as important. Examples of internal resources and capabilities include:

- Personnel – fire brigade, HAZMAT response team, emergency medical services, security,

emergency management group, evacuation team, public information officer

- Equipment – fire protection and suppression equipment, communications equipment, first aid supplies, emergency supplies, warning systems, emergency power equipment, decontamination equipment, equipment to evacuate occupants with disabilities
- Facilities – command center, media briefing area, shelter areas, first stations, sanitation facilities
- Organizational Capabilities – training, evacuation plan, employee support system
- Backup Systems – arrangements with other facilities to provide for:
 - Payroll
 - Communications
 - Emergency Power
 - Shipping and Receiving
 - Information Systems Support
 - Recovery Support
 - Method or equipment to account for location of occupants
 - Employee Skills (medical, engineering, communications, foreign language) that might be needed in an emergency

Maintain contact with internal department/agency offices, and communicate with them to establish OEP activation procedures and the primary and alternate means of communication that will be used. The decision to activate is based upon the best available information, including an understanding of local tensions, the sensitivity of target agency(ies), and previous experience with similar situations. Advice shall be solicited, when possible, from the GSA building manager, appropriate Federal Protective Service official, and Federal, State, and local law enforcement agencies.

IV. 4.0 ADDRESS SPECIAL CONSIDERATIONS

To ensure full preparedness and successful OEP activation and administration, a number of logistical considerations should be coordinated and accounted for. Each is discussed in the following sections.

4.1 Primary and Alternate Command Centers

Emergency operations are directed from a Command Center. It should be centrally located and easily accessible for effective communication and control with good communications capability (e.g., two telephones, portable radios and pagers, messengers). An alternate Command Center location is used if the primary location is incapacitated, or if evacuation is necessary. Special consideration must be made for rapid transportation of team members from their workstations to the Command Center and for quick notification of team members of an emergency.

4.2 Evacuation and Shelter Facilities

When evacuation of the facility is necessary, rally points are established where occupants convene, and are accounted for, to ensure that the facility has been completely evacuated. In some cases, it may be necessary to arrange for alternate facilities to provide shelter for evacuees. If evacuees are to remain in the shelter location for an extended period of time, other considerations may involve arranging for medical support, food and transportation.

4.3 Primary and Alternate Means of Communications

A primary and alternate means of communications must be available to activate the occupant emergency organization, inform building occupants of the nature of an emergency and what actions to take, to coordinate activities during an emergency.

- All building occupants must understand how to operate and respond to the alarm system to avoid confusion and delay in reporting fire or other emergencies. The fire alarm system is used to initiate immediate evacuation of the building. Drills are scheduled to test the OEP functions and familiarize plan members with emergency procedures of the Plan. These systems are tested on a regular schedule to ensure that the equipment is working properly. An oral announcement may be used to warn of other emergency or non-emergency situations. These could be, but not limited to: earthquakes, floods, and windstorms, explosions, civil disturbances, bomb threats, demonstrations and hostage situations.
- In most cases, the building's fire alarm system may not be used as a means of notifying the organization and the occupants without approval of the Building Manager and or the Fire Department. As such, appropriate use of telephones, public address systems, and/or messengers may prove more feasible. If telephones are used, a Communications Coordinator should be appointed by the Administrative Officer to set up a system of contacting all members of the emergency organization. The Administrative Officer/person should also be responsible for updating lists of telephone numbers. Multilevel buildings may have emergency telephone systems for coordinating emergency activities. However, most buildings must rely on the normal telephone system, the public address system, the fire alarm, and messengers.

4.4 Child Care Centers

The Designated Official and FPS Inspectors should work with the director of a childcare center in a Federal facility to develop and post emergency response procedures. Center staff should know whom to contact in the event of a medical emergency, how the center will be notified of a fire or other danger that may require evacuation, the location of fire alarm boxes and fire extinguishers, the primary and secondary evacuation routes, and the locations of safe areas.

4.5 Disabled Occupants

Occupants with disabilities who need assistance during an emergency should be involved in planning to inform appropriate personnel of their needs, including exactly what kind of assistance is required. Consider the following when evaluating the facility's capacity to address occupants with disabilities during an emergency:

- More time may be needed to evacuate disabled individuals.

[RETURN TO TOP](#)

- Audible warnings and emergency instructions are not effective for deaf or hard of hearing occupants and, as such, other notification means are needed.
- Blind or partially sighted occupants need to depend on others to lead them during an evacuation.
- Occupants in wheelchairs may require assistance to evacuate the building.
- Persons with mental disabilities may be unable to understand the emergency and could become disoriented or confused about the proper way to react.
- Respiratory illnesses may become aggravated by stress.
- Emergency, oxygen and respiratory equipment may not be readily available.
- Medication regimen of occupants with serious conditions may be interrupted.

Other examples of people who do not fit the legal definition of a person with a disability, but who may need assistance or special planning for emergencies include the elderly, pregnant women, and people who are obese. There may also be people with temporary or intermittent needs. Contact local emergency services to determine what evacuation equipment (such as evacuation chairs) they can offer. It is important to provide instruction on the use of evacuation chairs to affected occupants in an actual emergency.

4.6 Protocols for Nights/Weekends/Holidays

- In the event of an emergency at night, over the weekend, or on a holiday, the senior Federal official present should act as the DO and initiate appropriate action. This person will need to coordinate with the senior FPS Officer, contract guard on the premises and/or with appropriate maintenance personnel.
- Procedures must also be spelled out and responsibilities assigned for handling emergencies that occur during nights, weekends, and holidays. The OEO's members and their titles and telephone numbers should be noted on forms.

4.7 Emergency Telework

Telework⁴ is simply a way of getting work done from a different location. It can serve multiple purposes – and have multiple benefits – when it is implemented effectively in an organization and, as such, should be part of agency emergency planning. The National Strategy for Pandemic Influenza Implementation Plan references the benefits of using telework to slow the spread of disease by keeping face-to-face contact to a minimum (often referred to as “social distancing”) while maintaining operations as close to normal as possible. Telework can also help agencies retain functionality as infrastructure issues and other challenges make the main work site difficult to access.

⁴ The Office of Personnel Management defines telework as “work arrangements in which an employee regularly performs officially assigned duties at home or other work sites geographically convenient to the residence of the employee.”

V. 5.0 ENHANCED PROTECTION FOR INCREASED THREAT

Facility-specific steps should be established for increasing protection based on changes to threats that could potentially affect individual facilities. For increases in protection associated with terrorist threats, the Homeland Security Advisory System (HSAS) is a color-coded [terrorism](#) threat level system designed to target protective measures when information specific to an individual sector or geographic region is received. It combines threat information with vulnerability assessments and provides communications to public safety officials and the public. The scale consists of five color-coded threat levels to reflect the probability of a terrorist attack and its potential gravity. Each level triggers specific actions by Federal agencies and State and local governments and affects the level of security at government facilities.

VI. 6.0 POST-EMERGENCY RECOVERY

Facility recovery operations are intended to restore essential services and resume normal operations as quickly and safely as possible. To facilitate post-emergency recovery, consider the following during planning:

- Identify long-term implication of interruption to normal services
- Make contractual arrangements with vendors for such post-emergency services as records preservation, equipment repair, earthmoving or engineering
- Meet with insurance carriers to discuss property and business resumptions policies
- Determine critical operations and make plans for bringing those systems back on-line. The process may entail:
 - Repairing or replacing equipment
 - Relocating operations to an alternate location
 - Contracting operations on a temporary basis
- Establish procedures for:
 - Ensuring the chain of command
 - Maintaining lines of succession for key personnel
 - Moving to alternate headquarters (include these considerations in all exercise scenarios.)
- Determine the audiences that may be affected by an emergency and identify their information needs. When emergencies expand beyond the facility, the community will want to know the nature of the incident, whether the public's safety or health is in danger, what is being done to resolve the problem and what was done to prevent the situation from happening.
- Maintain complete and accurate records at all times to ensure a more efficient emergency response and recovery. Certain records may also be required by regulation or by your insurance carriers or prove invaluable in the case of legal action after an incident.

[RETURN TO TOP](#)

- Administrative actions include many that are covered by a well written, coordinated, and implemented OEP. For example:
 - Maintain training records
 - Maintain all written communications
 - Document drills and exercises and their critiques
 - Acquire equipment
 - Stockpile supplies
 - Designate emergency facilities
 - Establish training facilities
 - Establish mutual aid agreements
 - Prepare a resource inventory

VII. 7.0 COMPLETING THE OEP TEMPLATE

This section provides step-by-step guidance for completing the OEP Template.

OEP Cover Page – Each OEP is unique to a facility. Enter building name, address, and date information to replace generic text.



Emergency Notification Numbers - All building occupants should know whom to contact in case of emergency. Enter building-specific emergency notification numbers. Note that for GSA owned or leased facilities, the Federal Protective Service must be notified of any emergency situation. Other department/agency facilities may replace this with another provider as appropriate.

Emergency Notification Numbers

Site:	
Medical Emergency:	
Security Emergency:	
National Disaster Hotline:	1-877-687-6872

Responsible Officials' Sign-Off Sheet - OEO officials (e.g., the designated official and the occupant emergency coordinator) must certify their participation in the OEP development and verify their understanding of emergency procedures affecting the facility and employees within for which they are responsible.

Additional officials may be added as appropriate.

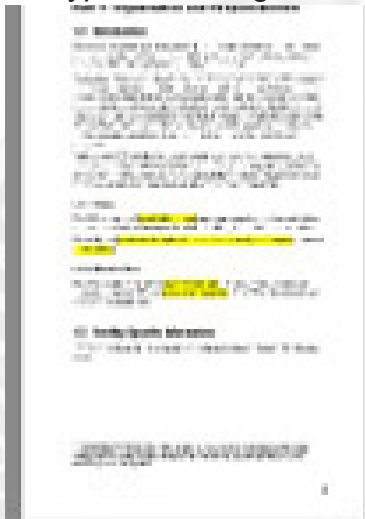
Responsible Officials' Sign-Off Sheet

Signature: _____ Date: _____

Signature	Date	Signature	Date

Part 1: Organization and Responsibilities

Introduction - The introduction gives management a brief overview of the purpose of the OEP, the facility’s emergency management policy, authorities and responsibilities of key personnel, the types of emergencies that could occur, and where response operations will be managed.



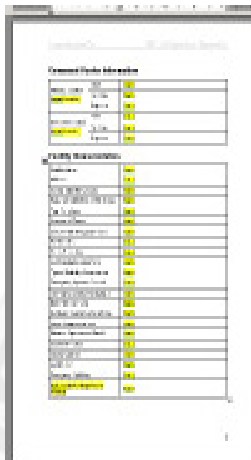
Replace highlighted text with facility specifics as follows:

Scope

- [insert building name]
- [insert brief description of number of stories and type of complex]
- [insert address]
- Effective Date
- [insert effective date]
- [name of building/facility]

Facility-Specific Information – consists of three forms that provide information on the command center, facility characteristics, and occupants.

- Command Center - information with primary and alternate locations and addresses.
- Facility Characteristics - potentially impacting emergency response procedures.
- Occupants Form - outlines the primary occupant agency, number of occupants, and lists occupants by floor, and subsequent contact information and special considerations such as hazardous materials use and storage.



Occupant Emergency Organization (OEO) – provides an overview of the structure and purpose of the OEO and an overview of responsibilities of the various components of the OEO.

- Replace highlighted text with facility specifics as follows:
 - [Insert what is used...colored safety hats and/or armbands].
- Throughout this section, modify or delete text to reflect facility-specific structure.



Part 2: Activation and Contact Information

Provides the protocol for activating the OEP. Throughout this section, modify or delete text to reflect facility-specific structure pertaining to:

- Who makes the decision to activate the OEP?
- How is the decision made?
- Actions if there is immediate danger to persons or property



Facility Emergency Contact Information - Replace highlighted text with name, title, desk and mobile telephone numbers for facility contacts as follows:

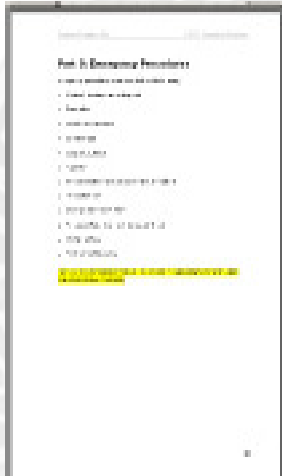
- General Services Administration
- Federal Protective Service
- Command Center Team (CCT)
- Floor Team (FT)
- Damage Control Team (DCT)

Throughout this section, modify or delete text to reflect facility-specific structure.



Part 3: Emergency Procedures

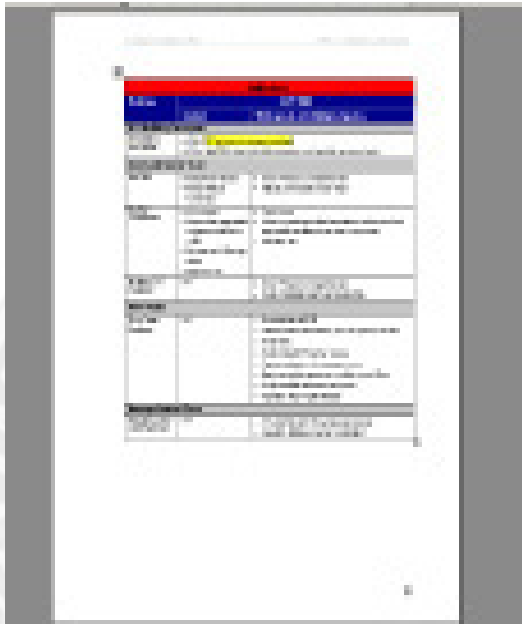
The OEP Template outlines proposed actions to be taken in a number of building-related emergencies. Table 2-1 provides a list of types of emergencies to consider in facility-specific planning. Modify text to reflect facility-specific emergency procedures and contingency plans. Replace yellow highlighted text with facility-specific information.



Attachment 2 provides a series of sample emergency procedures that can be used as a starting point. Following are some additional points to consider for select procedures:

Medical (Attachment 2-1)

- OEO members and other identified occupants may be the fastest source of first aid/ cardiopulmonary resuscitation. All FPS officers are qualified in first aid/CPR.
- The facility’s health unit, if there is one, can usually provide immediate medical attention. Local physicians and emergency medical unites are normally closer than a hospital; the area should be surveyed to determine their availability, and their telephone numbers should be on the Emergency Call List. Local police, fire, and rescue squads can provide ambulance services and paramedics; police and fire department personnel can also maintain order during an emergency requiring large-scale medical services.



Evacuation (Attachment 2-2)

- All occupants should know the locations of fire alarm boxes and extinguishers, as well as how/when to use them, and the procedures to follow when the alarm is sounded. Occupants should know whom to notify after an alarm as been sounded so the Command Center Team can be activated.
- FPS officers and typically members of the Disaster Control Team are trained in fighting small fires. Once the fire department arrives, the fire official in charge will assume command.
- Orderly evacuation is the simplest and most reliable action, and is used as a response to relatively common incidents such as fire drills and alarms, and also to more serious emergencies such as bomb threats. In most situations where an airborne release originates from a source inside a building, evacuation follows. Evacuation considerations include: Evacuation may lead to other risks, by taking the occupants from the physically secure environment of the building into the streets. Evacuation routes may also be hazardous in that they may expose individuals to contaminated areas as they exit the facility. Properly trained Floor Team Coordinators, Area/Wing Monitors, Stairway Monitors, and Elevator Monitors can lead the safest and fastest evacuation of a building. FPS officers and/or local police can control traffic and crowds during an evacuation. If evacuation is ordered because of a fire, the local fire department official in charge will assume command.
- For childcare center evacuation:
 - Become familiar with the location of all stairways and exits, and the nearest building fire alarm manual pull stations, duress alarms and their operation.
 - All personnel members must be trained on the proper fire protection and evacuation

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

practices.

- Personnel should not attempt to secure or recover items of clothing or personal property after an alarm has sounded. The facility should not be reentered until the incident commander gives the all clear.
- In case of emergency or drill, all personnel should leave the building in an orderly manner - Walk, Don't Run. The personnel should search their rooms in the Center, closing all doors before leaving. Additionally, the Director or other assigned personnel will search all areas within the Center and ensure that all occupants have been safely evacuated.
- Take attendance and immediately proceed to the Safe Haven (enter appropriate, detailed address/location) as directed by the Center Director or designee
- Determine if parents should be notified and/or asked to pickup children. The decision to have parents pick up their children will be made based on expected time out of the Center or the nature of the emergency.
- Physically challenged children will be provided with assistance to help them exit the building. Infants will be evacuated in designated evacuation cribs.

Table 2-1: Types of Emergencies to Consider

Historical types of emergencies that have occurred	<ul style="list-style-type: none"> • Fires • Severe Weather • Hazardous Material Spills • Transportation Accidents • Earthquakes 	<ul style="list-style-type: none"> • Hurricanes • Tornadoes • Missing child • Utility Outages • Prohibited access to the facility
Geographic	Proximity to: <ul style="list-style-type: none"> • Flood plains, seismic faults, and dams • Companies that produce, store, and use/transport hazardous materials • Major transportation routes and airports • Nuclear power plants 	
Technological	<ul style="list-style-type: none"> • Safety system failure • Telecommunications failure • Computer system failure 	<ul style="list-style-type: none"> • Power failure • Heating/cooling system failure • Emergency notification system failure
Human Error	<ul style="list-style-type: none"> • Poor training • Poor maintenance • Carelessness 	<ul style="list-style-type: none"> • Misconduct • Substance abuse • Fatigue
Physical	<ul style="list-style-type: none"> • Ruptured gas mains • Water damage • Smoke damage • Structural damage • Pandemic Outbreak 	<ul style="list-style-type: none"> • Explosion • Building collapse • Trapped persons • Chemical release • Air or water contamination

Hazardous Substance (Attachment 2-3)

- Supervisors are required to label all hazardous chemicals in their workplaces and list them on Material Safety Data Sheets (MSDSs), and to develop, publish, and implement a hazard communication program, inclusive of employee training.⁵
- The Designated Official must maintain an inventory of hazardous materials used in chemical laboratories and hazardous material storage areas in the building. This inventory should include the following information for each chemical that poses a potential health or physical hazard:
 - Substance name and trade name
 - National Stock Number/Chemical Abstracts Service Number, if applicable
 - Name and location of user
 - Container size
 - Quantity of chemical normally in use and stored
- The Chemical Transportation Center provides 24-hour information on handling accidents in the transportation of chemicals, as the official “Hotline” for this type of emergency at 1-800-424-9300.

Bomb Threat (Attachment 2-4)

- Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Provide occupants with instruction and a checklist positioned by the telephone so that they may act quickly, but remain calm and obtain appropriate information.
- FPS officers and local police can help in training for bomb searches and provide leadership during a search. The bomb disposal unit of the local police would, in most instances, provide the quickest response for defusing or otherwise disposing of a bomb. A sample bomb threat checklist is also included in Attachment 2-4.
- The evacuation of occupants may be necessary.

⁵ The Hazard Communication Standard (29 CFR 1910.1200) establishes uniform requirements for evaluation of all hazardous chemicals used in U.S. workplaces and communication of this information to the appropriate personnel. This Standard was designed to ensure that (1) employers receive the information they need to inform and train employees properly and to design and put in place employee protection programs, and (2) that employees receive necessary hazard information so they can participate in the development of protective measures in their workplaces and support them once they are in place.

Suspicious Object (Attachment 2-5)

- Because of their familiarity with the space where they work, occupants can most easily spot something that does not belong there. They should be warned, however, not to touch suspicious objects, and to report them immediately upon discovery to the FPS.
- The evacuation of occupants may be necessary.
- Prepare announcements to be used if necessary as follows:
 - *May I have your attention please? May I have your attention please? May I have your attention please?*
 - *We have identified a suspicious package on the ____ floor.*
 - *Occupants of the ____, ____, and ____ floor(s) (1 above and 1 below) are required to evacuate until the emergency is over. (REPEAT)*
 - *Please walk to the nearest exit and report to your floor's designated evacuation area.*
 - *Only the affected floors need to evacuate.*
 - *Do not use the elevators, please proceed to stairways. (REPEAT)*
- When the "All Clear" is given:
 - *May I have your attention please? May I have your attention please? May I have your attention please?*
 - *The emergency on the ____ floor is now over.*
 - *Occupants of the ____, ____, and ____ floors may return to their work areas.*

Shelter in-Place (SIP) (Attachment 2-6)

- When dangerous airborne contaminant releases originate from outside a building, evacuation is typically not appropriate. During such events, it may be necessary to Shelter-in-Place for a short period of time until local authorities can arrive to assess circumstances. Partnering with local authorities is crucial because OEPs should not conflict with the plans of local community first responder protocol. In many locations, particularly outside major population centers, local officials may not recommend SIP planning because the risks in these areas do not justify this course of action.
- There may be times when building occupants are required to remain inside a building if local community recognized experts determine that:
 - It is safer than outside
 - Releasing a large number of employees onto the roads and public transportation will only add to the confusion and panic, or
 - There is likely exposure to some hazard or harm, and releasing employees will spread the hazard to others, including family members.

- It is important to develop the building's proactive SIP plan with employees and other authorities to maximize the cooperation of employees with the SIP plan. It is recommended that a group consisting of key representatives be formed to develop building-specific SIP plans based on the following considerations/steps.

Step 1 Review Building's Vulnerability Assessment Reports - Review the executive summary of the building's Vulnerability Assessment reports, related security Threat Assessment reports, and the building's OEP.

Step 2 Identify Building Features - The purpose of identifying the existing features is to gather information about the ventilation system and the characteristics that determine the building's protective capability. This information is required for the development of each building's SIP plan by Property Management (PM) and building operating personnel. This assists in the development of HVAC control protocols for airborne contaminant releases. This plan should describe the operation of the building's heating, ventilation, and air conditioning (HVAC) systems during a SIP event.

Step 3 Identify Features Increasing Building Vulnerability - Identify features that make the building vulnerable to airborne contaminant releases originating from outside the building.

Step 4 Identify SIP Safe Zones - Based on the above SIP information, building authorities should identify a list of possible SIP safe zones. A SIP safe zone might be (a) designated room(s), the entire building, or a safe area. This document uses the term SIP in its general term, which indicates a safe zone inside the building where people can stay safely in the event of an outdoor release.

Step 5 Develop a Communications Plan - An effective communications plan for SIP should be developed based on building-specific OEP procedures.

Step 6 Conduct SIP Training and Drills - Practice drills using the SIP procedures among building occupants should be performed as part of routine OEP drills. Train and familiarize those who are occupants in the building on awareness and the procedures to be taken in an airborne toxic release initiated outdoors. Training plans should be developed by the DO with input from the BSC, Property Management (PM), FPS, and other law enforcement entities.

Step 7 Reactive Guidelines for SIP -Once notification has been received from the local authorities, the following reactive measures are recommended based on the information gathered in the proactive review and building system evaluations.

Part 3: Implement and Maintain the OEP

- Implementation is more than simply exercising the OEP during an emergency. It means acting on recommendations made during the vulnerability analysis, integrating the plan into company operations, training employees, and evaluating the plan.
- During an event, the decision to activate the OEP shall be based upon the best available information, including an understanding of local tensions, the sensitivity of target agency(ies), and previous experience with similar situations. Advice shall be solicited, when possible, from the GSA building manager, appropriate FPS officials, and Federal, State, and local law enforcement agencies.
- When there is immediate danger to persons or property, such as fire, explosion, or the discovery of an explosive device (not including a threat), occupants shall be evacuated or relocated in automatic accordance with the plan. This shall be accomplished by sounding the fire alarm system or by other appropriate means. A warning message should be prepared beforehand for each of the protective actions that are practical for the building. This will ensure that the actions can be taken as rapidly as possible and that the instructions will be clearly understood. The messages should be worded to be effective without causing panic.

- Integrate the Plan into Facility Operations

Emergency planning must become part of the building's corporate culture:

- Look for opportunities to build awareness
- Educate and train personnel
- Test procedures
- Involve all levels of management, all departments, and the community in the planning process
- Make emergency management part of what personnel do on a day-to-day basis

1.0 Test the OEP to ensure:

- Senior management supports the responsibilities outlined in the plan
- Emergency planning concepts are fully incorporated into the facility's accounting, personnel, and financial procedures
- Emergency preparedness information is distributed
- There are constant safety reminders to occupants
- Personnel are aware of their responsibilities during an emergency
- All levels of the organization are involved in evaluating and updating the plan

2.0 Training, Drills, and Exercises

- Everyone who works at or visits the facility requires some form of training. Consider how to involve community responders in training activities, and conduct reviews after each training

[RETURN TO TOP](#)

activity to identify areas for improvement and record best practices. Involve both personnel and community responders in the evaluation process.

2.1 Planning Considerations

- Assign responsibilities for developing a training plan. Consider the training and information needs for employees, contractors, visitors, managers, and those with an emergency response role identified in the OEP and OEO. General training for all employees should address:
 - Individual roles and responsibilities
 - Information on the subject of threats, hazards, and protective actions
 - Notification, warning, and communications procedures
 - Means for locating family members in an emergency
 - Emergency response procedures
 - Evacuation, shelter, and accountability procedures
 - Location and use of common emergency equipment
 - Emergency shutdown procedures

2.2 Training Activities

The following training activities should be incorporated into the training plan:

- Orientation and Education sessions – are regularly scheduled discussion sessions to provide information, answer questions, and identify needs and concerns.
- Tabletop Exercises – members of the emergency management group meet in a conference room setting to discuss their responsibilities and how they would react to emergency scenarios. Using floor plans and building schematics, each key position ensures that they know where to go, what to do, and have the opportunity to discuss “what ifs”. This is a cost-effective and efficient way to identify areas of overlap and confusion before conducting more demanding training activities.
- Walk-Through Drills – The emergency management group and response teams actually perform their emergency response functions. This activity generally involves more people and is more thorough than a tabletop exercise.
- Functional Drills – These drills test specific functions such as medical response, emergency notifications, warning, and communications procedures and equipment. These tests may be performed singularly or collectively. Personnel are asked to evaluate the systems and identify problem areas.
- Evacuation Drills – Personnel walk the evacuation route to a designated area where procedures for accounting for all personnel are tested. Conditions of drills should be varied so that occupants are prepared to know how to respond to varying conditions. For example, use of alternate exits because primary exits are blocked. Participants are asked to make notes as they investigate potential hazards during emergencies (e.g. stairways cluttered

[RETURN TO TOP](#)

with debris, smoke in hallways). Plans are modified accordingly.

- Full-Scale Exercises – A real-life emergency situation is simulated as closely as possible. This exercise involves company emergency response personnel, employees, management and community response organizations.
- After Action Reports – After an exercise, drill, or actual emergency, an analysis should be conducted to identify issues that could require a modification to the OEP.

2.3 Facility Training Schedule

- Distribute the first draft to group members for review. Revise as needed. For a second review, conduct a tabletop exercise with management and personnel who have a key emergency management responsibility. In a conference room setting, describe an emergency scenario and have participants discuss their responsibilities and how they would react to the situation. Based on this discussion, identify areas of confusion and overlap, and modify the plan accordingly.
- Capabilities and hazards must be analyzed after a vulnerability analysis is conducted. The single most important determination for a facility and security managers to make in determining the needs for an occupant emergency plan is a comprehensive risk assessment for the facility.

3.0 Evaluate and Modify the OEP

- Conduct an evaluation of the entire plan at least once a year. Attachment 3-1 provides checklists that can be used to evaluate OEP procedures. Evaluation and modification of OEPs should take place after each training drill, exercise, and emergency. OEP review is also relevant when personnel or responsibilities change, alongside facility layout, design, policy and procedure changes. Each modification requires that personnel and OEO individuals be briefed. Some issues to consider are:
 - Methods to involve all levels of management in evaluating and updating the plan
 - Ways to sufficiently address problem areas and resource shortfalls identified in the vulnerability analysis
 - Inclusion of lessons learned from drills and actual events
 - Review emergency management group and ERT to understand respective responsibilities as well as to provide training for new members
 - Reflection of changes in the physical layout of the facility
 - Specification of any new facility processes
 - Updated photographs and other records of facility assets
 - Assessment of the facility training objectives
 - Changes of hazards to the facility
 - Citing names, titles, and telephone numbers in OEP, and ensuring they are kept current

Attachment 1: General Responsibilities of the OEO Teams

Designated Official - the highest-ranking official of the primary occupant agency; or alternatively, a designee selected by mutual agreement of occupant agency officials as prescribed by 41 CFR § 101-20.003(g). Responsible for activating the plan in all emergencies during normal duty hours along with the following:

- Developing and maintaining the OEP to protect life and property, and to minimize the damage in the event of a disaster.
- Coordinating the plan with the OEP Coordinator and tenant agency officials.
- Organizing, and providing training for, an adequate staff to conduct the emergency operations required by the facility's OEP.
- Disseminating the basic provisions of the OEP to all persons employed in the building and arranging for publication and distribution of a roster of organization personnel responsible for emergency operations.
- Maintaining liaison, and cooperating, with the heads of the tenant agencies, or their designees, as well as Federal, State, and local agencies that might respond to an emergency in the facility.
- Taking all necessary actions to ensure that the facility's organization operates safely and efficiently in emergencies.
- Exercising command responsibility where appropriate for the orderly evacuation of all personnel in the building (including non-tenants) in accordance with the OEP.
- Coordinating and directing fire and evacuation drills.
- Participates in the facility's Emergency Response Team and Building Security Committee.

Occupant Emergency Coordinator - The official appointed by the Designated Official and serves as the primary assistant to the Designated Official to ensure the continued viability of the OEP and its organization. During emergencies the Occupant Emergency Coordinator operates the Command Center. Under the general direction of the Designated Official, the Occupant Emergency Coordinator performs the following duties:

- Coordinating training for the occupant emergency organization members as required.
- Monitoring fire drills and evacuations to ensure procedures are workable, and initiating further training when necessary.

Floor Team Coordinator - Supervises and expedites the planned and controlled movement of all building occupants in an emergency. Under the general direction of the Designated Official, the Floor Team Coordinator serves as head of occupant evacuations and performs the following duties:

- Plans personnel movement routes and establishes movement procedures.
- Assigns and trains floor wardens and related personnel within, into, or out of the building, during drills and actual emergencies, as required by the plan.

- Assures that all building occupants, including members of the organization, comply with procedures indicated by the alarm signal as specified by the plan.
- Coordinates bomb search of office space.
- Is a member of the Emergency Command Center during emergencies.
- Advises Designated Official of the progress of evacuation and/or bomb searches.

Damage Control Team Coordinator - Under the direction of the designated official, the damage control coordinator serves as head of the utilities controls group as follows:

- Establish a plan to control mechanical devices such as: ventilation equipment, water, gas, and electrical distribution systems at the direction of the Fire Chief or Designated Official.
- During emergency situations the Utility Officer immediately proceeds to the Emergency Command Center to await instructions from the Fire Chief or Designated Official.
- Dispatches individuals or mechanical teams to operate building utilities or assist emergency personnel in the control of building utility systems.

Medical Coordinator - The medical coordinator is head of the Health and First Aid Unit and is responsible for training and equipping all employees assigned to perform first aid in an emergency.

- Arranging with the American Red Cross or other sources for first aid and medical self-help training for all organizational personnel as requested by members of the organization.
- Supervising the selection of first aid or medical treatment areas as required.
- Directing first aid or medical self-help operations and controlling access to medical supplies, as required, to ensure their proper use, conservation and availability for emergency use.
- Establish policy and rules governing emergency treatment of the ill and injured. The maintenance of adequate sanitation and hygienic standards, and other matters relating to emergency health, hygiene and medical activities during emergencies.

Administrative Officer – The administrative officer must administer actions during and after an emergency which include:

- Maintain telephone logs
- Keep a detailed record of events
- Maintain a record of injuries and follow-up actions
- Account for personnel
- Coordinating notification of family members
- Issue press releases
- Maintain sampling records
- Manage finances
- Coordinate personnel services

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

- Document incident investigations and recovery operations
Technical Advisors – Occupants familiar with the building’s utilities and mechanical systems or other areas of expertise who advise the DO and OEC such as: Building/Property Manager, Maintenance Manager, and Physical Security Specialist.

Attachment 2: Sample Emergency Procedures

Emergency procedures and considerations are provided for the following that can be tailored to specific facility needs:

[2-1 Medical– localized and widespread](#)

[2-2 Evacuation](#)

[2-3 Hazardous Substance](#)

[2-4 Bomb Threat](#)

[2-5 Suspicious Object](#)

[2-6 Sheltering In Place](#)

[2-7 Explosion](#)

[2-8 Natural Disaster – with advance notice and without](#)

[2-9 Demonstrations](#)

[2-10 Missing Child – Code Adam](#)

[2-11 Enhanced Protection due to Increased Threat](#)

[2-12 Post-Emergency Recovery](#)

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

2-1 MEDICAL		
Position	ACTIONS	
	Limited	Widespread with Multiple Injuries
ALL Building Occupants		
All Building Occupants	<ul style="list-style-type: none"> • CALL 911 [or other emergency number] • If First Aid/CPR trained, provide assistance until medical personnel arrive. 	
Command Center Team		
DO/OEC	<ul style="list-style-type: none"> • Notify Floor Monitor • Notify Medical Coordinator 	<ul style="list-style-type: none"> • Go to Primary Command Center • Activate Command Center Team
Medical Coordinator	<ul style="list-style-type: none"> • Go to scene • Ensure that appropriate assistance has been called • Recommend follow-up action • Report to DO 	<ul style="list-style-type: none"> • Go to scene • Advise regarding medical assistance and ensure that appropriate assistance has been summoned • Report to DO
All other CCT members	NA	<ul style="list-style-type: none"> • Go to Primary Command Center • Notify or activate teams as appropriate.
Floor Team		
Floor Team Members	NA	<ul style="list-style-type: none"> • Provide first aid/CPR • Obtain medical assistance (see emergency call list) • Notify OEC • Notify Federal Protective Service • Reserve elevators for emergency use • Meet responding emergency unit at ground floor • Verify medical assistance response • Report to Floor Team Monitor
Damage Control Team		
Damage Control Team Members	NA	<ul style="list-style-type: none"> • Provide first aid/CPR and rescue services. • Report to Damage Control Coordinator.

2-2 Evacuation

Evacuation policies and procedures should:

- Determine conditions under which an evacuation would be necessary.
- Establish a clear chain of command.
- Identify personnel with the authority to order an evacuation.
- Designate “evacuation wardens” who will assist others in an evacuation and account for personnel.
- Establish a system for accounting personnel.
- Consider employees’ transportation needs for community-wide evacuations.
- Establish procedures for assisting persons with disabilities and those who do not speak English.
- Consider evacuation procedures for Child Care Centers.
- Include post evacuation procedures:
 - Designate personnel to continue or shut down critical operations while an evacuation is underway. They must be capable of recognizing when to abandon the operation and evaluate themselves.
 - Coordinate plans with the local emergency management office.
 - Final decision for personnel (e.g. resume work, go home, etc.) will be made by the DO and communicated to everyone along appropriate communication channels.

Designate primary and secondary evacuation routes and exits. Have routes and exits within the facility clearly marked, well lit, and announced with appropriate signage. Evacuation routes, exits, location destinations, etc., must be discreet outside the facility to ensure proper protection of building occupants.

Be reviewed and approved through:

- Distribute the first draft to group members for review – Revise as necessary
- During second review, conduct tabletop exercise with management and personnel with key emergency management responsibility. In conference room setting, describe an emergency scenario and have participants discuss their responsibilities and how they would react to the situation. Based on discussion, identify areas of confusion and overlap, and modify plan accordingly.
- Arrange a briefing for the DO, chief executive officer, and senior management – obtain written approval.
- Install emergency lighting in case a power outage occurs during an evacuation.
- Ensure that evacuation routes and emergency exits are:

Wide enough to accommodate the number of evacuating personnel

- Clear and unobstructed at all times

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

- Unlikely to expose evacuating personnel to additional hazards
- Capable of avoiding (or having alternate routes that avoid) the main lobby
- Be evaluated by someone not in your organization

2-2 EVACUATION			
Position	ACTIONS		
ALL Building Occupants			
All Building Occupants	<ul style="list-style-type: none"> • Activate the nearest fire alarm pull box then dial [insert number] to notify [insert title] and provide specifics. • Follow instructions provided by the Command Center Team. 		
Command Center Team			
DO/OEC	<ul style="list-style-type: none"> • Go to Primary Command Center and activate the Command Center Team • Verify fire department notification and response and brief responding personnel • Coordinate activities 		
Medical Coordinator	<ul style="list-style-type: none"> • Go to Primary Command Center and advise regarding medical assistance 		
Floor Team Coordinator	<ul style="list-style-type: none"> • Go to Primary Command Center and activate Floor Teams and coordinate Floor Team activities and verify occupant status 		
Damage Control Coordinator	<ul style="list-style-type: none"> • Go to Primary Command Center and activate the Damage Control Team • Determine building conditions (e.g., environmental, structural, etc.) 		
Administrative Officer	<ul style="list-style-type: none"> • Go to Primary Command Center and record activities 		
Floor Team	Fire Floor	First Floor	Other Floors
Floor Monitors	<ul style="list-style-type: none"> • Activate fire alarm (if not already done). • Supervise and verify evacuation. • Report to Floor Team Coordinator. 	<ul style="list-style-type: none"> • Lead fire department to control center. • Restrict building access. • Assist with occupant evacuation 	<ul style="list-style-type: none"> • If floor is to be evacuated, follow Fire Floor Team instructions. • If not, stand by for instructions
Area Monitors	<ul style="list-style-type: none"> • Evacuate area occupants • Inspect area to ensure total evacuation • Report status to Floor Monitor. 		
Elevator Monitors	<ul style="list-style-type: none"> • Direct occupants to the nearest safe stairwell. • Assist in elevator evacuation of the disabled if elevator use of this purpose has been authorized. 		
Stairway Monitors	<ul style="list-style-type: none"> • Inspect stairway for smoke or other obstruction and report status to Area Monitor. • Keep occupants moving in a single file down the stairway. 		
Monitors for Disabled	<ul style="list-style-type: none"> • Evacuate disabled to safe area. • Report status to Area Monitor 		
Damage Control Team			
Damage Control Team Members	<ul style="list-style-type: none"> • Report to Damage Control Coordinator and activate emergency systems 		

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

2-2 EVACUATION			
Position	ACTIONS		
Floor Monitors	<ul style="list-style-type: none"> • Activate fire alarm (if not already done). • Supervise evacuation. • Verify evacuation. • Report to FTC. 	<ul style="list-style-type: none"> • Lead fire department to control center. 	<ul style="list-style-type: none"> • If floor is to be evacuated, follow Fire Floor Team instructions. • If not, stand by for instructions
Area Monitors	<ul style="list-style-type: none"> • Evacuate area occupants • Inspect area to ensure total evacuation • Report status to Floor Monitor (including relocation of disabled). 	<ul style="list-style-type: none"> • Restrict building access. • Assist with occupant evacuation 	
Elevator Monitors	<ul style="list-style-type: none"> • Direct occupants attempting to use elevators to the nearest safe stairwell. • Assist in elevator evacuation of the disabled if elevator use of this purpose has been authorized. 	<ul style="list-style-type: none"> • Report to First Floor Monitor • Capture assigned elevators (either automatically or using required special key or the regular call button). • After capture, use of elevators can be authorized only by the fire department, DO, or OEC. 	
Stairway Monitors	<ul style="list-style-type: none"> • Inspect stairway for smoke or other obstruction, if obstructed direct occupants to another stairway. • Keep occupants moving in a single file down the stairway. • Report status to Area Monitor. 	<ul style="list-style-type: none"> • Lead fire department to control center. • Restrict building access. • Assist with occupant evacuation 	
Monitors for Disabled	<ul style="list-style-type: none"> • Evacuate disabled to safe area. • Report status to Area Monitor 		
Damage Control Team			
Damage Control Team Members	<ul style="list-style-type: none"> • Report to Damage Control Coordinator • Activate emergency systems: Alarm systems, Smoke control, Fire extinguishment, and Emergency power 		

2-3 HAZARDOUS SUBSTANCE	
Position	ACTIONS
ALL Building Occupants	
All Building Occupants	<ul style="list-style-type: none"> • Dial [insert number] to notify [insert title] and provide specifics. • Follow instructions provided by the Command Center Team.
Command Center Team	
DO/OEC	<ul style="list-style-type: none"> • Activate Command Center Team. • Determine if an evacuation is appropriate: <ul style="list-style-type: none"> o If yes, follow evacuation procedures. o If no, follow shelter-in-place procedures. • Notify fire department. • Notify Federal Protective Service. • Notify appropriate utility company or hazard materials expert. • Go to Alternate Command Center. • Hold occupants at relocation site. • Do not permit reentry until determined safe by proper authorities. • In case of explosion, follow instructions under Bomb Explosion.
All Other CCT Members	<ul style="list-style-type: none"> • Go to Primary Command Center. • Notify or activate appropriate teams as appropriate.
Floor Team	
Floor Monitors	<ul style="list-style-type: none"> • Activate Floor Teams. • Supervise evacuation. • Report to Floor Team Coordinator at relocation site Alternate Command Center.
Area Monitors	<ul style="list-style-type: none"> • Coordinate area evacuation. • Report conditions to Floor Monitors. • Accompany area occupants to relocation site. • Hold occupants and await instructions.
Stairwell Monitors	<ul style="list-style-type: none"> • Control evacuation via stairways. • Report to Area Monitors.
Monitors for the Disabled	<ul style="list-style-type: none"> • Assist individuals requiring assistance to relocation site. • Remain with disabled. • Report to Area Monitors when possible.
Elevator Monitors	<ul style="list-style-type: none"> • Go to relocation site. • Report to Floor Monitor.
Damage Control Team	
Damage Control Team Members	<ul style="list-style-type: none"> • Report to Damage Control Coordinator at relocation site Command Center

2-4 BOMB THREAT			
Position		Actions	
ALL Building Occupants			
All Building Occupants		<ul style="list-style-type: none"> • Dial [insert number] to notify [insert title] and provide specifics. • Follow instructions provided by the Command Center Team. 	
Command Center Team			
DO/OEC		<ul style="list-style-type: none"> • Go to Primary Command Center • Verify FPS notification and response 	
All Other CCT Members		<ul style="list-style-type: none"> • Go to Primary Command Center. • Notify or activate appropriate teams as appropriate. 	
Floor Team	Affected Floors	First & Ground Floors	Unaffected Floors
Floor Monitors	<ul style="list-style-type: none"> • Initiate evacuation/relocation. • Supervise and verify evacuation. • Report to Floor Team Coordinator. 	<ul style="list-style-type: none"> • Control building access. • Keep people away from building perimeter • Control occupant movement, according to instructions received from Primary Command Center 	
Area Monitors	<ul style="list-style-type: none"> • Instruct occupants to search their work areas. • Evacuate/relocate occupants. • Inspect area to ensure total evacuation. • Search assigned public areas and exit routes. • Report to Floor Monitors. 	NA	
Elevator Monitors	NA		NA
Stairwell Monitors	<ul style="list-style-type: none"> • Inspect stairwells and exit routes. • Lead occupants to safe area. • Report to Area Monitors. 	NA	
Disabled Occupant Monitors	<ul style="list-style-type: none"> • Verify status of disabled occupants. • Report to Area Monitors. 	NA	
Damage Control Team			
Damage Control Team Members		Search assigned areas including maintenance, storage, outside, and rooftop areas	

Bomb Threat Received

If a bomb threat is received by phone:

- Remain calm. Keep the caller on the line for as long as possible. **DO NOT HANG UP**, even if the caller does.
- List carefully. Be polite and show interest.
- Try to keep the caller talking to learn more information.
- If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
- If your phone has a display, copy the number and/or letters on the window display.
- Complete the Bomb Threat Checklist immediately. Write down as much detail as you can remember. Try to get exact words.
- Immediately upon termination of the call, **DO NOT HANG UP**. From a different phone, contact FPS immediately with information and await instructions.

If a bomb threat is received by handwritten note or through the mail:

- Call [Insert Correct Contact Information]
- Handle note as minimally as possible.

If a bomb threat is received by e-mail:

- Call [Insert Correct Contact Information]
- Do not delete the message.
- **DO NOT:**
 - Use two-way radios or cellular phone; radio signals have the potential to detonate a bomb.
 - Evacuate the building until police arrive and evaluate the threat.
 - Activate the fire alarm.
 - Touch or move a suspicious package.

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

Following is information to be recorded by a bomb threat message recipient during or immediately after the threat is communicated.

Date: _____

Time: _____

Time Caller Hung Up: _____

Phone Number Where Call Was Received: _____

Questions to ask Caller: _____

Where is the bomb located? (Building, Floor, Room, etc.): _____

When will it go off? _____

What does it look like? _____

What kind of bomb is it? _____

What will make it explode? _____

Did you place the bomb? (Yes, No) _____

Why? _____

What is your name? _____

Where are you? _____

Record Exact Words of Threat: _____

Record Information About Caller: _____

Where is the caller located? (Background and level of noise) _____

Estimated age _____

Is the voice familiar? If so, who does it sound like? _____

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Circle Any That Apply

Caller's Voice

- Accent
- Angry
- Calm
- Clearing throat
- Coughing
- Cracking voice
- Crying
- Deep
- Deep breathing
- Disguised
- Distinct
- Excited
- Female
- Laughter
- Lisp
- Loud
- Male
- Nasal
- Normal
- Ragged
- Rapid
- Raspy
- Slow
- Slurred
- Soft
- Stutter

Background Sounds:

- Animal Noises
- House Noises
- Kitchen Noises
- Street Noises
- Booth
- PA System
- Conversation
- Music
- Motor
- Clear
- Static
- Office machinery
- Factory machinery
- Local
- Long distance

Threat Language:

- Message Read Incoherently
- Taped
- Irrational
- Profane
- Well-spoken

2-5 SUSPICIOUS OBJECT			
Position	Actions		
ALL Building Occupants			
All Building Occupants	<ul style="list-style-type: none"> Do not touch suspicious objects Report them immediately upon discovery. Dial [insert number] to notify [insert title] Provide specifics. Follow instructions provided by the Command Center Team. 		<u>Signs of a Suspicious Package</u> <ul style="list-style-type: none"> No Return Address Excessive Postage Stains Strange Odor Strange Sounds Unexpected Delivery Poorly Handwritten Misspelled Words Incorrect Titles Foreign Postage Restrictive Notes
Command Center Team			
DO/OEC	<ul style="list-style-type: none"> Go to Primary Command Center Activate Command Center Team Verify fire department notification and response Brief responding personnel Evacuate or relocate occupants Building Manager to put elevators in Phase I Service. 		
All Other CCT Members	<ul style="list-style-type: none"> Go to Primary Command Center. Notify or activate appropriate teams as appropriate. 		
Floor Team	Affected Floors	First and Ground Floors	Unaffected Floors
Floor Monitors	<ul style="list-style-type: none"> Carry out evacuation or relocation plan. Supervise and verify evacuation. Report to Floor Team Coordinator. 	<ul style="list-style-type: none"> Control building access. Keep people away from building perimeter 	<ul style="list-style-type: none"> After evacuation, restrict use of elevators, escalators and stairwells
Area Monitors	<ul style="list-style-type: none"> Coordinate area evacuation. Determine location of suspicious object; avoid using stairwells, elevators or escalators in immediate area. Inspect area to ensure total evacuation. Report status to Floor Monitor. 		
Elevator Monitors	NA	<ul style="list-style-type: none"> Report to First Floor Monitor. Hold elevators and assist emergency units. 	
Stairwell Monitors	<ul style="list-style-type: none"> Inspect stairwells and exit routes. Lead occupants to safe area. Report status to Area Monitors. 	NA	NA
Disabled Occupant Monitors	<ul style="list-style-type: none"> Coordinate evacuation if disabled occupants. Report status to Area Monitor. 	NA	NA
Damage Control Team			
Damage Control Team Members	NA	NA	NA

2-6 SHELTERING-IN-PLACE

This information on sheltering-in-place (SIP) provides a general guideline for developing a plan for SIP with tenant agency and other building occupant cooperation.

Step 1 - Review Building Vulnerability Assessment Reports and OEP

Step 2 - Identify Building Features

- Determine the building's age⁶.
- Determine the building's type of ventilation system – natural ventilation, unit ventilators (through-the-wall units in each room), or duct system with air handling units, HVAC, elevators, and building envelope.
- If a duct system, record the number of different zones and air handling units, and the locations of switches for each.
 - Are there protections on the intake and re-circulation ducts of the HVAC system?
 - How long does it take to stop the intake of air into your facility?
 - Is the HVAC system shut off in one central location, or are multiple shutoffs required?
- Determine if the building has smoke purge fans, and whether the intakes of the smoke purge fans are elevated or at ground level.
 - Record the locations and identification of switches for the smoke purge fans.
 - Determine if the building has automatic dampers in working condition on outside air fans and air handlers.
 - List all exhaust fans and the location and identification of the control for each.
 - Determine if stairwells are protected from smoke (external and isolated).
- Determine whether the building has a public address system. If yes, record the locations of the broadcast microphone and controls.
- Record the information on communication with the building security personnel.
- Obtain a copy of the evacuation routes posted for a fire emergency.
- Evaluate the elevator system for its impact on building airflow to determine availability of use during a SIP event.
- Evaluate the potential for air infiltration through the building envelope.
- Determine if there are safe zones for possible SIP.

Step 3 – Identify Features Increasing Building Vulnerability

- If the building has mechanical ventilation with a duct system, record the location of all fresh-air intakes that are at ground level and accessible to the public or next to a street or roadway.

⁶ Buildings constructed after 1970 tend to be more airtight than older buildings, due to increased energy conservation standards.

- List the locations of mechanical rooms having air handlers, whether each mechanical room is kept locked, and which have outside entrances.
- Determine where the lobby and any public access areas of the building share an air-handling unit with office areas.
- Determine if security-screening procedures are in place to prevent hazardous materials from being brought into the building.

Step 4 – Identify SIP Safe Zones

In general, a SIP safe zone should:

- Be identified based on the features that make a building vulnerable to the outside airborne contaminant releases.
- Have the least air infiltration when the HVAC and other ventilation systems are shut off.
- Have sufficient space for all building occupants. In some situations, the SIP zone may consist of the entire building or significant portions of the building. If the safe zone is a number of designated room(s), then it is preferred to be located in the inner part of the building (no windows to the outside). The rooms should have doors that are fairly effective at preventing airflow from the hallways: at least there should be no gap around the edges of the door, and preferably there should be a gasket to completely seal the room. Opening and closing a conventional door can pump significant amounts of air into the safe zone. Safe rooms are best located on mid floors and in interior rooms away from outside walls.
- Have a shelter kit. The identified safe zone should have enough space for all building occupants. Before an incident occurs, your SIP safe zone should have a shelter kit.
- Not be bathrooms, kitchens, and other unsafe spaces with exhausted ducts to outside. Bathrooms are typically a bad choice for a SIP location because they often have an exhaust duct that leads directly outside. If the exhaust fan is turned off, then the duct can allow contaminants to enter the facility from outside. Additionally, the stack effect can draw air into the bathroom from within the building, eventually contaminating the building during an indoor release. If the exhaust fan is left on, then air will be drawn into the bathroom from other parts of the building, which will eventually contaminate the bathroom.
- Have a Knox Box key repository with all necessary keys and cards needed for the fire and hazardous materials team responders to gain access to your safe areas.

Step 5 – Develop a Communication Plan

The plan should suggest how to:

- Receive timely information on the threat of airborne contaminant releases outside of the building and effectively communicate the information to building authorities.
- Activate the organization in response to a threat.
- Inform building occupants of the nature of an emergency and what action to take.
- Coordinate activities during the SIP.
- Use all available resources to get word out (e-mail, voice-mail system, telephone, OEP

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

monitor, office-to-office personal notification) when informing building authorities and occupants.

- Prepare a warning message before an incident for each protective action practical for the building. This will ensure the actions can be taken as rapidly as possible and that instructions will be clearly understood. Messages should be worded to be effective without causing panic.
- Provide instructions on turning off fans or closing windows during SIP. In buildings with unit ventilators, sheltering messages may require instructions for turning off ventilators. In buildings with natural ventilation, instructions for closing windows and doors may be required.
- Consider procedures and communication avenues for the following activities:
 - Determining if/when the outside release occurs in conjunction with local emergency responders
 - Determining the characteristics of the release in conjunction with local emergency responders
 - Deciding upon the best action to take in conjunction with local emergency responders based on conditions and events
 - Deciding if a SIP condition exists
 - Issuing the order authorizing a SIP
 - Communicating emergency instructions to all in the building
 - Sheltering-in-place
 - Monitoring the event in conjunction with local emergency responders
 - Issuing “All Clear” notifications as appropriate

Step 6 – SIP Training Drills

Training and drills should satisfy the following objectives:

- Develop an employee awareness of potential airborne hazards. When trained, the building occupants can serve to detect hazards and reduce response time by being aware of odors, signs, symptoms, and suspicious activities. Training should include familiarization with the warning properties of hazardous chemicals stored or used outside and within the building, information on what actions are to be taken, and awareness of suspicious activities relating to fresh air intakes, mechanical rooms, and abandoned parcels. This training should be part of a program that trains building occupants to the Awareness level in WMD.
- Develop an understanding of the responses and what steps to take for each of the possible protective programs.
- Inform building occupants about the BSC, their job, and how they can be contacted.
- Inform those employees taking prescriptions or other medications that they should keep an on-hand supply on their person.

- Discuss and take necessary actions with authorities related to special needs that may be required by some building occupants.
- Train building occupants on water conservation for the duration of the SIP.
- Train property managers for SIP conditions.
- Train contractors and contract employees.
- Identify and mark safe SIP zones (locations and accountability for them)
- Ensure guards are familiar with SIP procedures in alignment with post orders.
- Assign duties to specific employees with backups.
- Coordinate actions with local emergency responders including ensuring familiarization with where safe rooms are, number of people within, and other safety measures in place.

Stages of OEP integration.

- Conduct orientation drills and meetings where ERT becomes acquainted with local responders in preparation for an emergency.
- Facility “Walk Through” exercises, with Fire Department officials and EMS responders to preplan facility OEPs.
- Participate in, or observe tabletop exercises for emergency managers to allow decision makers to learn what will happen when an emergency occurs and how to integrate the internal response within the operational framework.
- Offer to host and participate in Functional and Full-Scale exercises.
- Allow local emergency responders to conduct Walkthroughs to determine multiple routes to and from safe areas.
- Determine various possible upgrade and up wind decontamination sites that would be used by local responders in an emergency.

Step 7 – Reactive Guidelines for SIP

Once notification has been received from local authorities, the following guidelines are recommended if SIP is required:

- Inform building occupants of SIP conditions, direct them to SIP safe zone(s), and account for people;
- Notify the Building Security Committee (BSC) members, Federal Security Authorities, property management personnel, and all other occupants of the building about the incident and SIP requirements;
- Minimize the rate of air exchange with the outside as to keep indoor concentration as low as possible for as long as possible by closing all windows and doors to the outside, and closing all necessary doors;
- Shut-off all HVAC fans and close all HVAC dampers, including exhaust dampers. Shut off other fans such as kitchen and bathroom exhausts. If shutting off these systems takes more

time due to the building condition, then shutting off the whole electrical system should be evaluated during SIP proactive planning;

- Do not use elevators – they create a piston effect and can pump air into or out of the building;
- Seal the doors, windows, and vents if necessary;
- Establish communication with outside through a TV, radio, cell phone, or others and ensure that emergency responders know your location(s);
- Once the threat has passed and the authority having jurisdiction gives an “all clear,” evacuate the building and flush it with outdoor air. When leaving, be aware and cognizant of signs and symptoms of contamination in the event evacuee pass through a contamination pocket in the structure or outside. SIP requires two distinct actions be taken without delay to maximize the passive protection;
- Reduce indoor/outdoor air exchange rate before hazardous plume arrives. Close all windows and doors and turn off all fans, air conditioners, HVAC, elevators and combustion heaters.
- Increase indoor/outdoor air exchange rate as soon as hazardous plume has passed. Open all windows and doors and turn on all fans to ventilate the building. Though tightly sealed, a building does not prevent contaminated air from entering; it minimizes the rate of infiltration. Outside air enters more slowly, and once the external hazard has passed, the building releases the contaminated air slowly as long as it remains closed. If there is a release close to the ground near a tall building, and if the building’s air intakes are on the roof or upper floors of the building far from the release areas, operating the HVAC so as to pressurize the building with air taken-in through the HVAC system will usually be better than shutting off the HVAC entirely. Actions such as this can only be taken if there is a very good knowledge of the release location and the dispersion of the contamination and if the designated official authorizes it. This decision should be made in consultation with local emergency responders if available as the weather; contaminant chemical and physical properties can cause variable reactions with the contaminant’s behavior.

The amount of protection varies with the following:

- Duration of exposure. Protection varies with time, diminishing as the time of exposure increases. SIP is therefore suitable only for exposures of short duration, generally three hours or less, depending upon building conditions and the nature of the incident.
- Natural filtering. Some filtering occurs when an airborne agent is deposited in the building shell or upon interior surfaces as air respire through the building. This filtering effect is greatest in tight-fitted buildings.

Distribution of the SIP

- Place the final plan in three-ring binders and number all copies and pages.
- Each individual receiving a copy should be required to sign for it and be responsible for posting subsequent changes.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

- Determine which sections of the plan would be appropriate to share with other government agencies (some section may refer to classified information or include private listings of names, telephone numbers, or radio frequencies) and emergency response agencies (appropriate sections).

2-7 EXPLOSION			
Position		Actions	
ALL Building Occupants			
All Building Occupants		<ul style="list-style-type: none"> • Dial [insert number] to notify [insert title] and provide specifics. • Follow instructions provided by the Command Center Team. 	
Command Center Team			
DO/OEC		<ul style="list-style-type: none"> • Go to Primary Command Center. • Activate Command Center Team. 	
All Other CCT Members		<ul style="list-style-type: none"> • Go to Primary Command Center. • Notify or activate appropriate teams as appropriate. 	
Floor Team	Affected Floors	First & Ground Floors	Unaffected Floors
Floor Monitors	<ul style="list-style-type: none"> • Notify Floor Team. • Supervise evacuation, first aid, and rescue. • Report conditions to Floor Team Coordinator. 	Control access to the building	<ul style="list-style-type: none"> • Inform occupants. • Maintain control of occupants. • Control egress. • Maintain communication with Floor Team Coordinator. • Evacuate to a safe area if instructed to do so by Floor Team Coordinator.
Area Monitors	<ul style="list-style-type: none"> • Coordinate area evacuation, first aid, and rescue. • Inspect area to determine conditions. • Report to Floor Monitor. 		
Elevator Monitors	NA	<ul style="list-style-type: none"> • Capture elevators. • Hold until determined safe for use. • Assist emergency teams. 	
Stairwell Monitors	<ul style="list-style-type: none"> • Inspect assigned stairwell. • Report conditions to Area Monitors. • Lead occupants to safe area if required. 	NA	
Monitors for Disabled	<ul style="list-style-type: none"> • Move disabled occupants to safe area. 		
Damage Control Team			
Damage Control Team Members		<ul style="list-style-type: none"> • Assist in rescue. • Control access. • Inspect elevators, fire protection systems, and utilities. • Report conditions to Damage Control Team Coordinator. Make required repairs. 	

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

2-8 NATURAL DISASTER		
Position	ACTIONS	
	Advance Notice	No Advance Notice
ALL Building Occupants		
8. All Building Occupants	Follow instructions provided by the Command Center Team.	
Command Center Team		
DO/OEC	<ul style="list-style-type: none"> Activate the Command Center Team. Review plans and decide course of action Notify occupants. 	
Medical Coordinator	<ul style="list-style-type: none"> Go to scene Ensure that appropriate assistance has been called Recommend follow-up action Report to DO 	<ul style="list-style-type: none"> Go to scene Advise regarding medical assistance
Floor Team Coordinator	<ul style="list-style-type: none"> Review plans with floor monitors 	<ul style="list-style-type: none"> Go to Primary Command Center Coordinate and assist Floor Teams
Damage Control Coordinator	<ul style="list-style-type: none"> Activate DCT for damage prevention work. 	<ul style="list-style-type: none"> Go to Primary Command Center Activate Damage Control Team
Administrative Officer	NA	<ul style="list-style-type: none"> Go to Primary Command Center Record activities
Floor Team		
Elevator Monitors	NA	<ul style="list-style-type: none"> Capture assigned elevators. Restrict use until determined safe (mechanical safety inspection may be required).
Damage Control Team		
Damage Control Team Members	<ul style="list-style-type: none"> Protect windows and doors. Secure outdoor objects. 	<ul style="list-style-type: none"> Assess damage. Determine needs for controlling dangerous conditions. Provide repair, rescue, and first aid services as directed. Isolate unsafe areas. Report to Damage Control Coordinator.

Building Manager to place Elevators in Phase I Service upon complete evacuation.

2-9 DEMONSTRATIONS		
Position	ACTIONS	
	Advance Notice	No Advance Notice
ALL Building Occupants		
All Building Occupants	Follow instructions provided by the Command Center Team.	
Command Center Team		
DO/OEC	<ul style="list-style-type: none"> Go to Primary Command Center Notify Federal Protective Service – if FPS not in area, notify local police department. Notify Floor Team Coordinator. 	
Medical Coordinator	<ul style="list-style-type: none"> Go to scene Ensure that appropriate assistance has been called Report to DO Advise regarding medical assistance 	
Floor Team Coordinator	<ul style="list-style-type: none"> Go to Primary Command Center Activate Ground Level Floor Team 	
Damage Control Coordinator	<ul style="list-style-type: none"> Activate DCT for damage prevention work. 	<ul style="list-style-type: none"> Go to Primary Command Center Activate Damage Control Team
Administrative Officer	NA	<ul style="list-style-type: none"> Go to Primary Command Center Record activities
Floor Team		
Ground Level	<ul style="list-style-type: none"> Secure perimeter doors. Avoid any interaction with demonstrators. Prevent any occupant interaction with demonstrators. Follow instructions in responding to FPS officers and/or local police. 	
Damage Control Team		
Damage Control Team Members	<ul style="list-style-type: none"> Protect windows and doors. Secure outdoor objects. 	<ul style="list-style-type: none"> Assess damage. Determine needs for controlling dangerous conditions. Provide repair, rescue, and first aid services as directed. Isolate unsafe areas. Report to Damage Control Coordinator.

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

2-10 MISSING CHILD - CODE ADAM	
Position	ACTIONS
ALL Building Occupants	
All Building Occupants	<ul style="list-style-type: none"> • Immediately report lost or missing child notifications to security personnel • Assist in search for missing child according to communicated description
Command Center Team	
DO/OEC	<ul style="list-style-type: none"> • Obtain a detailed description of the missing child. At a minimum, the description should include: name, race, gender, age, eye color, hair color, approximate height, weight, any identifying marks, description of clothing (to include shoe color and style¹), time the child was last seen, last known location. • Direct or take parent/guardian/responsible party to a pre-determined contact location/main staging area for easy access in case more information is needed. • Report information to entrance control posts immediately by issuing a Code Adam Alert for building/location. • Pass description information to entrance control posts. If available, use a public address (PA) system to broadcast an announcement that a Code Adam Alert is in effect so that all tenants are alerted to look for the missing child. • Establish a central command location to which all Command Center Team members can report and coordinate their efforts with all responding personnel. Notifying a Regional Dispatch Center (i.e. FPS MegaCenter) that a Code Adam Alert has been initiated. • Instruct all access control posts to continue to control/monitor building access in addition to being aware of all people leaving the building. • Advise non-security personnel to participate through observation and reporting only. • Terminate Code Adam Alert when parent/guardian positively identifies child, and safety has been established. If found unharmed and no criminal activity has occurred, reunited child with parent/guardian. • Contact local law enforcement authorities if Alert renders negative results.
Floor Team Coordinator	<ul style="list-style-type: none"> • Coordinate and assist Floor Teams
Administrative Officer	<ul style="list-style-type: none"> • Assist with search efforts; track and document areas that have been searched and cleared. • Record activities/document the incident • Prepare initial report of incident and supplement with other pertinent information in update or follow-up report with original report's case control number
All other CCT Members	<ul style="list-style-type: none"> • Assist with search efforts
Floor Team	
Floor Team Members	<ul style="list-style-type: none"> • Conduct a thorough search of the building to positively identify all children located in the building • Search all potential hiding places, offices, common areas, and exterior areas of the property • If a CCTV system is in place, monitor it closely for the missing child • If CCTV system has capabilities of viewing without interrupting ongoing recording, review video to identify the last time child was seen
Floor Team Members	<ul style="list-style-type: none"> • Conduct a thorough search of the building • Search all potential hiding places, offices, common areas, and exterior areas of the property • Positively identify all children located in the building • If a CCTV system is in place, monitor it closely for the missing child • If CCTV system has capabilities of viewing without interrupting ongoing recording, review video to identify the last time child was seen • Announce Code Adam Alert cancellation upon DO determination via available means of dissemination

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

2.11 Enhanced Protection Due to Increased Threat
Low Condition (Green): Low risk of terrorist attack. Security partners should consider the following general measures in addition to the facility-specific protective measures they develop and implement:
Refine and exercise as appropriate preplanned protective measures
Ensure that personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency protective measures
Institutionalize a process to ensure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks and that all reasonable measures are taken to mitigate these vulnerabilities
Guarded Condition (Blue): General risk of terrorist attack. In addition to the protective measures taken in the previous threat condition, security partners should consider the following general measures in addition to the facility-specific protective measures they develop and implement:
Check communications with designated emergency response or command locations
Review and update emergency response procedures
Provide the public with any information that would strengthen its ability to act appropriately
Elevated Condition (Yellow): Significant risk of terrorist attack. In addition to the protective measures taken in the previous threat condition, security partners should consider the following general measures in addition to the facility-specific protective measures they develop and implement:
Increase surveillance of critical locations
Coordinate emergency plans as appropriate with nearby jurisdictions
Assess whether the precise characteristics of the threat require the further refinement of preplanned protective measures
Implement, as appropriate, contingency and emergency response plans
High Condition (Orange): High risk of terrorist attack. In addition to the protective measures taken in the previous threat condition, security partners should consider the following general measures in addition to the facility-specific protective measures they develop and implement:
Coordinate necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations
Take additional precautions at public events and possibly consider alternative venues or even cancellation
Prepare to execute contingency procedures, such as moving to an alternate site or dispersing the facility's workforce
Restrict threatened facility access to essential personnel only
Severe Condition (Red): Severe risk of terrorist attack. Under most circumstances, the protective measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the protective measures taken in the previous threat condition, security partners should consider the following general measures in addition to the facility-specific protective measures they develop and implement:
Increase or redirect personnel to address critical emergency needs
Assign emergency response personnel and pre-positioning and mobilizing specially trained teams or resources
Monitor, redirect, or constrain transportation systems
Close public and government facilities

2-12 Post-Emergency Recovery

Immediately after an emergency, take steps to resume operations.

- As soon as possible, report to the OEP Team following notification of an incident/emergency;
- Maintain contact with all members of the OEP Team and facilitate the flow of information between members of the OEP Team;
- Identify the required support personnel who may be needed;
- Dispatch, as required, members of the OEP Team, to assist in the incident/emergency;
- Assist in the coordination and movement of personnel away from impacted area;
- Advise, in consultation with members of the OEP Team and local authorities, when the building is safe for reoccupation when the incident has concluded sound the All Clear; and
- Upon arrival of FPS and/or local authorities, the OEC shall brief emergency responders of the existing emergency.

Within 48 hours of the emergency:

- Call a follow-up meeting of the OEP Team to discuss the events of the emergency.
- Reinforce actions/responses, which worked well.
- Lessons learned change actions/responses that did not work well.
- Recommend changes to the OEP. Local emergency personnel shall be invited, if appropriate.
- Responsible for scheduling evacuation drills for their building.
- Determine if any critical operations cannot be disrupted.
- Brief all building occupants on the drill and given assignments.
- Recruit non-occupants of the building to observe the drill and make critical evaluations.
- Notify Safety and Security that a simulated emergency is in progress.
- Decide if occupants are to be evacuated to off-site facilities.
- Notify the relocation center if an off-site evacuation is to be performed.
- Identify the locations to be evacuated.
- Ensure all occupants are aware of these different locations and when to use them.
- Post these locations in each area and exercise these evacuations.
- Identify person (s) responsible for ensuring all people have been evacuated.
- Identify when occupant may return.

2-12 Post-Emergency Recovery

- Communicate with floor wardens, and conduct visual inspections of the building for evacuation hazards.
- Establish a recovery team, if necessary.
- Establish priorities for resuming operations.
- Continue to ensure the safety of personnel on the property. Assess remaining hazards.
- Maintain security at the incident scene.
- Conduct an employee briefing.
- Keep detailed records. Consider audio recording all decisions. Take photographs of or videotape the damage.
- Account for all damage-related costs. Establish special job order numbers and charge codes for purchases and repair work.
- Follow notification procedures. Notify employees' families about the status of personnel on the property. Notify off-duty personnel about work status. Notify insurance carriers and appropriate government agencies.
- Protect undamaged property. Close up building openings. Remove smoke, water and debris.
- Protect equipment against moisture. Restore sprinkler systems. Physically secure the property. Restore power.
- Conduct an investigation. Coordinate actions with appropriate government agencies.
- Conduct salvage operations. Segregate damaged from undamaged property. Keep damaged goods on hand until an insurance adjuster has visited the premises, but you can move material outside if it's seriously in the way and exposure to the elements won't make matters worse.
- Take an inventory of damaged goods.
- Restore equipment and property. For major repair work, review restoration plans with the insurance adjuster and appropriate government agencies.
- Assess the value of damaged property. Assess the impact of business interruption.
- Maintain contact with customers and suppliers.

Attachment 3: Reviewing OEP Procedures and Identifying Best Practices

This section provides code requirements and industry practices for emergency action plans to distinguish areas of conformance and shortfalls. The three columns on the right of the tables are provided for agency analysis.

Employee Emergency Plans and Fire Prevention Plans [OSHA 29 CFR § 1910.38]	Compliance with Requirement or Standard		
	Yes	No	Comments
Emergency escape procedures			
Escape routes			
Procedures to be followed by employees who remain to operate critical plant operations before they evacuate			
Procedures to account for all employees after evacuation has been completed			
Duties for employees designated to perform rescue and medical functions			
The preferred means of reporting fires and other emergencies			
The names or regular job titles of people or departments that can be contacted for further information or explanation of duties under the plan.			

Emergency Drills and Review of Emergency Plans [OSHA 29 CFR § 1910.38]	Compliance with Requirement or Standard		
	Yes	No	Comments
Objectives of the drill			
Frequency of drills			
Nature of drills—announced versus surprise			
Drill safety and assessment of means of egress			
Roles and responsibilities of emergency evacuation staff			
Accountability of building occupants			
Staff roles and responsibilities			
Coordination with fire department			
Coordination within the facility			

National Fire Protection Association Standards (NFPA)

The NFPA establishes national standards for fire drills in codes such as NFPA 1, Fire Prevention Code, and NFPA 101®, Life Safety Code®, which are commonly adopted by many local jurisdictions.

Under NFPA 1, emergency action drills are required for those buildings containing more than 500 occupants. A building may also be required to conduct drill exercises if it contains less than 500 occupants but it houses 100 or more individuals above or below street level. In addition to requiring drills NFPA 1 also requires the following:

- Drills will be conducted periodically
- Drills will be conducted as needed to familiarize occupants with procedures
- Drills will be conducted at both planned and unexpected times
- Drills will vary conditions to address unusual conditions
- All building personnel will participate in drills
- NFPA 1 also requires the establishment of emergency plans covering all building occupants. These plans are to be updated and reviewed on an annual basis.

ASIS International’s Disaster Preparation Guide

American Society for Industrial Security (ASIS) International’s “Disaster Preparation Guide”

Evacuations - ASIS Recommendations	Compliance with Requirement or Standard		
	Yes	No	Comments
Describing the conditions under which evacuation would be ordered.			
Develop evacuation procedures, with appropriate options for the various hazards that avoid potential secondary hazards (i.e., live high voltage wires that could fall; fuel lines that could be ruptured by earthquake explosion; fire damage; etc.).			
Identifying the individual responsible for ordering an evacuation and establishing lines of succession for carrying out evacuation functions.			
Indicating under what conditions it would be safe to complete facility shutdown before ordering general evacuation.			
Describing the alerting and communication systems for signaling impending or immediate evacuation for each type of evacuation your facility may require.			
Procedures for search and rescue teams, if evacuation alarms are inoperative.			
Maps indicating evacuation routes from buildings and the facility site.			

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

Evacuations - ASIS Recommendations	Compliance with Requirement or Standard		
	Yes	No	Comments
Clearly marked evacuation routes throughout company facilities, with two exit options (and fire escapes where needed) for every employee.			
Assuring that all personnel know the evacuation routes, routines, and check-in procedures for both area and site evacuations.			
Helping any handicapped employees to evacuate.			
Special attention to ensure any non-English-speaking employees understand warning signals and know where and how to evacuate the work place.			
Identifying public or company provided safe reassembly areas that will not leave evacuees exposed to adverse weather conditions—below freezing temperatures, driving rains, etc.—or to radiological hazards following a nuclear incident or attack.			
Assigning responsibility in an evacuation to a rear guard to ensure that all personnel get clear.			
An organized head-count to ensure that all facility occupants have exited.			
A system for identifying missing persons.			
Ensuring that vital records are evacuated.			
Identifying critical equipment to be evacuated and explaining how and by whom it will be moved.			
A facility status report to specified company and civil authorities from the responsible onsite person following a site evacuation.			
Periodic evacuation drills for all facilities.			
Designating responsible staff members (by name and title) to maintain and update the evacuation plan on a standby basis.			

Sheltering in Place - ASIS Recommendations	Compliance with Requirement or Standard		
	Yes	No	Comments
Identifying existing shelter space in company facilities.			
Orderly movement to onsite shelter, with a general traffic pattern and ready-made directional signs.			
Assigning corridor, floor, and building wardens to assist employee movement.			
Crisis stocking of food, water, medical supplies, and other necessities for fallout shelter stay (for on-site company shelters only).			
Designating shelter managers and support staff.			

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

Sheltering in Place - ASIS Recommendations	Compliance with Requirement or Standard		
	Yes	No	Comments
Obtaining radiation-measuring devices from local emergency management officials.			
Arranging training for shelter managers and radiological monitors from local and state emergency management officials.			
Receiving and registering additional people from nearby areas, in close coordination with government officials, if company facilities have been included in the local in-place fallout shelter inventory.			
Coordinating with local authorities to identify shelter locations assigned to company employees outside the facility in accordance with the local in-place shelter allocation.			
Printed instructions advising employees of shelter locations and routes to get there, either within the facility or nearby.			
Identifying the individual responsible for maintaining on-site shelters.			
Assuring that key workers required to continue essential operations are provided blast shelter in or near the work place.			
Coordinating all key worker shelter needs with the local government.			
Determining when occupants can be released from shelter.			

Business & Industry Emergency Management Guide	Compliance with Guidelines		
	Yes	No	Comments
Determine the conditions under which an evacuation would be necessary.			
Establish a clear chain of OEP.			
Identify personnel with the authority to order an evacuation.			
Designate “evacuation wardens” to assist others in an evacuation and to account for personnel.			
Establish specific evacuation procedures.			
Establish a system for accounting for personnel.			
Consider employees’ transportation needs for community-wide evacuations.			
Establish procedures for assisting persons with disabilities and those who do not speak English.			
Post evacuation procedures.			
Designate personnel to continue or shut down critical operations while an evacuation is underway.			

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Coordinate plans with the local emergency management office.			
--	--	--	--

Attachment 4: Additional Resources

Telephone Hotlines

- Domestic Preparedness Chemical/Biological Help Line (phone: 800-368-6498, fax: 410-612-0715, e-mail: cbhelp@sbccom.apgea.army.mil) This service provides technical assistance during business hours to eligible State and local emergency responders and their organizations.
- National Response Center Hotline (800-424-8802) A service that receives reports of oil, chemical, biological, and radiological releases and actual or potential domestic terrorism; provides technical assistance to emergency responders; and connects callers with appropriate Federal resources. The hotline operates 24 hours a day, 365 days a year.
- Nuclear Regulatory Commission Operations Center (301-816-5100, collect calls accepted) accepts reports of accidents involving radiological materials.

Authorities / References

- Under 41 CFR § 102-74.250, the decision to activate the OEP must be made by the Designated Official, or by the designated alternate official. After normal duty hours, the senior officer in the Operations Center on duty will represent the Designated Official or his/her alternates and must initiate action to cope with emergencies in accordance with the OEP.
- Code requirements for fire drills, which address emergency evacuation planning, are found in several national standards:
 - Code of Federal Regulations, Title 41, Chapter 102 Federal Management Regulations, Part 102-71, Subpart 102-74.230, Occupant Emergency Program (41 CFR § 102-74.230).
 - Code of Federal Regulations, Title 29, Part 1904 Recording and Reporting Occupational Injuries and Illnesses, Section 39 Reporting Fatality and Multiple Hospitalization Incidents to OSHA (29 CFR § 904.39).
 - Code of Federal Regulations, Title 29, Chapter 1910 Occupational Safety and Health Standards, Section 38 Employee Emergency Plans and Fire Prevention Rules (29 CFR § 1910.38)
 - Code of Federal Regulations, Title 29, Part 1910 Occupational Safety and Health Standards, Section 120 Hazardous Waste Operations and Emergency Response (29 CFR § 1910.120).
 - Code of Federal Regulations, Title 29, Part 1910 Occupational Safety and Health Standards, Section 165 Employee Alarm Systems (29 CFR § 1910.165).
 - Code of Federal Regulations, 29 CFR § 1960 Basic Program Elements for Federal Employee Occupational Safety and Health Matters, Section 16 Compliance with

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Occupational Safety and Health Administration Standards (29 CFR §1960.70), and 29 CFR § 1960, Reporting of Serious Accidents.

- The General Services Administration Accident and Fire Prevention Handbook PBS P 5900.2C.
- U.S. Equal Employment Opportunity Commission, Fact Sheet on Obtaining and Using Employee Medical Information as Part of Emergency Evacuation Procedures, dated October 31, 2001.
- Emergency Preparedness Guide, National Organization on Disability: <http://www.nod.org/emergency>
- The Property Professional's Guide to Emergency Preparedness, BOMA International: http://www.boma.org/pubs/property_gep.htm
- Protecting Buildings And Their Occupants From Airborne Hazards, U.S. Army Corps of Engineers Technical Instruction, October 2001: <http://www.fema.gov/fima/antiterrorism/resources.shtm>
- Emergency Preparedness in the Built Environment, International Facility Management Association (IFMA), November 2001: <http://www.ifma.org/profdev/seminar/catalog/ep.cfm/actionbig=7>
- GSA Occupant Emergency Program (OEP) Guide, U.S. General Services Administration, March 2002: <http://www.usda.gov/oo/beprepared/OEPplans.htm>
- Shelter-In-Place at Your Office: A general guide for preparing a shelter-in-place plan in the workplace, National Institute for Chemical Studies: <http://www.nicsinfo.org/OEP%20plan%20for%20offices%20NICS%20feb2003.pdf>
- Planning Protective Action Decision-Making: Evacuate or Shelter-in-Place, Oak Ridge National Laboratory, June 2002. <http://www.ornl.gov/>
- Protecting Buildings From a Biological or Chemical Attack: actions to take before or during a release, Lawrence Berkeley National Laboratory, January 2003: <http://securebuildings.lbl.gov/images/BldgAdvice.pdf>
- Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks; CDC and NIOSH, May 2002 (<http://www.cdc.gov/niosh/bldvent/2002-139.html>)
- Risk Management Guidance for Health, Safety and Environmental Security under Extraordinary Incidents, ASHRAE, January 2003 (http://xp20.ashrae.org/ABOUT/Task_Force_Rpt_12Jan02.pdf)
- Emergency Management Guide for Business and Industry, FEMA (<http://www.fema.gov/business/guide/toc.shtm>)
- Critical Incident Protocol, Michigan State University: <http://www.cj.msu.edu/~outreach/CIP/CIP.PDF>
- Evacuation Plans and Procedures e-Tool, OSHA: <http://www.osha.gov/SLTC/e-tools/>

[evacuation/index.html](#)

- Small Business Disaster Planning Guide, Small Business Association, Institute for Business & Home Safety: <http://www.ibhs.org/docs/openforbusiness.pdf>
- Developing a Preparedness Plan and Conducting Emergency Evacuation Drills, National Fire Protection Association: <http://www.nfpa.org/Research/nfpafactsheets/emergency/emergency.asp>
- Model Shelter-in-Place Plan for Businesses, National Institute for Chemical Studies: <http://www.nicsinfo.org/OEP%20plan%20for%20offices%20NICS%20feb2003.pdf>
- Shelter-in-Place in an Emergency, American Red Cross: <http://www.redcross.org/services/disaster/beprepared/shelterinplace.html>
- Business and Industry Preparedness Guide, American Red Cross: http://www.redcross.org/services/disaster/beprepared/busi_industry.html#fema
- Army Training Support Center (<http://www.atsc.army.mil>) provides a digital library with approved training and doctrine information. Files include Field Manuals, Mission Training Plans, Soldier Training Pubs, and more.
- Centers for Disease Control and Prevention (CDC) (<http://www.bt.cdc.gov>) information regarding infectious diseases
- CBIAC: Chemical and Biological Defense Information and Analysis Center (<http://www.cbiac.apgea.army.mil>) Collects, reviews, analyzes, and summarizes chemical warfare/contraband detection (CW/CBD) information.
- Chemical and Biological Warfare – Health and Safety (<http://www.ntis.gov/hs/prep-response.aspx>) Department of Commerce National Technical Information Service (NTIS) site has information on chemical and biological agents, Government research, detoxification and decontamination studies, developing immunizations, and drug theories.
- Chemical Accident Prevention Provisions Overview (CAPPO) (<http://www.epa.gov/emergencies/content/lawsregs/rmpover.htm>) information on the CEPPO office, upcoming events, publications, legislation and regulations, and links to outside resources Also contains information on accident prevention and risk management planning
- Chemical Transportation Emergency Center (CHEMTREC) (<http://www.chemtrec.com/Chemtrec/>) source of technical assistance from chemical product safety specialists, emergency response coordinators, toxicologists and other hazardous materials (HazMat) specialists
- FEMA – Guide for Terrorism Emergency Management (http://www.city.waltham.ma.us/lepcweb/cterr/FEMA_Guide_for_Terrorism.htm) Currently 35 links to various emergency management-related bibliographies. At least 10 of these relate to WMD.
- Federal Radiological Emergency Response Plan (<http://www.nrc.gov/NRC/AEOD/FRERP/downld.html>)

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- U.S. Army Center for Health Promotion and Preventive Medicine (CHPPM) (<http://chppm-www.apgea.army.mil>) Home Page providing links especially requests for CHPPM services. Links connect to Directorates of Environmental Health Engineering, Health Promotion and Wellness, Laboratory Sciences, Occupational Health, and Toxicology.
- U.S. Army Medical Research and Development (R&D) Command (<http://MRMC-www.army.mil>) Links include military infectious disease, chemical and biological links, scientific and technical reports, and Web site links.
- U.S. Army Medical Research Institute of Chemical Defense (<http://chemdef.apgea.army.mil>) provides data links to open literature for medical management of chemical casualties and assay techniques for chemical agents.
- U.S. Army Medical Research Institute of Infectious Diseases (<http://www.usamriid.army.mil>) provides links to Medical Command (MEDCOM), Ebola site, outbreak reporting site, CDC, Defense Technical Information Center (DTIC), U.S. Army, and more.

Cross-Reference Websites

Environmental Protection Agency (EPA)

- [EPA's Chemical Emergency and Prevention Office \(CEPPO\)](#). CEPPO provides leadership, advocacy, and assistance to prevent and prepare for chemical emergencies, respond to environmental crises, and inform the public about chemical hazards in their community.
- [EPA's Environmental Response Team \(ERT\)](#) The ERT is a group of skilled experts in environmental emergencies who provide on-scene assistance on a "round-the-clock" basis to deal with environmental disasters.
- [EPA's Role in Counterterrorism](#). This Web site describes EPA's counterterrorism efforts and shares relevant counterterrorism information and resources.

Department of Defense (DoD)

- [DoD's Chemical and Biological Defense Information Analysis Center](#). This Web site is DoD's focal point for chemical and biological warfare information.
- [DoD's Counter proliferation: Chem Bio Defense](#). This is a DoD "web network" on nuclear, biological, and chemical (NBC) defense.
- [DoD's Hazardous Technical Information Services \(HTIS\)](#) HTIS is a service of the Defense Logistics Agency, located in Richmond, Virginia.
- [DoD's Medical \(Army Surgeon General\)](#). This Web site contains extensive medical documents, training materials, audiovisual clips, a search engine, and links to other sites.

Department of Justice (DOJ)

- Federal Bureau of Investigation (FBI)
- [Awareness of National Security Issues and Response Program \(ANSIR\)](#). The ANSIR is the

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

“public voice” of the FBI for espionage, cyber and physical infrastructure protection.

- [National Domestic Preparedness Office \(NDPO\)](#). The NDPO Web site provides a location for information regarding the available Federal training and programs intended to enhance the capabilities of the public safety community in dealing with weapons of mass destruction (WMD). The NDPO mission, members, services, newsletter, and recommended links are contained on this site.
- [Office for State and Local Domestic Preparedness Support \(OSLDPS\)](#). OSLDPS provides technical assistance to States and local jurisdictions to enhance their ability to develop, plan, and implement a program for WMD preparedness.

Federal Emergency Management Agency (FEMA)

- [Background: Terrorism](#). This FEMA Web site provides basic background information on terrorism-related issues.
- [Terrorism Annex to the Federal Response Plan](#). The site includes the full text of the Annex in PDF format that can be downloaded and reproduced.
- [National Fire Academy](#). The National Fire Academy homepage provides links to the course catalog and to specific courses and job aids relating to terrorism preparedness.
- [FEMA's Emergency Response to Terrorism Self-Study Course](#) - This Web site provides a link to a self-study course designed to provide basic awareness training to prepare first responders to respond safely and effectively to incidents of terrorism.

Department of Health and Human Services

- Office of Emergency Preparedness / [National Disaster Medical System](#) – The website provides information on current and previous disaster responses, counter terrorism programs and links to other Federal sites.
- Centers for Disease Control and Prevention, [Bioterrorism Preparedness and Response Program](#) – The website provides information on bioterrorism preparedness issues, response planning and recent publications related to bioterrorism.
- Centers for Disease Control and Prevention (CDC) also provide helpful (though not comprehensive) lists of chemical and biological agents that might be used by terrorists. These lists are included in “Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response,” in CDC’s [Morbidity and Mortality Weekly Report](#), April 21, 2000 (Vol. 49, No. RR-4).

Federal Law Enforcement Links:

- [Bureau of Alcohol, Tobacco and Firearms \(ATF\)](#)
- [Bureau of Industry and Security \(BIS\)](#)
- [Federal Bureau of Investigations \(FBI\)](#)
- [Drug Enforcement Administration \(DEA\)](#)

- [United States Customs Service](#)
- [United States Secret Service](#)

Useful Links:

- [The Information Security Oversight Office \(ISOO\)](#)
- [Federal Law Enforcement Center \(FLETC\)](#)
- [United States Dept of Justice](#)
- [NOAA Computer Security Program](#)
- [NOAA Office for Law Enforcement \(OLE\)](#)
- [National Counterintelligence Executive \(NCIX\)](#)
- [\(DAVIS/DITIS\) --DOD Poster collection](#)

Acronyms

- ASIS American Society for Industrial Security
- BSC Building Security Committee
- CCT Command Center Team
- CHEMTREC Chemical Transportation Emergency Center
- CPR Cardiopulmonary Resuscitation
- DCT Disaster Control Team
- DO Designated Official
- ERT Emergency Response Team
- FMR Federal Management Regulations
- FPS Federal Protective Service
- FT Floor Team
- FTC Floor Team Coordinator
- GSA General Services Administration
- HAZMAT Hazardous Materials
- HSAS Homeland Security Advisory System
- HVAC Heating, ventilation, and air conditioning
- ICS Incident Command System
- LEPC Local Emergency Planning Commission
- MSDS Material Safety Data Sheet

BACK

[RETURN TO TABLE OF CONTENTS](#)

- NFPA National Fire Protection Association
- NIMS National Incident Management System
- NRP National Response Plan
- OEC Occupant Emergency Coordinator
- OEO Occupant Emergency Organization
- OEP Occupant Emergency Plan
- OSHA Occupational Safety and Health Administration
- SIP Shelter in place

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

[BACK](#)

Protecting the Homeland



U.S. Customs and
Border Protection

[RETURN TO TOP](#)

Emergency Notification Numbers

Fire

Medical Emergency

Building Security

Federal Protective Service

1 – 877 – 437 – 7411

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

RESPONSIBLE OFFICIALS' SIGN-OFF SHEET

A. By their signatures below, the following officials certify that they have participated in the development of this Occupant Emergency Plan (OEP) and fully understand the procedures to be followed in an emergency affecting the facility and the employees for which they are responsible.

Position	Primary		Alternate	
Designated Official	Name		Name	
	Title		Title	
	Signature		Signature	
Occupant Emergency Coordinator	Name		Name	
	Title		Title	
	Signature		Signature	
	Name		Name	
	Title		Title	
	Signature		Signature	

I. PART 1: ORGANIZATION AND RESPONSIBILITIES

A. Introduction

1. The best way to protect against the potentially harmful effects of both man-made incidents and natural disasters is to ensure that all building occupants know how to respond in an emergency. This involves pre-planning, training, and rehearsal.
2. Pre-planning includes establishing the Occupant Emergency Organization (OEO) comprised of employees designated to undertake certain responsibilities to ensure that personnel are moved quickly to safety, that damage to property is minimized, and that proper authorities are notified in the event of a localized emergency, as outlined in this Occupant Emergency Plan (OEP)¹. Training is conducted to ensure that all tenants understand the contents of the OEP and their individual responsibilities. Rehearsals, or drills, provide an opportunity to practice emergency procedures to ensure efficient response in the event of a real emergency.
3. Participation in OEP activities includes all tenants regardless of employment status (e.g., managers, supervisors, OEP team members, volunteers, contracting officers, and hosts of visitors). Each individual must assume the responsibility for own planning and safety in an emergency, as well as working effectively with emergency planning officials.

B. Scope

1. This OEP applies to all _____ employees, support contractors, and visitors and assumes a localized emergency in which the building is impacted in part or in whole.
2. The facility is a _____ located at _____.

C. Effective Date

1. The effective date of this OEP is _____. This document supersedes all previously recognized OEPs for _____. This OEP will be reviewed and updated on an annual basis.

D. Facility-Specific Information

1. Information on the facility, its occupants, and command center is included in the following tables.

¹Federal Management Regulations (FMR), Subpart 102-74.230A requires Federal agencies that occupy Federal property to develop Occupant Emergency Plans with technical assistance provided by GSA for establishing and maintaining them.

E. Command Center Information

Primary Location	Street	
	City, State	
	Telephone	
Alternate Location	Street	
	City, State	
	Telephone	

F. Facility Characteristics

Facility Name	
Address	
Normal Operating Hours	
Required Authorization for Access	
Year Completed	
Number of Floors	
Government Occupied Floors	
Basement(s)	
Gross Floor Area	
Net Assignable Floor Area	
Type of Building Construction	
Emergency Systems Control	
Fire Alarm System and Signals	
Automatic Sprinkler	
In-House Emergency Telephone	
Voice Communications	
Elevator Capture and Recall	
Smoke Detection	
Smoke Control	
Health Unit	
Emergency Lighting	

H. Occupant Emergency Organization (OEO)

1. The Occupant Emergency Organization (OEO) is made up of the following teams that together comprise the building's OEP Emergency Response Team (ERT)¹:

(a) The Command Center Team (CCT) directs all emergency operations from the building's Command Center. CCT members in a large facility, would include:

- o Designated Official (DO) – The highest-ranking official of the primary occupant agency; or alternatively, a designee selected by mutual agreement of occupant agency officials. Responsible for activating the plan in all emergencies during normal duty hours.
- o Occupant Emergency Coordinator (OEC) – An official appointed by the Designated Official and serves as the primary assistant to the Designated Official to ensure the continued viability of the OEP and its organization. During emergencies the OEC operates the Command Center.
- o Floor Team Coordinator – Supervises and expedites the planned and controlled movement of all building occupants in an emergency.
- o Damage Control Team Coordinator – Controls dangerous conditions until further help arrives to assess potential and real damage.
- o Medical Coordinator – The head of the Health and First Aid Unit and is responsible for training and equipping all employees assigned to perform first aid in an emergency.
- o Administrative Officer – Records emergency procedures and activities.
- o Technical Advisors – Occupants familiar with the building's utilities and mechanical systems or other areas of expertise who advise the DO and OEC.

2. In a small facility, some positions, such as Administrative Officer, Medical Coordinator, and Floor Team Coordinator, may not be needed; or one person could perform several functions.

(a) Floor Teams are assigned to each floor of a facility. In a large facility, a typical Floor Team would include:

- Floor Monitors – supervisory personnel selected by the individual Tenant Agency. During a supervisor's absence, there should be an acting supervisor who should assume the Floor Monitor responsibility. In agencies where the supervisory employee is frequently assigned outside the office, a responsible, conscientious, non-supervisory staff employee may be selected. Floor monitors act in several different capacities, depending on the emergency.
- Floor Area or Wing Monitors – one is assigned for each major area of the floor.

[RETURN TO TOP](#)

- Stairwell Monitors – support the Area/Wing Monitors by controlling movement of persons on stairways.
- Elevator Monitors – support the Area/Wing Monitors; one is assigned for each floor where elevators may be captured.
- Exit Monitors – support floor monitors for street and ground level.
- Monitors for Disabled – employees appointed by the floor wardens to assist people with special needs during emergencies. Where possible, two monitors should be assigned to each person. In an emergency, monitors are responsible for remaining with the person throughout the emergency and assisting in their evacuation, following the instructions of the command center and/or the floor warden.

(b) The Damage Control Team consists of the Property Manager and other individuals familiar with the facility’s construction, equipment, and overall operating system. Team members report to the Damage Control Coordinator.

3. OEO personnel are provided with the following visual identifiers to be used during activation of the OEP:

Visual Identifier

Part 4 provides an overview of general responsibilities for these personnel.

NOTE: DELETE CONTENT IN PART 4 THAT IS NOT APPLICABLE TO THE FACILITY

II. PART 2: ACTIVATION AND CONTACT INFORMATION

A. The activation and implementation of this OEP is conducted by the Designated Official (DO) and coordinated from the building’s Command Center (CC).

[MODIFY TEXT TO REFLECT FACILITY-SPECIFIC PROTOCOL]

1. Who makes the decision to activate?

(a) Normal Duty Hours - Designated Official, or by the Designated Alternate Official.

(b) After Normal Duty Hours - The senior official on duty will represent the Designated Official or his/her alternates and must initiate action to cope with emergencies in accordance with the OEP.

(c) How is the decision made?

- o The decision to activate is based upon the best available information, including an understanding of local tensions, the sensitivity of target agency(ies), and previous experience with similar situations. Advice shall be solicited, when possible, from the GSA building manager, appropriate Federal Protective Service official, and Federal, State, and local law enforcement agencies.
- o If there is immediate danger to persons or property (e.g., fire, explosion, or the discovery of an explosive device (not including a threat)), evacuate or relocate occupants in accordance with this OEP without outside consultation. Sound the fire alarm system or use other appropriate means to signal evacuation.

B. Facility Emergency Contact Information

GENERAL SERVICES ADMINISTRATION Facility Contacts				
Position	Primary		Alternate	
Property Manager	Name		Name	
	Phone		Phone	
	Mobile		Mobile	
Building Engineer	Name		Name	
	Phone		Phone	
	Mobile		Mobile	
[ADD OTHER CONTACTS AS NEEDED]	Name		Name	
	Phone		Phone	
	Mobile		Mobile	

FEDERAL PROTECTIVE SERVICE Facility Contacts				
Position	Primary		Alternate	
Building Security	Name		Name	
	Phone		Phone	
	Mobile		Mobile	
FPS Inspector	Name		Name	
	Phone		Phone	
	Mobile		Mobile	
FPS MegaCenter	Phone		Phone	
[ADD OTHER CONTACTS AS NEEDED]	Name		Name	
	Phone		Phone	
	Mobile		Mobile	

COMMAND CENTER TEAM (CCT)				
Position	Primary		Alternate	
Designated Official	Name		Name	
	Phone		Phone	
	Mobile		Mobile	
Occupant Emergency Coordinator	Name		Name	
	Phone		Phone	
Floor Team Coordinator	Name		Name	
	Title		Title	
	Phone		Phone	
Damage Control Coordinator	Name		Name	
	Title		Title	
	Phone		Phone	
Medical Team Coordinator	Name		Name	
	Title		Title	
	Phone		Phone	

COMMAND CENTER TEAM (CCT)				
Position	Primary		Alternate	
Technical Advisor: Safety and Health	Name		Name	
	Title		Title	
	Phone		Phone	
Technical Advisor: Physical Security Specialist	Name		Name	
	Title		Title	
	Phone		Phone	
Administrative Officer	Name		Name	
	Title		Title	
	Phone		Phone	

FLOOR TEAM:	Floor Number			
Position	Primary		Alternate	
Floor Monitor	Name		Name	
	Phone		Phone	
	Mobile		Mobile	
Area or Wing Monitor	Name		Name	
	Phone		Phone	
	Mobile		Mobile	
Stairwell Monitor	Name		Name	
	Phone		Phone	
	Mobile		Mobile	
Elevator Monitor	Name		Name	
	Phone		Phone	
	Mobile		Mobile	
Exit Monitor	Name		Name	
	Phone		Phone	
	Mobile		Mobile	
Monitor for Disabled Occupants	Name		Name	
	Phone		Phone	
	Mobile		Mobile	

NOTE: DUPLICATE THE FLOOR TEAM TABLE SO THAT THERE IS ONE FOR EACH FLOOR IN THE BUILDING

DAMAGE CONTROL TEAM					
Position	Primary			Alternate	
Building Manager	Name			Name	
	Phone			Phone	
	Mobile			Mobile	
[ADD OTHER POSITIONS AS APPROPRIATE]	Name			Name	
	Phone			Phone	
	Mobile			Mobile	

III. PART 3: EMERGENCY PROCEDURES

A. Emergency procedures are provided for the following:

1. [Medical– Localized and Widespread](#)
2. [Evacuation](#)
3. [Hazardous Substance](#)
4. [Bomb Threat](#)
5. [Suspicious Object](#)
6. [Explosion](#)
7. [Natural Disaster – with advance notice and without](#)
8. [Demonstrations](#)
9. [Missing Child – Code Adam](#)
10. [Enhanced Protection Due to Increased Threat](#)
11. [Shelter-in-Place](#)
12. [Post-Incident Recovery](#)

NOTE: MODIFY TEXT TO REFLECT FACILITY-SPECIFIC EMERGENCY PROCEDURES AND CONTINGENCY PLANS

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Medical		
Position	ACTIONS	
	Limited	Widespread with Multiple Injuries
ALL Building Occupants		
All Building Occupants	<ul style="list-style-type: none"> • CALL 911 [or] • If First Aid/CPR trained, provide assistance until medical personnel arrive. 	
Command Center Team		
DO/OEC	<ul style="list-style-type: none"> • Notify Floor Monitor • Notify Medical Coordinator 	<ul style="list-style-type: none"> • Go to Primary Command Center • Activate Command Center Team
Medical Coordinator	<ul style="list-style-type: none"> • Go to scene • Ensure that appropriate assistance has been called • Recommend follow-up action • Report to DO 	<ul style="list-style-type: none"> • Go to scene • Advise regarding medical assistance and ensure that appropriate assistance has been summoned • Report to DO
All other CCT members	NA	<ul style="list-style-type: none"> • Go to Primary Command Center • Notify or activate teams as appropriate.
Floor Team		
Floor Team Members	NA	<ul style="list-style-type: none"> • Provide first aid/CPR • Obtain medical assistance (see emergency call list) • Notify OEC • Notify Federal Protective Service • Reserve elevators for emergency use • Meet responding emergency unit at ground floor • Verify medical assistance response • Report to Floor Team Monitor
Damage Control Team		
Damage Control Team Members	NA	<ul style="list-style-type: none"> • Provide first aid/CPR and rescue services. • Report to Damage Control Coordinator.

Evacuation			
Position	ACTIONS		
ALL Building Occupants			
All Building Occupants	<ul style="list-style-type: none"> • Activate the nearest fire alarm pull box then dial _____ to notify _____ and provide specifics. • Follow instructions provided by the Command Center Team. 		
Command Center Team			
DO/OEC	<ul style="list-style-type: none"> • Go to Primary Command Center and activate the Command Center Team • Verify fire department notification and response and brief responding personnel • Coordinate activities 		
Medical Coordinator	<ul style="list-style-type: none"> • Go to Primary Command Center and advise regarding medical assistance 		
Floor Team Coordinator	<ul style="list-style-type: none"> • Go to Primary Command Center and activate Floor Teams and coordinate Floor Team activities and verify occupant status 		
Damage Control Coordinator	<ul style="list-style-type: none"> • Go to Primary Command Center and activate the Damage Control Team • Determine building conditions (e.g., environmental, structural, etc.) 		
Administrative Officer	<ul style="list-style-type: none"> • Go to Primary Command Center and record activities 		
Floor Team	Fire Floor	First Floor	Other Floors
Floor Monitors	<ul style="list-style-type: none"> • Activate fire alarm (if not already done). • Supervise and verify evacuation. • Report to Floor Team Coordinator. 	<ul style="list-style-type: none"> • Lead fire department to control center. • Restrict building access. • Assist with occupant evacuation 	<ul style="list-style-type: none"> • If floor is to be evacuated, follow Fire Floor Team instructions. • If not, stand by for instructions
Area Monitors	<ul style="list-style-type: none"> • Evacuate area occupants • Inspect area to ensure total evacuation • Report status to Floor Monitor. 		
Elevator Monitors	<ul style="list-style-type: none"> • Direct occupants to the nearest safe stairwell. • Assist in elevator evacuation of the disabled if elevator use of this purpose has been authorized. 	<ul style="list-style-type: none"> • Report to First Floor Monitor • Capture assigned elevators. • Use of elevators can be authorized only by the fire department, DO, or OEC. 	
Stairway Monitors	<ul style="list-style-type: none"> • Inspect stairway for smoke or other obstruction and report status to Area Monitor. • Keep occupants moving in a single file down the stairway. 	<ul style="list-style-type: none"> • Lead fire department to control center. • Restrict building access. • Assist with occupant evacuation 	
Monitors for Disabled	<ul style="list-style-type: none"> • Evacuate disabled to safe area. • Report status to Area Monitor 		
Damage Control Team			
Damage Control Team Members	<ul style="list-style-type: none"> • Report to Damage Control Coordinator and activate emergency systems 		

Hazardous Substance	
Position	ACTIONS
ALL Building Occupants	
All Building Occupants	<ul style="list-style-type: none"> • Dial ___ to notify and provide specifics. • Follow instructions provided by the Command Center Team.
Command Center Team	
DO/OEC	<ul style="list-style-type: none"> • Activate Command Center Team. • Determine if an evacuation is appropriate: <ul style="list-style-type: none"> o If yes, follow evacuation procedures. o If no, follow shelter-in-place procedures. • Notify fire department. • Notify Federal Protective Service. • Notify appropriate utility company or hazard materials expert. • Go to Alternate Command Center. • Hold occupants at relocation site. • Do not permit reentry until determined safe by proper authorities. • In case of explosion, follow instructions under Bomb Explosion.
All Other CCT Members	<ul style="list-style-type: none"> • Go to Primary Command Center. • Notify or activate appropriate teams as appropriate.
Floor Team	
Floor Monitors	<ul style="list-style-type: none"> • Activate Floor Teams. • Supervise evacuation. • Report to Floor Team Coordinator at relocation site Alternate Command Center.
Area Monitors	<ul style="list-style-type: none"> • Coordinate area evacuation. • Report conditions to Floor Monitors. • Accompany area occupants to relocation site. • Hold occupants and await instructions.
Stairwell Monitors	<ul style="list-style-type: none"> • Control evacuation via stairways. • Report to Area Monitors.
Monitors for the Disabled	<ul style="list-style-type: none"> • Assist individuals requiring assistance to relocation site. • Remain with disabled. • Report to Area Monitors when possible.
Elevator Monitors	<ul style="list-style-type: none"> • Go to relocation site. • Report to Floor Monitor.
Damage Control Team	
Damage Control Team Members	<ul style="list-style-type: none"> • Report to Damage Control Coordinator at relocation site Command Center

Bomb Threat			
Position		ACTIONS	
ALL Building Occupants			
All Building Occupants		<ul style="list-style-type: none"> • Dial ___ to notify and provide specifics. • Follow instructions provided by the Command Center Team. 	
Command Center Team			
DO/OEC		<ul style="list-style-type: none"> • Go to Primary Command Center • Verify FPS notification and response 	
All Other CCT Members		<ul style="list-style-type: none"> • Go to Primary Command Center. • Notify or activate appropriate teams as appropriate. 	
Floor Team	Affected Floors	First & Ground Floors	Unaffected Floors
Floor Monitors	<ul style="list-style-type: none"> • Initiate evacuation/relocation. • Supervise and verify evacuation. • Report to Floor Team Coordinator. 	<ul style="list-style-type: none"> • Control building access. • Keep people away from building perimeter • Control occupant movement, according to instructions received from Primary Command Center 	
Area Monitors	<ul style="list-style-type: none"> • Instruct occupants to search their work areas. • Evacuate/relocate occupants. • Inspect area to ensure total evacuation. • Search assigned public areas and exit routes. • Report to Floor Monitors. 	NA	
Elevator Monitors	NA	NA	
Stairwell Monitors	<ul style="list-style-type: none"> • Inspect stairwells and exit routes. • Lead occupants to safe area. • Report to Area Monitors. 	NA	
Disabled Occupant Monitors	<ul style="list-style-type: none"> • Verify status of disabled occupants. • Report to Area Monitors. 	NA	
Damage Control Team			
Damage Control Team Members		<ul style="list-style-type: none"> • Search assigned areas including maintenance, storage, outside, and rooftop areas 	

Sample Bomb Threat Checklist

Following is information to be recorded by a bomb threat message recipient during or immediately after the threat is communicated.

Date _____

Time _____

Time Caller Hung Up _____

Phone Number Where Call Was Received _____

Questions to ask Caller:

Where is the bomb located? (Building, Floor, Room, etc.) _____

When will it go off? _____

What does it look like? _____

What kind of bomb is it? _____

What will make it explode? _____

Did you place the bomb? (Yes, No) _____

Why? _____

What is your name? _____

Where are you? _____

Record Exact Words of Threat: _____

Record Information About Caller: _____

Where is the caller located? (Background and level of noise) _____

Estimated age _____

BACK

Is the voice familiar? If so, who does it sound like? _____

Other Points: _____

Caller's Voice _____

CIRCLE ANY THAT APPLY

Caller's Voice:

- Accent
- Angry
- Calm
- Clearing throat
- Coughing
- Cracking voice
- Crying
- Deep
- Deep breathing
- Disguised
- Distinct
- Excited
- Female
- Laughter
- Lisp
- Loud
- Male
- Nasal
- Normal
- Ragged
- Rapid
- Raspy
- Slow
- Slurred
- Soft
- Stutter

Background Sounds:

- Animal Noises
- House Noises
- Kitchen Noises
- Street Noises
- Booth
- PA System
- Conversation
- Music
- Motor
- Clear
- Static
- Office machinery
- Factory machinery
- Local
- Long distance

Threat Language:

- Message Read Incoherently
- Taped
- Irrational
- Profane
- Well-spoken

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Suspicious Object			
Position		ACTIONS	
ALL Building Occupants		<u>Signs of a Suspicious Package</u>	
All Building Occupants		<ul style="list-style-type: none"> No Return Address Excessive Postage Stains Strange Odor Strange Sounds 	
Command Center Team		Unexpected Delivery	
DO/OEC	<ul style="list-style-type: none"> • Go to Primary Command Center • Activate Command Center Team • Verify fire department notification and response • Brief responding personnel • Evacuate or relocate occupants • Building Manager to put elevators in Phase I Service. 	<ul style="list-style-type: none"> Poorly Handwritten Misspelled Words Incorrect Titles Foreign Postage 	
All Other CCT Members	<ul style="list-style-type: none"> • Go to Primary Command Center. • Notify or activate appropriate teams as appropriate. 	Restrictive Notes	
Floor Team	Affected Floors	First and Ground Floors	Unaffected Floors
Floor Monitors	<ul style="list-style-type: none"> • Carry out evacuation or relocation plan. • Supervise and verify evacuation. • Report to Floor Team Coordinator. 	<ul style="list-style-type: none"> • Control building access. • Keep people away from building perimeter 	After evacuation, restrict use of elevators, escalators and stairwells
Area Monitors	<ul style="list-style-type: none"> • Coordinate area evacuation. • Determine location of suspicious object; avoid using stairwells, elevators or escalators in immediate area. • Inspect area to ensure total evacuation. • Report status to Floor Monitor. 		
Elevator Monitors	NA	<ul style="list-style-type: none"> • Report to First Floor Monitor. • Hold elevators and assist emergency units. 	
Stairwell Monitors	<ul style="list-style-type: none"> • Inspect stairwells and exit routes. • Lead occupants to safe area. • Report status to Area Monitors. 	NA	NA
Disabled Occupant Monitors	<ul style="list-style-type: none"> • Coordinate evacuation if disabled occupants. • Report status to Area Monitor. 	NA	NA
Damage Control Team			
Damage Control Team Members	NA	NA	NA

Explosion			
Position		ACTIONS	
ALL Building Occupants			
All Building Occupants		<ul style="list-style-type: none"> • Dial ___ to notify ___ and provide specifics. • Follow instructions provided by the Command Center Team. 	
Command Center Team			
DO/OEC		<ul style="list-style-type: none"> • Go to Primary Command Center. • Activate Command Center Team. 	
All Other CCT Members		<ul style="list-style-type: none"> • Go to Primary Command Center. • Notify or activate appropriate teams as appropriate. 	
Floor Team	Affected Floors	First and Ground Floors	Unaffected Floors
Floor Monitors	<ul style="list-style-type: none"> • Notify Floor Team. • Supervise evacuation, first aid, and rescue. • Report conditions to Floor Team Coordinator. 	<ul style="list-style-type: none"> • Control access to the building 	<ul style="list-style-type: none"> • Inform occupants. • Maintain control of occupants. • Control egress. • Maintain communication with Floor Team Coordinator. • Evacuate to a safe area if instructed to do so by Floor Team Coordinator.
Area Monitors	<ul style="list-style-type: none"> • Coordinate area evacuation, first aid, and rescue. • Inspect area to determine conditions. • Report to Floor Monitor. 		
Elevator Monitors	NA	<ul style="list-style-type: none"> • Capture elevators. • Hold until determined safe for use. • Assist emergency teams. 	
Stairwell Monitors	<ul style="list-style-type: none"> • Inspect assigned stairwell. • Report conditions to Area Monitors. • Lead occupants to safe area if required. 	NA	
Monitors for Disabled	<ul style="list-style-type: none"> • Move disabled occupants to safe area. 		
Damage Control Team			
Damage Control Team Members		<ul style="list-style-type: none"> • Assist in rescue. • Control access. • Inspect elevators, fire protection systems, and utilities. • Report conditions to Damage Control Team Coordinator. Make required repairs. 	

Natural Disaster		
Position	ACTIONS	
	Advance Notice	No Advance Notice
ALL Building Occupants		
All Building Occupants	<ul style="list-style-type: none"> Follow instructions provided by the Command Center Team. 	
Command Center Team		
DO/OEC	<ul style="list-style-type: none"> Activate the Command Center Team. Review plans and decide course of action Notify occupants. 	
Medical Coordinator	<ul style="list-style-type: none"> Go to scene Ensure that appropriate assistance has been called Recommend follow-up action Report to DO 	<ul style="list-style-type: none"> Go to scene Advise regarding medical assistance
Floor Team Coordinator	<ul style="list-style-type: none"> Review plans with floor monitors 	<ul style="list-style-type: none"> Go to Primary Command Center Coordinate and assist Floor Teams
Damage Control Coordinator	<ul style="list-style-type: none"> Activate DCT for damage prevention work. 	<ul style="list-style-type: none"> Go to Primary Command Center Activate Damage Control Team
Administrative Officer	<ul style="list-style-type: none"> NA 	<ul style="list-style-type: none"> Go to Primary Command Center Record activities
Floor Team		
Elevator Monitors	NA	<ul style="list-style-type: none"> Capture assigned elevators. Restrict use until determined safe (mechanical safety inspection may be required).
Damage Control Team		
Damage Control Team Members	<ul style="list-style-type: none"> Protect windows and doors. Secure outdoor objects. 	<ul style="list-style-type: none"> Assess damage. Determine needs for controlling dangerous conditions. Provide repair, rescue, and first aid services as directed. Isolate unsafe areas. Report to Damage Control Coordinator.

Building Manager to place Elevators in Phase I Service upon complete evacuation.

Demonstrations		
Position	ACTIONS	
	Advance Notice	No Advance Notice
ALL Building Occupants		
All Building Occupants	<ul style="list-style-type: none"> Follow instructions provided by the Command Center Team. 	
Command Center Team		
DO/OEC	<ul style="list-style-type: none"> Go to Primary Command Center Notify Federal Protective Service – if FPS not in area, notify local police department. Notify Floor Team Coordinator. 	
Medical Coordinator	<ul style="list-style-type: none"> Go to scene Ensure that appropriate assistance has been called Report to DO Advise regarding medical assistance 	
Floor Team Coordinator	<ul style="list-style-type: none"> Go to Primary Command Center Activate Ground Level Floor Team 	
Damage Control Coordinator	<ul style="list-style-type: none"> Activate DCT for damage prevention work. 	<ul style="list-style-type: none"> Go to Primary Command Center Activate Damage Control Team
Administrative Officer	NA	<ul style="list-style-type: none"> Go to Primary Command Center Record activities
Floor Team		
Ground Level	<ul style="list-style-type: none"> Secure perimeter doors. Avoid any interaction with demonstrators. Prevent any occupant interaction with demonstrators. Follow instructions in responding to FPS officers and/or local police. 	
Damage Control Team		
Damage Control Team Members	<ul style="list-style-type: none"> Protect windows and doors. Secure outdoor objects. 	<ul style="list-style-type: none"> Assess damage. Determine needs for controlling dangerous conditions. Provide repair, rescue, and first aid services as directed. Isolate unsafe areas. Report to Damage Control Coordinator.

Missing Child - Code Adam	
Position	ACTIONS
ALL Building Occupants	
All Building Occupants	<ul style="list-style-type: none"> • Immediately report lost or missing child notifications to security personnel • Assist in search for missing child according to communicated description
Command Center Team	
DO/OEC	<ul style="list-style-type: none"> • Obtain a detailed description of the missing child. At a minimum, the description should include: name, race, gender, age, eye color, hair color, approximate height, weight, any identifying marks, description of clothing (to include shoe color and style¹), time the child was last seen, last known location. • Direct or take parent/guardian/responsible party to a pre-determined contact location/main staging area for easy access in case more information is needed. • Report information to entrance control posts immediately by issuing a Code Adam Alert for building/ location. • Pass description information to entrance control posts. If available, use a public address (PA) system to broadcast an announcement that a Code Adam Alert is in effect so that all tenants are alerted to look for the missing child. • Establish a central command location to which all Command Center Team members can report and coordinate their efforts with all responding personnel. Notifying a Regional Dispatch Center (i.e. FPS MegaCenter) that a Code Adam Alert has been initiated. • Instruct all access control posts to continue to control/monitor building access in addition to being aware of all people leaving the building. • Advise non-security personnel to participate through observation and reporting only. • Terminate Code Adam Alert when parent/guardian positively identifies child, and safety has been established. If found unharmed and no criminal activity has occurred, reunited child with parent/guardian. • Contact local law enforcement authorities if Alert renders negative results.
Floor Team Coordinator	<ul style="list-style-type: none"> • Coordinate and assist Floor Teams
Administrative Officer	<ul style="list-style-type: none"> • Assist with search efforts; track and document areas that have been searched and cleared. • Record activities/document the incident • Prepare initial report of incident and supplement with other pertinent information in update or follow-up report with original report's case control number
All other CCT Members	<ul style="list-style-type: none"> • Assist with search efforts
Floor Team	
Floor Team Members	<ul style="list-style-type: none"> • Conduct a thorough search of the building to positively identify all children located in the building • Search all potential hiding places, offices, common areas, and exterior areas of the property • If a CCTV system is in place, monitor it closely for the missing child • If CCTV system has capabilities of viewing without interrupting ongoing recording, review video to identify the last time child was seen

¹ A child's clothes may be changed, but an abductor does not usually remove or change shoes

Enhanced Protection Due to Increased Threat
Low Condition (Green): Low risk of terrorist attack. Security partners should consider the following general measures in addition to the facility-specific protective measures they develop and implement:
Refine and exercise as appropriate preplanned protective measures
Ensure that personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency protective measures
Institutionalize a process to ensure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks and that all reasonable measures are taken to mitigate these vulnerabilities
Guarded Condition (Blue): General risk of terrorist attack. In addition to the protective measures taken in the previous threat condition, security partners should consider the following general measures in addition to the facility-specific protective measures they develop and implement:
Check communications with designated emergency response or command locations
Review and update emergency response procedures
Provide the public with any information that would strengthen its ability to act appropriately
Elevated Condition (Yellow): Significant risk of terrorist attack. In addition to the protective measures taken in the previous threat condition, security partners should consider the following general measures in addition to the facility-specific protective measures they develop and implement:
Increase surveillance of critical locations
Coordinate emergency plans as appropriate with nearby jurisdictions
Assess whether the precise characteristics of the threat require the further refinement of preplanned protective measures
Implement, as appropriate, contingency and emergency response plans
High Condition (Orange): High risk of terrorist attack. In addition to the protective measures taken in the previous threat condition, security partners should consider the following general measures in addition to the facility-specific protective measures they develop and implement:
Coordinate necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations
Take additional precautions at public events and possibly consider alternative venues or even cancellation
Prepare to execute contingency procedures, such as moving to an alternate site or dispersing the facility's workforce
Restrict threatened facility access to essential personnel only

Severe Condition (Red): Severe risk of terrorist attack. Under most circumstances, the protective measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the protective measures taken in the previous threat condition, security partners should consider the following general measures in addition to the facility-specific protective measures they develop and implement:

Increase or redirect personnel to address critical emergency needs

Assign emergency response personnel and pre-positioning and mobilizing specially trained teams or resources

Monitor, redirect, or constrain transportation systems

Close public and government facilities

Shelter-In-Place (SIP)	
Position	ACTIONS
ALL Building Occupants	
All Building Occupants	
Command Center Team	
DO/OEC	
Medical Coordinator	
Floor Team Coordinator	
Damage Control Coordinator	
Administrative Officer	
Floor Team	
Floor Team Members	•
Damage Control Team	
Damage Control Team Members	•

A complete procedure should be established for Shelter In Place (SIP) at each facility. The following are sample actions to consider in development of a procedure:

- Notification is received from various sources that there is an outdoor hazard and that SIP is in effect
- Inform building occupants of SIP conditions, direct them to SIP safe zone(s), and account for people
- Notify the Building Security Committee (BSC) members, Federal Security Authorities, property management personnel, and all other occupants of the building about the incident and SIP requirements
- Minimize the rate of air exchange with the outside as to keep indoor concentration as low as possible for as long as possible by closing all windows and doors to the outside, and closing all necessary doors
- Shut-off all HVAC fans and close all HVAC dampers, including exhaust dampers. Shut off other fans such as kitchen and bathroom exhausts. If shutting off these systems takes more time due to the building condition, then shutting off the whole electrical system should be evaluated during SIP proactive planning.
- Do not use elevators – they create a piston effect and can pump air into or out of the building.
- Seal the doors, windows, and vents if necessary.
- Establish communication with outside through a TV, radio, cell phone, or others and ensure that emergency responders know your location(s).

Post-Incident RecoveryImmediately after an emergency, take steps to resume operations:

- As soon as possible, report to the OEP Team following notification of an incident/emergency.
- Maintain contact with all members of the OEP Team and facilitate the flow of information between members of the OEP Team.
- Identify the required support personnel who may be needed.
- Dispatch, as required, members of the OEP Team, to assist in the incident/emergency.
- Assist in the coordination and movement of personnel away from impacted area.
- Advise, in consultation with members of the OEP Team and local authorities, when the building is safe for reoccupation when the incident has concluded sound the All Clear.
- Upon arrival of FPS and/or local authorities, the OEC shall brief emergency responders of the existing emergency.

Within 48 hours of the emergency/incident:

- Call a follow-up meeting of the OEP Team to discuss the events of the emergency
- Reinforce actions/responses, which worked well
- Lessons learned change actions/responses that did not work well
- Recommend changes to the OEP. Local emergency personnel shall be invited, if appropriate
- Responsible for scheduling evacuation drills for their building.
- Determine if any critical operations cannot be disrupted.
- Brief all building occupants on the drill and given assignments.
- Recruit non-occupants of the building to observe the drill and make critical evaluations.
- Notify Safety and Security that a simulated emergency is in progress.
- Decide if occupants are to be evacuated to off-site facilities.
- Notify the relocation center if an off-site evacuation is to be performed
- Identify the locations to be evacuated.
- Ensure all occupants are aware of these different locations and when to use them.
- Post these locations in each area and exercise these evacuations.
- Identify person(s) responsible for ensuring all people have been evacuated.
- Identify when occupant may return.
- Communicate with floor wardens, and conduct visual inspections of the building for evacuation hazards.
- Establish a recovery team, if necessary.
- Establish priorities for resuming operations.
- Continue to ensure the safety of personnel on the property. Assess remaining hazards.
- Maintain security at the incident scene.
- Conduct an employee briefing.
- Keep detailed records. Consider audio recording all decisions. Take photographs of or videotape the damage.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Post-Incident Recovery

- Account for all damage-related costs. Establish special job order numbers and charge codes for purchases and repair work.
- Follow notification procedures. Notify employees' families about the status of personnel on the property. Notify off-duty personnel about work status. Notify insurance carriers and appropriate government agencies.
- Protect undamaged property. Close up building openings. Remove smoke, water and debris.
- Protect equipment against moisture. Restore sprinkler systems. Physically secure the property. Restore power.
- Conduct an investigation. Coordinate actions with appropriate government agencies.
- Conduct salvage operations. Segregate damaged from undamaged property. Keep damaged goods on hand until an insurance adjuster has visited the premises, but you can move material outside if it's seriously in the way and exposure to the elements won't make matters worse.
- Take an inventory of damaged goods.
- Restore equipment and property. For major repair work, review restoration plans with the insurance adjuster and appropriate government agencies.
- Assess the value of damaged property. Assess the impact of business interruption.
- Maintain contact with customers and suppliers.

IV. PART 4: OEO RESPONSIBILITIES

A. Command Center Team (CCT)

Position	Responsibilities
Designated Official	<ul style="list-style-type: none"> • Selects and trains CCT members • Coordinates with all tenants and develops, applies, and maintains an OEP. • Initiates activities to prepare occupants for emergencies and inform them of response procedures. • Ensures that appropriate procedures are followed during emergencies. • Identifies and establishes working relationships with Federal, State, and local agencies that might respond to an emergency in the facility. • Activates the plan if experience warrants doing so, if people or property is in immediate danger, or if the official gets advance notice of an emergency. • Sits on the facility's Emergency Response Team and Building Security Committee.
Occupant Emergency Coordinator	<ul style="list-style-type: none"> • Assists the DO and performs delegated duties as appropriate. • Serves as liaison between DO and other members of the CCT.
Floor Team Coordinator	<ul style="list-style-type: none"> • Assists in the development of the OEP. • Coordinates planning of occupant movement between floors during an emergency. • Coordinates floor, wing, stairwell, elevator, and other monitor activities.

Position	Responsibilities
Technical Advisors	<ul style="list-style-type: none"> • Building Manager (GSA or Lessor) - Works with the OEC and provides information about the building and the operation of its mechanical systems. • Physical Security Specialist and/or FPS Inspector - Works with the OEC; provides advice on security and law enforcement matters; and serves as liaison with Federal and local law enforcement agencies. • Other occupants familiar with the building's utilities and mechanical systems.
Damage Control Coordinator	<ul style="list-style-type: none"> • Assists the OEC. • Identifies utilities, alarm systems, communications equipment, and other pertinent systems and equipment in the building. • Makes recommendations on the use of facilities and equipment. • Maintains emergency call list for utilities and hazardous substances. • Directs Damage Control Team activities.
Medical Coordinator	<ul style="list-style-type: none"> • Assists the OEC. • Identifies available medical emergency services. • Maintains first aid equipment. • Arranges CPR, first aid, and other paramedical training. • Maintains list of personnel with CPR and paramedical training. • Maintains the list of disabled occupants as provided by Floor Monitors.
Administrative Officer	<ul style="list-style-type: none"> • Assists the OEC. • Records enacted emergency procedures. • Maintains organization records and updates them monthly. • Provides required administrative services (phones, faxes, radios, etc.) and prepares reports.

B. Floor Teams

Position	Responsibilities
Floor Monitor (FM)	<ul style="list-style-type: none"> • Assist FTC • Maintain communication with CC during an emergency; provide progress reports on evacuation; notify CC when floor is completely cleared • Designate exact boundaries of floor areas and assign responsibilities for these areas • Make necessary changes in floor organization with approval of the FTC and OECs • Ensure that evacuation routes are clearly identified and posted on bulletin boards, corridor intersections, and office exits and are known to occupants • Maintain a list of disabled occupants and communicate the list to the CC.
Area or Wing Monitors	<ul style="list-style-type: none"> • Work with FM; notify FM when area has been completely cleared • Ensure that evacuation routes are clearly identified and made known to occupants • Direct orderly flow of occupants during drills and emergencies, along the prescribed evacuation routes • Ensure that area or wing is completely vacated, when required • Ensure that windows and doors are closed lights on, and electrical appliances off during fire evacuations • Leave windows and doors open and lights on during bomb threat evacuations • Assign Monitors for the disabled, one per disabled person • Supervise Stairwell Monitors and Monitors for the disabled • Maintain list of disabled occupants including name, telephone extension, room number, and type of disability within area of responsibility; provide revisions to the FM.

Position	Responsibilities
Stairwell Monitors	<ul style="list-style-type: none"> • Support the Area/Wing Monitor • If evacuating because of a bomb threat, search stairwell • Control movement of occupants on stairways, keeping them in single file and moving steadily at a walking pace; instruct occupants to grasp handrails • Keep door open to stairway until the area/wing is clear • Restrict and monitor use of stairwells and escalators as necessary
Elevator Monitors	<ul style="list-style-type: none"> • Assist and Support Area/Floor Monitors • Be familiar with the provisions of GSA Bulletins covering emergency plans for using elevators to evacuate disabled occupants • Be familiar with manual operation of elevators • Capture assigned elevator and permit use only as directed by FM • During fire evacuation, direct occupants attempting to use elevator to appropriate stairway; relinquish control of elevator to firefighting personnel when they arrive • If emergency personnel are arriving by elevator, meet them and direct them to the scene of the emergency • Assist the evacuation of disabled occupants by elevator if elevator has been approved for use
Exit Monitors	<ul style="list-style-type: none"> • Work with FMs • Ensure the exits are open and free of hindrances • Deny unauthorized access to the building • Direct orderly movement of occupants to safety areas • Assist in evacuation of disabled occupants
Monitors for Disabled	<ul style="list-style-type: none"> • Know locations and telephone numbers of the disabled occupants to be assisted, types of disabilities, and the location of crutches, wheelchairs, and other support devices • Know which elevators may be used for evacuation of disabled occupants • Assist disabled occupants from their workplaces to the elevator, down, and out of the building. If elevator cannot be used, assist person to an area adjacent to the nearest safe stairway and get or await help. • Coordinate with the Area and Floor Monitors to ensure that this information is up-to-date

C. Damage Control Team

- Generally, the damage control team’s job is to control dangerous conditions until further help arrives and to assess potential and real danger. This may include the following duties:
- Ensure that appropriate response organization (e.g., Fire Department, Police Department, medical, hazardous materials, etc.) has been notified.
- Initiate reasonable fire suppression or confinement using facility portable fire extinguishers.
- Assist emergency response personnel.
- Disconnect utilities or equipment.
- Conduct bomb search.
- Protect or remove equipment, records, hazardous substances, etc.
- Perform rescue and first aid.
- Make emergency repairs.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.





**APPENDIX 20.5: WORKPLACE VIOLENT BEHAVIOR
PREVENTION PLAN (SAMPLE)**

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Note: This document should be revised and edited to assure that it describes the Workplace Violent Behavior Prevention Plan at your facility. The portions of the document that are underlined must be revised such that the appropriate information is provided. This appendix is provided as a reference only.

I. PURPOSE

A. Workplace Violent Behavior Prevention Plans:

1. Assure that a safe and healthful workplace is maintained;
2. Minimize or eliminate violent behavior (e.g., verbal or physical aggression);
3. Minimize the severity of injuries resulting from violent behavior; and
4. Assure that employees exposed to violent behavior are provided appropriate medical care and counseling.

II. BACKGROUND

- A. Violent behavior of visitors and/or employees in insert name of facility and other locations where facility employees are required to perform their duties is an occupational health hazard. Workplace violence is preventable and most acts of violence in the workplace have warning signs (verbal and non-verbal). Prevention of violence in the workplace greatly enhances services provided by allowing staff to safely interact with visitors and other employees. Additionally, preventive measures reduce costs associated with work-related injuries.
- B. Insert name of facility is required by Federal law ([Public Law 91-596](#) and [Executive Order 12196](#)) to provide a place of employment free from recognized hazards that are causing or are likely to cause death or serious physical harm. The Occupational Safety and Health Administration (OSHA) has cited Federal facilities for failing to protect its workers from violent behavior in accordance with Executive Order 12196, "Occupational Safety and Health Programs for Federal Employees," paragraph 1-201a.

III. Policy

- A. Violent behavior will not be tolerated at this facility. Persons committing acts of violence will be reported to the appropriate authorities and prosecuted to the fullest extent of the law. Appropriate disciplinary action will be instituted against employees, customers and visitors who are verbally or physically aggressive.

IV. RESPONSIBILITIES

A. The Facility Director is responsible for:

1. Assuring that employees are provided a safe and healthful work environment;
2. Notifying appropriate law enforcement agencies when a CBP visitor or employee is assaulted as a result of direct or indirect employment-related involvement within the workplace.

Note: Each facility should designate an appropriate official to coordinate development and implementation of the facility's Plan. Facility organizations (such as Health Services, Police and Security Service, and the Safety Office) must work together to assure that this Plan is effective. Other organizations that should be involved include emergency medical care personnel, social welfare workers, and nursing service. It is recommended that a representative of one of these offices be designated as the coordinator, and that representatives of these organizations serve as a subcommittee of the Facility Safety Committee. If a representative from one of these organizations is designated as coordinator, the appropriate section (C, D, or E) can be combined with this paragraph.

B. [Insert appropriate title](#) will serve as the facility Workplace Violent Behavior Prevention Plan Coordinator and is responsible for:

1. Coordinating the facility Workplace Violent Behavior Prevention Plan;
2. Assuring that all employees are provided violent behavior prevention training;
3. Reviewing the facility's Plan annually to assure that it is current, relevant, and addresses the facility's needs;
4. Reviewing incident investigation reports prepared by supervisors, conducting incident investigations, if deemed appropriate, and identifying corrective actions to preclude incidents of violence at the facility; and
5. Providing the Facility Safety Committee periodic reports concerning plan effectiveness.

Note: The following responsibilities should be assigned to Health Services or other appropriate clinical organization.

C. [Insert appropriate title](#) is responsible for:

1. Assisting in the presentation of violent behavior prevention training related to assaults, etc.;
2. Assisting and supporting the coordinator and the Facility Safety Committee when implementing an effective Workplace Violent Behavior Prevention Plan throughout the facility; and
3. Assisting with counseling of staff that have been exposed to violent behavior in the workplace, as appropriate.

Note: The following responsibilities should be assigned to the Police and Security Service or other appropriate organization.

D. Insert appropriate title is responsible for:

1. Assuring that incidents involving violence at the facility, in the surrounding neighborhood, or at off-site work areas, are reported and addressed as part of the facility's Workplace Violent Behavior Prevention Plan;
2. Developing recommendations and implementing corrective action(s) intended to preclude recurrence of violence at the facility (in coordination with the requirements of this Plan); and
3. Assisting in the presentation of violent behavior prevention training related to violent behavior throughout the facility.
4. Assisting and supporting the coordinator and the Facility Safety Committee in implementing an effective Workplace Violent Behavior Prevention Plan throughout the facility.

Note: The following responsibilities should be assigned to the Facility Safety Office or other appropriate organization.

E. Insert appropriate title is responsible for:

1. Assuring that incidents of violence involving employees (either as victims or perpetrators) are reported and addressed as part of the facility's Workplace Violent Behavior Prevention Plan;
2. Developing recommendations and implementing corrective action(s) intended to preclude recurrence of violent behavior incidents involving employees (in coordination with the requirements of this Plan);
3. Assisting in the presentation of violent behavior prevention training for employees.
4. Assisting and supporting the coordinator and the Facility Safety Committee in implementing an effective Workplace Violent Behavior Prevention Plan throughout the facility; and
5. Additional Responsibilities: Any additional responsibilities resulting from facility level requirements should be included in paragraphs 1, 2, 3, or 4, as appropriate.

F. Supervisor responsibilities include:

1. Enforcing CBP safety rules, regulations, and standards, including those concerning violent behavior;
2. Identifying unsafe conditions and practices in areas of the supervisor's responsibility and taking prompt corrective action, as appropriate;

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

3. Notifying appropriate personnel of work-related injuries that occur to employees under their supervision;
 4. Investigating injuries or illnesses that occur to employees under their supervision, documenting the investigation, and instituting or recommending corrective actions intended to preclude recurrence of similar injuries;
 5. Assuring that employees under their supervision receive prompt and appropriate medical attention in the event of injury;
 6. Completing compensation forms, when appropriate;
 7. Instructing employees under their supervision in safe work practices and correcting employees that do not follow safe work practices;
 8. Assuring that employees who are verbally or physically assaulted, who witness violent behavior in the workplace, or who have demonstrated warning signs associated with potential violent behavior, are provided counseling, professional support, and critical incident stress debriefings;
 9. Asking for support from the Employee Assistance Program (EAP). The EAP is available to offer professional counseling to those who seek it, and to provide debriefings to individuals and groups affected by trauma. Encouraging employees to take advantage of the EAP as a way of preserving health, not as a sign of sickness;
 10. Initiating disciplinary action, as appropriate, against employees who assault visitors or other employees; and
 11. Assuring that all employees complete appropriate violent behavior prevention training (see paragraph 7).
- G. Employees are responsible for:
1. Following safe work practices (those that minimize the potential for violent behavior);
 2. Recognizing unsafe conditions and immediately taking corrective action to eliminate those unsafe conditions under the control of the employee;
 3. Reporting unsafe conditions to supervisory personnel;
 4. Reporting work-related injuries to supervisory personnel;
 5. Attending OSHA training related to violent behavior prevention; and
 6. Attending counseling and support meetings, as appropriate.

H. Facility Safety Committee is responsible for:

1. Providing assistance and support for the facility Workplace Violent Behavior Prevention Plan and serving as the focal point for facility-wide violent behavior prevention initiatives;
2. Assisting in the development and revision of policies, programs, and procedures related to violent behavior prevention; recommending approval; and evaluating the effectiveness of these policies, programs, and procedures;
3. Recommending and monitoring resource allocations for the facility Workplace Violent Behavior Prevention Plan;
4. Reviewing and commenting on assessments and annual assessment updates (including corrective actions and interim corrective actions) conducted to identify potential sources of violent behavior at the facility or at other work sites where CBP employees are assigned;
5. Identifying trends and developing strategies to reduce or eliminate risks associated with violent behavior at the facility; and
6. Promoting violent behavior-prevention throughout the facility.

I. The Violent Behavior Prevention Subcommittee is a subcommittee of the Facility Safety Committee, consisting of representatives of insert appropriate titles and is responsible for:

1. Assisting the Workplace Violent Behavior Prevention Plan Coordinator in developing and implementing an effective Workplace Violent Behavior Prevention Plan; and
2. Providing technical support and assistance for the facility's Plan.

NOTE: If facility management does not feel that a subcommittee is needed (for whatever reason), this Section could be deleted.

J. Other Appropriate Officials: This Section should be revised to include insert other facility officials that have responsibilities assigned to them as part of the facility's Workplace Violent Behavior Prevention Plan, as appropriate.

V. IDENTIFICATION OF POTENTIAL SOURCES OF VIOLENT BEHAVIOR

A. Assessments of potential sources of violent behavior are conducted by insert appropriate title. A copy of the final report dated insert appropriate date can be obtained in insert appropriate title and location. Following is a list of potential sources of violent behavior:

1. Assessment: While it is good management practice to conduct an assessment of any hazard located within a workplace, such an assessment for violent behavior prevention is not required by Federal regulations. Using assessments to identify potential sources of violent behavior is one method to assure that the facility is in compliance with OSHA regulations. If there have been no potential sources of violent behavior identified, the chances of non-compliance with OSHA regulations or a deficient program greatly increase. Summarize all potential sources of violent behavior identified by the assessment. Any special considerations that may increase the likelihood of violence (e.g., money kept on site, programs that provide services to employees, applicants, etc.) should be noted;
 2. Training: The persons performing the assessment must have completed appropriate training concerning the identification of sources of violent behavior or have appropriate experience;
 3. Maintenance of Records: It is recommended that assessment reports completed as part of the facility's Workplace Violent Behavior Prevention Plan be maintained on file for three years; and
 4. Priorities: Each CBP facility should identify where potential sources of violent behavior are located at the facility. Priority should be given to locations where money is handled; entrances (e.g., facility access by visitors and relatives); isolated areas; poorly lit areas; and security posts.
- B. Employees - Insert appropriate summary of potential violent behavior that could be expected from this group.
1. Employees: Persons committing violence in this category have a direct employment-related involvement with the workplace. This section should recognize frustrations sometimes associated with interaction with customers, or beneficiaries and any specific requirements associated with the services provided at the facility.
 - (a) As Victims - Employees working in the cashier's office, the cafeteria, and the main reception area interact with customers continually. Employees must notify their respective Security Office or police immediately if they suspect that anyone may have a weapon;
 - (b) As Perpetrators - Employees in stressful situations; worried about downsizing or having performance problems; that have deteriorating relationships with other employees, spouses, or associates; or that have been assaulted previously, have the potential for violent behavior. Employees must be informed that all weapons are prohibited at this facility, and possession of a weapon could result in disciplinary action or dismissal.

C. Visitors - Insert appropriate summary of potential violent behavior that could be expected from this group.

1. Visitors: Persons committing violence in this category have an indirect employment-related involvement with the workplace. This category includes current/former spouse or lover, a relative or friend, or some other person who has a dispute involving an employee.

D. Perpetrators of Criminal Activities - Insert appropriate summary of potential violent behavior that could be expected from these groups.

1. Perpetrators of Criminal Activities: This category includes persons who have no legitimate relationship to the facility but may commit criminal acts of violence in and around the workspace. If a facility handles money, the potential for robbery should be addressed. Additionally, the crime rate of the neighborhood surrounding the facility and any necessary precautions (traveling in groups after dark, parking in well lighted areas, etc.) should be discussed.

Note: While the Workplace Violent Behavior Prevention Plan must be communicated effectively to employees, portions of the Plan could contain information that would assist criminals (e.g., locations of locked doors). Such portions of the Plan may need to be considered "confidential" to avoid its misuse by any person intending on committing criminal activity.

E. Annual Assessment Update: Insert appropriate title will perform an update assessment of the potential sources of violent behavior identified at the facility insert appropriate time period, after any significant incident involving violent behavior, and prior to any changes to the use or function of an area that could impact the potential for violent behavior. A report of this update assessment will be provided to the Facility Safety Committee and corrective actions will be developed, as appropriate.

1. Annual Updates: While it is good management practice to conduct an annual assessment of any hazard located within a workplace, such an update is not required by Federal regulations. Annual assessment updates for sources of violent behavior are recommended as one method to assure that the facility is in compliance with OSHA regulations concerning violent behavior prevention. If the current use or function of a location has changed significantly from that at the time of the initial assessment, the chances of non-compliance with OSHA regulations greatly increase.

F. Assessment Training:

1. Training: The personnel assigned responsibility to perform this annual assessment must have completed appropriate training concerning the identification of potential sources of violent behavior or have appropriate experience.

VI. CONTROLS

A. Building Access: Insert appropriate summary of initiatives implemented to prevent violent behavior related to building access.

1. Building Access: This section should summarize all controls related to building access that have been implemented to prevent violent behavior or to limit the impact of such behavior. A summary of facility regulations concerning building access should be included in this section. All employees should be aware of these procedures, which must be discussed during training.

B. Office Access - Insert appropriate summary of initiatives implemented to prevent violent behavior related to office or ward access.

1. Office Access: A description of the office procedures concerning access to restricted areas of the offices or wards should be included in this section. All employees should be aware of these restrictions, and training should address these procedures.

C. Office Configuration - Insert appropriate summary of initiatives implemented to prevent violent behavior related to office or ward configuration.

1. Office Configuration: A description of the office procedures concerning access to restricted areas of individual offices or wards should be included in this section. All employees should be aware of these procedures, and training should address these procedures. Depending upon the configuration of the facility, Sections VI.B and VI.C may be combined.

D. Neighborhood Safeguards - Insert appropriate summary of initiatives implemented to prevent violent behavior related to the neighborhood and surrounding area.

1. Neighborhood Safeguards: A description of the safeguards implemented because of the neighborhood surrounding the building should be addressed in this section. All employees should be aware of these safeguards, and training should discuss these procedures.

VII. TRAINING

A. Employees:

1. Awareness Training: All employees must complete general violent behavior prevention awareness training, which addresses security issues at work, in and around the building, and while on travel;

Note: Awareness training can be either a separate training initiative or can be part of new employee orientation. Females should receive rape prevention training. Males should be invited, and allowed to attend and/or participate in this training. To obtain training materials on Workplace Violence refer to this

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

[OSHA website](#).

2. Customer Service Training: All employees and supervisors of employees that provide services to customers must complete customer service training that addresses methods to recognize potential violent behavior, appropriate responses, methods to obtain assistance, procedures to summon CBP Security or appropriate law enforcement, etc. This training must emphasize prevention, early intervention, and methods to minimize exposure of visitors and employees to violent behavior. Warning signs, response procedures, prevention techniques, and defensive techniques must be addressed by this training.

Note: *This training can be included as part of other customer service enhancement training or can be presented separately. Employees should complete this training before being placed in positions where they may be exposed to potentially violent behavior.*

- B. Supervisors: All supervisors must complete a training program that enables them to identify warning signs of potential violent behavior and learn what to do once violent behavior is detected. The supervisor also needs to be knowledgeable on the counseling services available to an employee.
 1. Supervisor Training: Violent behavior prevention training for supervisors can be included as part of other supervisor training or can be presented separately.

VIII. MEDICAL CARE AND COUNSELING

- A. Emergency Medical Care: Any employee that is injured on the job will be provided medical care by the insert appropriate title and location. If the employee cannot go to the insert appropriate medical personnel will come to the work area. Medical assistance can be obtained by calling the insert appropriate telephone number. If more involved medical care is required, the employee will be transported to insert name and address of appropriate hospital unless otherwise directed by the employee.
- B. Counseling: Supervisors must consult facility Human Resources Management personnel prior to recommending counseling for employees that have been identified as having the potential to act violently. Supervisors of employees that are verbally or physically assaulted or that witness violent behavior in the workplace should contact insert name, address, and telephone number of the Employee Assistance Program to determine the most appropriate method to address the needs of the employee. A traumatic incident can overwhelm an employee's defense mechanisms. The EAP provides counseling to minimize the impact of an operational traumatic incident on employees. Operational traumatic incidents are job-related (not necessarily on-duty) incidents that would cause mental or emotional trauma, such as, but not limited to, direct or indirect involvement in shootings, hostage incidents, suicides, vehicular or plane crashes, threats on life or major injuries. Post-trauma debriefings must be performed as soon as possible but no more than 48 hours after the incident unless the employee is incapacitated or otherwise unable to attend the debriefing within that

[RETURN TO TOP](#)

WARNING: *This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.*

time frame. Counseling and debriefings are provided at no charge by the Employee Assistance Program (EAP). The EAP will provide initial counseling/assessment and refer the employee to community based resources for further treatment, if additional counseling is required. After critical incidents, stress debriefing sessions that include interpersonal support techniques will be provided by insert appropriate title and location.

IX. DISCIPLINARY ACTIONS

- A. Supervisors must consult facility human resources management personnel prior to initiating any disciplinary action associated with violent behavior.

X. INVESTIGATION AND FOLLOW-UP

- A. All incidents of violence in the workplace will be investigated by the employee's supervisor and documented. The insert title and location of the Violent Behavior Prevention Plan Coordinator and the Facility Occupational Safety and Health staff will review the investigation report and will complete an investigation, if deemed appropriate.

Note: Corrective actions identified by the investigations should be implemented within 30 days from the date of the report of the investigation. Those corrective actions that require more than 30 days to implement should be included in the facility's abatement program and interim corrective actions must be implemented.

- B. Training: The persons performing incident investigations must have appropriate training or have appropriate experience.





APPENDIX: SMD/FIELD SECURITY OPERATIONS BRANCH (FUTURE)

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

I. GENERAL

- A. The Security Management Division (SMD) plans to expand operations to support Field Elements at Regional and District Office locations with the establishment of the Field Security Operations Branch.

II. SECURITY MANAGEMENT DIVISION, FIELD SECURITY OPERATIONS BRANCH

- A. SMD will create and staff a Field Security Operations Branch (FSOB) located at Headquarters CBP/IA/SMD. The FSOB primary function is to act as the administrative and operational control activity providing oversight, policies and standard procedures for the field security offices.
1. The FSOB will be required to provide ongoing support and guidance to all the field security staff;
 2. The FSOB Staffing Plan will enhance SMD's capability to meet internal and external customer requirements;
 3. Establish the FSOB as an oversight office at headquarters;
 4. Establish Regional and District Security Offices; identifying areas of responsibility and chain-of-command reporting requirements;
 5. The FSOB, Regional Security Offices (RSOs) and District Security Offices (DSOs) will support the overarching SMD area of responsibility; and
 6. The FSOB will provide security program oversight to all RSOs and DSOs which have been designated by the CBP Chief Security Officer for each of the field locations.

III. ESTABLISHMENT OF REGIONAL AND DISTRICT SECURITY OFFICES

- A. Three Regional Security Offices (RSOs) and thirty District Security Offices (DSOs) will be established and staffed according to the requirements as identified for each location. The FSOB will dedicate three staff members to the RSOs and DSOs within each Region. The RSOs and DSOs will be established to implement the security programs for CBP at each of their respective locations.

B. Regional Security Offices:

1. Three (3) Regional Security Offices (RSOs) will be established near, or co-located with, each of the CBP National Logistics Centers (NLCs). The Regional Security Office is focused on servicing CBP field locations' needs in all disciplines of security, ensuring that CBP maintains a strong security posture that is consistent with departmental and agency security regulations and in compliance

[RETURN TO TOP](#)

with national security policies;

2. The SMD will provide the initial staffing of the Regional Security Offices through temporary duty assignments. The Regional Security Officer is to maintain a multidisciplinary security team that is proactive, flexible, embodies the highest level of professionalism, supported by information technology, and viewed as a model for excellence by other Federal agencies.

C. District Security Offices

1. District Security Offices (DSOs) will be co-located with Office of Internal Affairs field offices. The FSOB will work with the Office of Field Operations, Office of Border Patrol, Air and Marine and Port Security Office to ensure the locations of the DSOs are established in cities which are in close proximity to high-profile ports of entry.

IV. RSO AND DSO SECURITY OPERATIONAL ACTIVITIES

- A. Security compliance and regulatory requirements are established in Presidential and Executive Orders during the establishment of the various programs: Continuity of Operations Oversight Program, Industrial Security Program, Internal Security Program, Operations Security Program and Physical Security Program.

- B. Security specialist will need to be appointed to fill the roles identified below and designated in writing for each of the RSOs and DSOs as appropriate areas of responsibility.

1. Physical Security Program:

(a) Access Control System;

- Key Control System;
- Intrusion Detection System; and
- Badge System/Operation.

(b) HSPD-7, Critical Infrastructure and Key Resource Protection;

(c) National Infrastructure Protection Program;

(d) Classified Facility Construction Requirements;

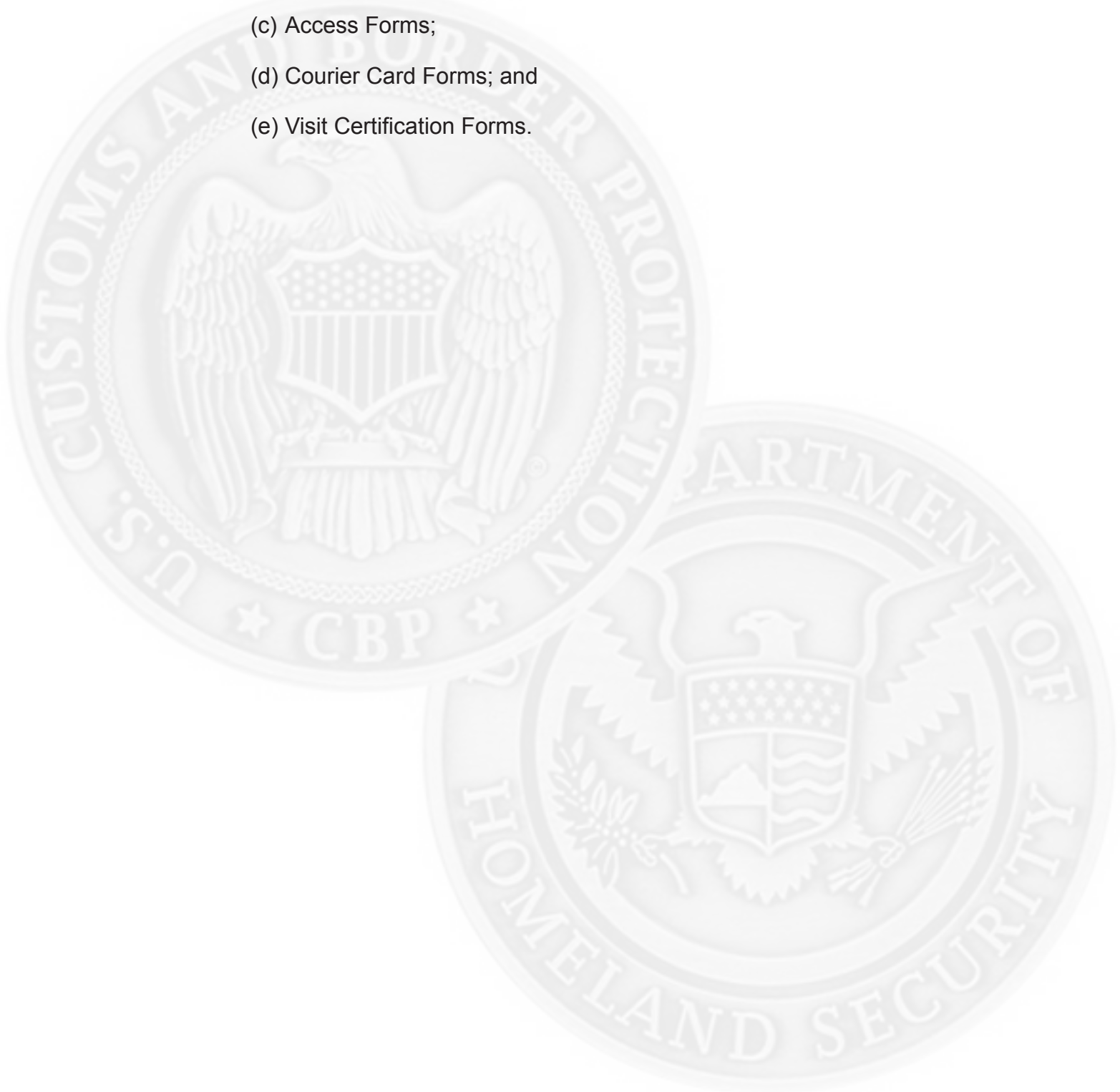
(e) Visitor Control for Government Facilities;

(f) Foreign National Vetting;

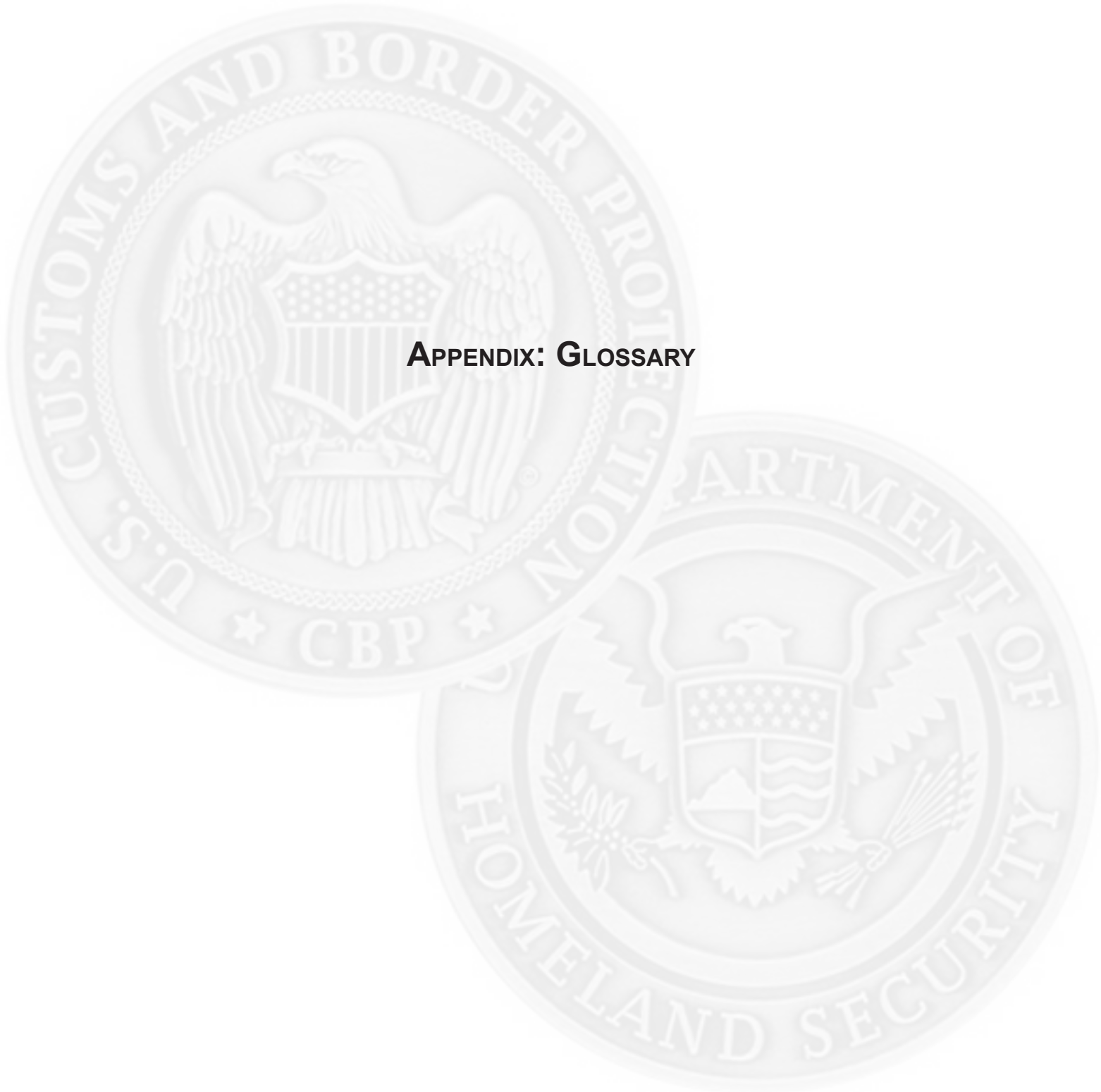
[RETURN TO TOP](#)

- (g) Incoming Visitor Authorization;
 - (h) Alternate Technical Representative for Guard Services;
 - (i) HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors; and
 - (j) Homeland Security Data Network (HSDN).
2. Information Security Program Requirements:
 - (a) Sensitive Security Information Coordinator;
 - (b) Sensitive But Unclassified Information Coordinator;
 - (c) National Security Classified Information; and
 - (d) Self-Inspections.
 3. Industrial Security Program Requirements:
 - (a) Contract Reviews incorporating Security Requirements;
 - (b) Contractor Owned and Operated Facility Inspections.
 4. Internal Security Program:
 - (a) Training and Awareness;
 - (b) Foreign Travel and Foreign Contact Reporting and Briefing/Debriefing;
 - (c) Foreign Visitor Vetting; and
 - (d) Security Issue Review Plan.
 5. Operations Security Program (OPSEC):
 - (a) OPSEC Plan;
 - (b) Occupant Emergency Plan.
 6. Continuity of Operations Oversight Program (COOP) Liaison:
 - (a) CBP Field Office Exercise Plan and Participant;
 - (b) Occupant Emergency Plan.
 7. Personnel Security Program Liaison:

- (a) Suitability & Clearance Forms (Federal and Contract Employees);
- (b) Credential Forms;
- (c) Access Forms;
- (d) Courier Card Forms; and
- (e) Visit Certification Forms.







APPENDIX: GLOSSARY

APPENDIX: GLOSSARY

A.C. or AC. See [Alternating Current](#)

Access. (1) A condition or equipment mode that allows authorized entry into a protected area without alarm by electronically or mechanically deactivating a sensor or sensors. (2) The ability and means to approach, store or retrieve data, or to communicate with or make use of Information Technology resources. (3) The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept if the security measures which are in force are not sufficient to prevent gaining knowledge of the classified information.

Access Code. A group of numbers and/or letters that when properly entered into a specific device allow authorized into a specific area without causing alarm or activating sensors.

Access Control. (1) An aspect of security that utilizes hardware systems and specialized procedures to control and monitor the movement of individuals, vehicles, or materials into, out of, or within secured areas. Access to various points may be a function of authorization level or time, or a combination of the two. (2) The use of physical security as a means of controlling movement into or out of secured areas.

Access Control Card. A card containing coded information that is read by an access control system; access is granted if the card is valid for that specific parameter; ie – date, time, place.

Access-Control System. An electronic, electro-mechanical or mechanical system designed to identify and/or admit authorized personnel to the secure area. Identification may be based on any number of factors such as a sequencing of combinations, special keys, badges, fingerprints, signature, voice, etc. These systems are for personnel access control only and are not to be used for the protection of stored information or materials.

Access Parameters. Specifications programmed or entered into an access control system to define authorization levels, entry times, identification codes and other system information.

Alarm. (1) an alarm device or an alarm signal. (2) One or more detection devices connected to a control device that indicate unauthorized intrusion. (3) An audible or visual warning device triggered by the presence of abnormal conditions in a machine or system.

Alarm Station. (1) A manually actuated device installed at a fixed location to transmit an alarm signal in response to an alarm condition, such as a concealed holdup button in a bank teller's cage. (2) A well-marked emergency control unit, installed a fixed location usually accessible to the public, used to summon help in response to an alarm condition. The control unit contains either a manually actuated switch or telephone connection to fire or police headquarters, or a telephone answering service.

[RETURN TO TOP](#)

Alarm Zone. Smaller subdivisions into which larger areas are divided to permit selective access to some areas while maintaining other areas secure and to permit pinpointing the specific location from which an alarm signal is transmitted.

Alternating Current. Abbreviated AC or A.C. a flow of electricity which reaches maximum voltage in one direction, decreases to zero volts, reverses itself and reaches maximum voltage in the other direction. The cycle is repeated continuously. In the U.S., utility companies provide 60 hertz power to customers.

Ambient Light. The normal, non-manipulated light level for an area.

Americans with Disabilities Act (ADA). Federal act requiring individuals with disabilities be reasonably accommodated.

Annealed. To subject glass or metal to a process of heating and slow cooling in order to toughen, strengthen or harden and reduce brittleness.

Annunciator. (1) A device that signals a change of protection zone status in a security system. An annunciator may log alarms or display a continuous status for each alarm sensor in a system. Annunciators include Cathode Ray Tube displays; sometimes called an alarm receiver, alarm monitor or alarm device. (2) The component of an alarm system that announces a change of status of the systems, usually in the form of audible and/or visual signals.

Area Detection. Coverage of an internal space or volume of a secured area by means of a space or volumetric detector. See [Volumetric Alarm](#).

Armory. An armory is a space within CBP law enforcement and detention facilities for the storage, issuance, and upkeep of weaponry, ammunition, and chemical agents. Armory spaces can include the issuing area, weapons maintenance area, leather storage area, ammunition storage area, and high-powered weapons and ammunition storage area.

Audit Trail. A sequential record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of states and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

Authority Having Jurisdiction (AHJ). An organization (local, state, federal), government office, appointee, or other person having authority to enforce and/or interpret laws, rules, specifications, and approve equipment or procedures.

Authorized Persons. Those persons who have a need-to-know for the classified information involved, and have been cleared for the receipt of such information. Responsibility for determining whether a person's duties require that he/she possess, or have access to, any classified information, and whether he/she is authorized to receive it, rests upon the individual who has possession, knowledge, or control of the information involved, and not upon the prospective recipient. Also includes persons approved to enter a controlled or restricted area.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Badge. An emblem (a small piece of plastic, cloth or metal) that signifies the bearer's status, rank or membership or affiliation. A device, patch, or accoutrement which is presented or displayed to indicate some feat of service, a special accomplishment, a symbol of authority (e.g., police), a simple means of identification. Also referred to in FLETC policy as a badge.

Balanced Magnetic Switch. A two-part sensor that generates an alarm condition when a change in the magnetic field between the parts is detected. Usually mounted on a door and doorframe to detect opening of the door. A balanced magnetic switch provides better protection against a defeat attempt than a standard magnetic contact.

Bar Lock. (1) A type of rim lock in which metal bars slide out from a central point on the door and into receivers on both sides of the door frame. Turning a key or bolt on the center element retracts the bars enough to let the door open. A door with a bar lock cannot be pulled out of its frame even if the hinge pins are removed. (2) a metal rod or tube which slides through fittings affixed to the front of a file cabinet, bent at the top and secured with a combination lock, which holds the drawers closed.

Battery Backup. A standby battery that is kept fully charged for use during a primary power failure. An essential element in all electrically operated security systems. Also called [Uninterruptible Power Supply \(UPS\)](#).

Biometric Access Control. A method of access verification in which the person seeking entry is identified by finger print, retinal eye pattern, palm pattern, hand geometry, voice analysis and similar features.

BNC Connector (Bayonet Neil-Concelman). A standard CCTV coaxial cable connector with a bayonet locking mechanism.

Bollard. A post used as a barrier against or to control pedestrian or vehicular traffic.

Bolt. The part of a lock which, when actuated, is projected (or "thrown") from the lock into a retaining member, such as a strike plate, to prevent a door or window from moving or opening. See also [dead bolt](#), flush bolt, and latch.

Building Security Committee. A committee consisting of representatives of all Federal tenants in the facility, generally responsible for identifying building-specific security issues and approving the implementation of security measures and practices. In the case of new construction or pending lease actions, the Building Security Committee may consist of the design team and planned tenants.

Bypassed. Circumvention of an alarm system, rendering it or a portion of it inoperative.

Camera Dome. Spherical high-impact plastic dome that covers a camera to protect it from the environment or conceals it from view.

Camera Housing. An enclosure designed to protect the CCTV camera from undue environmental exposure, tampering, or theft.

Candela. The unit of luminous intensity in a given direction. One candela is commonly called one candle power.

Capacitance. The property of two or more objects, which enables them to store electrical energy in an electric field between them. The basic measurement unit is the Farad. Capacitance varies inversely with the distance between the objects, so the change in capacitance with relative motion is greater when one object is nearer to the other.

Capacitance Alarm System. An alarm system in which a protected object is electrically connected as a capacitance sensor. The approach of an intruder causes sufficient change in capacitance to upset the balance of the system and initiate an alarm signal. Also called a proximity alarm system.

Capacitance Sensor. An electric condenser that radiates energy and detects changes in the capacitive coupling between an antenna and a ground. When an intruder enters the energy field the balance between the antenna and ground is disrupted, causing an alarm.

Card Access. A type of access control system that uses a card with a coded area or strip, on or inside the card, to actuate a lock or other access control device. To activate the device, the card is inserted into or through a slot where the data in the coded area is read. If the code is accepted, a signal will be transmitted to unlock the device or perform some other access control function. See definition of [Card Reader](#) for more information on types.

Card Key. A card, usually plastic, that contains encoded information to open a locking device.

Card Reader. A device that reads the information on a card key. Card readers may obtain data from access cards by reading punched holes, magnetic spots, stripes or wires, or any of several other methods that use punched, embossed, or embedded information. The reader may be an integral part of the lock, or it can be located in the immediate vicinity. Card readers fall in one of two categories, on-line or intelligent. On-line readers must communicate with a central processor that makes the entry/exit decision and transmits a signal back to the locking device. The intelligent card reader compares the data on the card with preprogrammed parameters and entry or exit is granted or denied by the card reader itself at the reader location. Intelligent readers are also called stand-alone or off-line readers.

Central Station. (1) An organization or business established for the purpose of monitoring subscribers' alarm systems from a centralized monitoring location rather than at the individual sites. Communication with subscriber alarm systems is generally by telephone line, but may be by wireless or direct wire. The central station notifies police or fire services immediately upon receipt of alarm. All alarms are recorded and investigated. Central stations may utilize WATS lines to extend services on a regional or national basis. (2) The control point of a monitoring system that is normally supervised by security personnel.

[RETURN TO TOP](#)

Central Station Alarm System. An alarm system that uses a central station, as distinguished from a proprietary alarm system where the alarm monitoring is done on-site.

Change Key. A key that will operate only one lock or group of keyed-alike locks, as distinguished from a master key.

Cipher Lock. A digital push-button combination type lock.

Classified Information. Official information that has been identified and marked as Top Secret, Secret, or Confidential in the interests of National Security.

Closed-Circuit Television. Abbreviated CCTV. A television system, usually hard-wired, used for proprietary purposes and not for public or general broadcast. Often used in security applications in conjunction with access control, general surveillance, motion detection, or alarm assessment.

Cognizant Security Authority. The Central Intelligence Agency has been designated by the National Foreign Intelligence Board to maintain cognizance over the Department of the Interior's security program relating to approvals for access to, and the receipt, handling, storage, and destruction of Sensitive Compartmented Information (SCI).

Combination. The group of numbers that represent the biting of a key and/or the tumblers of a lock or cylinder.

Combination Lock. A keyless lock which requires the turning of a numbered dial to a preset sequence of numbers for the lock to open. It is usually a three position, manipulation resistant, dial type lock, although cipher locks with push buttons are also referred to as combination locks.

Concrete Masonry Unit (CMU). Cinder block.

Controlled Area. A room, office, building, or facility to which access is monitored, limited or controlled. Admittance to a controlled area is limited to persons who have official business within the area.

Control Unit. The nerve center of the alarm system located on the premises.

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. As of 2004, most implementations of CPTED occur solely within the built environment.

CS-Mount. A CCTV industry standard for lens mounting, consisting of a 1-inch diameter threaded barrel with 32 threads per inch. The distance from the lens mounting surface to the sensor surface is 0.492 inches (12.497 mm).

Custodian. An individual who is designated the responsibility for maintaining the Classified Document Register (DI Form 1834) and the centralized storage for a given functional area, and is charged with the responsibility for safeguarding and accounting for classified information.

Cylinder. A housing that contains a tumbler mechanism and a keyway plug that can only be turned by the correct key. It includes a cam or spindle to transmit rotary action to a lock or latch mechanism.

Credentials. Documentation usually consists of an identity card, badge or a shield, etc., issued by a trusted third party after some form of identity verification. Credentials are utilized as identification showing that an individual is entitled to represent, or exercise official power as, part of a United States Government Agency.

Dead Bolt. A type of bolt that is moved in and out of the strike mechanically without spring action, as by a thumb latch knob. Dead bolt locks are available in single and double configuration; single throw/cylinder dead bolts have an actuating thumb switch on the interior side of the door; double dead bolts utilize a key on both sides of the lock to actuate the lock.

Dead Latch. A spring-actuated latch bolt having a beveled end and incorporating a feature that automatically locks the projected latch bolt against return by end pressure.

Dedicated Line. (1) A power or transmission line with a single function, such as data transmission, or to a single source such as an outlet for a computer. (2) A non-shared telephone line to an individual subscriber from a central station.

Dedicated Mode. Operation of an Automated Information System (AIS) when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts, has all of the following: a) a valid personnel clearance for all information on the system, b) formal access approval for and has signed nondisclosure agreements for all the information stored and/or processed (including all compartments, sub compartments and/or special access programs), and c) a valid need-to-know for all information contained in the system.

Delay. A time interval, measured by an electronic circuit, used to provide a desired alarm feature such as entry/exit delay.

Designated Official. The highest ranking official of the primary tenant agency of a Federal facility or, alternatively, a designee selected by mutual agreement of tenant agency officials. For facilities owned and leased by the U.S. General Services Administration (GSA), the definition appears in Title 41, Section 102-71.20, of the Code of Federal Regulations (41 CFR 102-71.20).

Detector. Any device that senses the presence of an intruder, an intrusion attempt, fire, etc.

Deterrent. Any physical or psychological device or method that discourages action. In the physical security arena, locks or window grills are physical deterrents and the presence of a guard or surveillance camera are psychological deterrents.

Door Closer. A device used to control the closing of a door by means of a spring and either hydraulic or air pressure or by electronic means. Multi-stage closers provide for adjustments of swing, latch, and back swing.

Doppler Effect. The change in the frequency of a wave, as a light wave or sound wave, resulting from relative motion of the source and the receiver.

Dual Technology Sensor. A sensor using two types of sensing technology (e.g. PIR and acoustic sensors) to reduce false alarms.

DUNS. The Data Universal Numbering System (DUNS) is a unique nine-digit numbering system that is used to identify a business.

Duress Alarm. (1) An alarm condition that signals a dangerous situation, such as an intruder. Often unobtrusive sensors so as to not place the victim in greater danger trigger these alarms. Duress alarms are usually designed to silently initiate an alarm, which is annunciated at a remote station or guard post. (2) A sensor used in a duress-sensing capacity.

Egress Button. A switch used near an access controlled door that, when pushed, sends a signal to the controller to release the door locking device. (See also [REX](#))

Electric Door Strike. An electrically activated door locking mechanism consisting of a solenoid and mechanical latching device. Application of electrical power causes the solenoid to withdraw the latching pin so that the door is free to open or to extend the pin to prevent the door from opening.

Electromagnetic Lock. A door lock that uses an electrically actuated magnetic attraction to secure the door. Magnetic locks use no moving parts.

End Device. Any device at the end of an operating network, such as an alarm sensor, access control reader, electrical lock, or hydraulic device.

Entry Function Lockset. A mortise or cylindrical lockset with the outside or both knobs locked or unlocked by an inside thumb turn and unlocked or unlatched by an outside key.

Expanded Metal. An open mesh formed by slitting and drawing sheet metal. It is made in various patterns and metal thickness, with either a flat or irregular surface.

Fail Safe. A condition whereby an electromechanical door lock reverts to the unlocked position in the event of a power failure. This feature may be necessary for compliance with life safety requirements in certain hardware applications.

[RETURN TO TOP](#)

Fail Secure. A condition whereby an electromechanical door lock reverts to a locked position when there is a power failure.

False Alarm. An alarm signal that does not represent a dangerous or unwanted condition, usually caused by some fault or problem in the system.

FIPS 201. Federal Information Processing Standard (FIPS) 201, entitled Personal Identity Verification of Federal Employees and Contractors, was developed to satisfy the requirements of HSPD 12, which is comprised of two (2) specific components PIV-I and PIV-II. FIPS 201 requires that the PIV card be a smart card and the card body is similar to a bank credit card conforming to the [ISO/IEC 7810](#) specification.

- The card must contain both contact and contactless interfaces, which may be provided by two separate integrated circuit chips (ICC) or by one dual-interface ICC. The contact interface must conform to the [ISO/IEC 7816-4:2005](#) specification.
- The contactless interface must conform to the [ISO/IEC 14443](#) specification.
- In most cases, physical access applications will use the contactless interface, although there are special cases in which the contact interface will be used for physical access. This is according to the [NIST FIPS 201 PDF](#), the Standard Publication for Personal Identity Verification (PIV) of Federal Employees and Contractors.

Floor Master Key. A master key which operates all or most lock cylinders on a particular floor of a building.

Foil. An electrically conductive ribbon used for a sensing circuit. Foil is normally between 0.001 and 0.0003 inch in thickness, and from 0.125 to 1.0 inch in width. It is commonly used on windows and other glass applications. The metal strip completes an electrical circuit that if broken, causes an alarm condition. Also called tape.

Foot Candle. A unit of illumination, one foot-candle is the amount of light emitted by one candle in one square foot. Abbreviated as fc. In the International Systems of Units, the unit is lux (lumens per square meter). One foot-candle is equal to 10.76 lux; typically this is approximated as 1 foot-candle being equal to 10 lux.

For Official Use Only (FOUO). The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

General Alarm. The notification, often by annunciation, of an evacuation or readiness alert throughout a facility.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Glassbreak Vibration Detector. A vibration detection system which employs a contact microphone to detect the particular frequency of the cutting or breaking of glass.

Grand Master Key. The key that operates two or more separate groups of locks, which are each operated by different master keys.

GSA. General Services Administration

Hinge. A type of bearing that connects two solid objects such as a door and a door frame. There are many types of door hinges. Four main types include:

- Pivot Hinges, which pivot in openings in the floor and the top of the door frame. Also referred to as a double-acting floor hinge. This type is found already in ancient dry stone buildings;
- Butt/Mortise Hinges, usually in threes or fours, which are inset (mortised) into the door and frame. Most residential hinges found in the U.S. are made of steel, although mortise hinges for out swing doors are often made of brass or stainless steel base to prevent corrosion;
- Continuous Hinges, which run the entire length of the door (also known as “Piano Hinges”); and
- Concealed Hinges, used for furniture doors (with or without self-closing feature, and with or without dampening systems). They are made of 2 parts: One part is the hinge cup and the arm; the other part is the mounting plate.

Hinge Dowel. A dowel or pin which projects from a door jamb into an opening in the edge of a door at its hinge which prevents removal of the locked door even if the hinges or hinge pins are removed.

Holdup Alarm. An alarm that originates from a point where holdup protection is required, such as a bank teller window or store cash register. It is usually a silent alarm to protect the cashier.

[HSPD-7.](#) Homeland Security Presidential Directive 7 instructs Federal departments and agencies to prepare plans for protecting physical and cyber critical infrastructure and key resources (CI/KR), owned or operated, including leased facilities by July 31, 2004.

[HSPD-12.](#) Homeland Security Presidential Directive 12 establishes a policy for a common identification standard for Federal employees and contractors and mandates the establishment of a “mandatory Government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors.”

IDMS. Personal Identity Verification Identity Management System. A system comprised of one or more systems or applications used to manage the identity verification, validation, and issuance processes. A DHS/HQ central data base used to house personal identifiable information for all DHS employees and contractors.

Internal Affairs Background Investigation Database (IABI). A CBP database utilized by CBP/PSD to input CBP personnel's employment, suitability and clearance status for verification purposes by CBP Security personnel.

Industrial Security. That portion of internal security that is concerned with the protection of classified information in the hands of U.S. industry.

Information. Any information or material regardless of its physical form or characteristics, which is owned by, produced by or for, or is under the control of the United States Government.

Infrared Motion Detector. A passive, low power, area protection device that detects a change in ambient temperature within the coverage pattern caused by the movement of a body. Sensor circuitry generates an alarm when a moving object causes a change in radiated energy levels within the coverage area. These units are more sensitive to objects moving across the beam pattern than to objects moving toward the sensor. Also called [Passive Infrared](#).

Infrared Sensor. (1) Passive: detects an intruder by body heat (Infrared Energy), (2) Active: a photoelectric beam that emits infrared to detect an intruder.

Initial Briefing. The initial indoctrination on the national security information provided to personnel prior to being authorized access to classified information and the execution of the Classified Information Nondisclosure Agreement form.

Intrusion Detection System. An alarm system comprised of intrusion sensors and alarm annunciation devices for the purpose of detecting intruders. Typical intrusion detectors include balanced magnetic contact switches and ultrasonic, infrared, or microwave motion or intrusion sensors.

Latch Guard. A plate, such as an astragal, applied to an out swinging door that covers a portion of the door leaf and the door frame at the area where a spring latch or dead bolt enters a strike plate.

Light Meter. A device used to measure the amount of light in a given area.

Line Supervision. A means where a known current is present on the line to the central station. Cutting or shorting the line changes this current, which results in an alarm.

Local Alarm. An alarm that annunciates at the location of a locking device, to discourage or announce intrusion attempts. The alarm usually uses a bell, siren, lighting system or combination of such devices. It usually turns off automatically after a pre-set time, although some require a manual shutoff. A local alarm may also be linked to a central station or other remote location.

Lux. Abbreviation for unit of illuminance set by the International System of Units (SI); lumens per square meter. A measurement of 10 Lux is equal to 1 foot-candle.

Magnetic Contact. A magnetically operated switch, typically used on doors and windows to detect opening.

Magnetic Lock. A type of door lock consisting of an electromagnet and opposing strike plate. When current is applied the strength of the electromagnet secures the door to the strike plate.

Magnetometer. An electronic device used specifically to search personnel for hidden metallic weapons (knives and guns) at entrances to airports, public schools, courthouses, and other guarded spaces. When used with access control equipment, they can perform two functions:

- (1) Detect the presence of concealed metal objects
- (2) Determine the size of those objects
 - Metal is detected by measuring the change in an established magnetic field when dense metal or ferrous materials are moved through the field. The antenna of a detector sets up a magnetic field around itself. As the antenna of the detector is brought near metal or metal is moved past the antenna, the pitch from a tone generator increases, thereby alerting the operator to the presence of metal. Measurement capabilities are adjustable allowing for varying the amount of metal desired to be detected.

Microwave Sensor. An active intrusion sensor that detects the movement of a person or object through a pattern of microwave energy. Microwave sensors are classified as monostatic, bistatic, or terrain following. Generally, they use the [Doppler Effect](#) to recognize movement within a protected area. Bistatic sensors operate on a beam break principle. Terrain-following microwave sensors are essentially bistatic sensors with antenna configurations that are not overall line-of-sight. Monostatic sensors are typically designated for indoor use; bistatic and terrain-following sensors are normally used for outdoor applications.

Mogul Lock. A high-security lock that incorporates a number of features designed to defeat attempts to pick or destroy it. The lock cylinder assembly employs multiple arrays of pass key pins, making picking of the lock much more difficult. The arrangement of the pass key pins in separate arrays requires that multiple cuts would have to be made into the lock housing or cylinder in order to defeat the lock cylinder assembly. The lock cylinder assembly may incorporate multiple sets of hardened dowel pins to prevent drilling through the lock housing in the area of the driver pins.

Mortis Lock. A lock with its case is mortised or recessed into the edge of the door. The most common variety of mortise lock has a door knob on each side of the door; however, entrance doors often have an exterior thumb-latch, rather than a door knob, to open the door. The mortise lock can be locked from the inside by a thumb turn, or by a button on the edge of the lock case. A key is required to lock or unlock it from the outside.

Multiplexer. A device that allows the simultaneous communication of two or more signals for transmission to a remote annunciator or central station. In video, a device that allows a camera to be electronically switched to a variety of image projection and recording devices.

National Security Information. Designated information, which requires protection in the interest of national defense or foreign relations of the United States, that is, information classified in accordance with Executive Order 12356 and not falling within the definition of Restricted Data or Formerly Restricted Data.

Nuisance Alarm. An alarm activation caused by environmental or other unexplained action. See also [False Alarm](#).

OMB. The Office of Management and Budget (OMB) is one of the agencies of the Executive Branch of the U.S. Government. Its predominant mission is to assist the President in overseeing the preparation of the Federal budget and to supervise its administration in Executive Branch agencies.

Passive Infrared Sensor (PIR). A sensor that is sensitive changes in infrared energy. It is designed to detect motion by sensing the change in infrared energy as a human passes in front of its normal background target.

Peened Hinge. A peened hinge is a metal hinge that has had its pins improved by peening. Peening is the process of working a metal's surface usually by mechanical means such as hammer blows or by blasting with shot (shot peening). Peening expands the pins head surface total area and precludes easy removal. Other methods of securing hinge pins include: spot welding, door pinning, and non-removable hinge pins (NRP) which use a set screw to secure the hinge pin; the set screw is accessible only with the door in the open position.

Perimeter Protection. A scheme of protection that uses devices to detect intrusion at points of entry into a protected area such as doors, windows, skylights, etc.

Photo Access Card (PAC). A PAC is a physical artifact, a plastic card issued by CBP to employees, contractors and detailees, which allow the bearers, authorized access to CBP Facilities.

Photoelectric Alarm. A kind of motion detector that uses a focused beam of light (usually ultraviolet) to detect an intruder. Any interruption in the light path will set off the alarm. The beam is usually aimed so that an intruder would have to break the beam in order to move through the protected area. Sometimes called an electric eye.

[PIV-I](#). Specifies the minimum requirements for a Federal Personal Identification Verification (PIV) system that meets control and security objectives of [HSPD-12](#), including the personal identity proofing process. PIV was defined by [NIST](#), the National Institute of Standards and Technology, an agency of the U.S. Commerce Department's Technology Administration dealing with the performance of background checks for employees and contractors.

[PIV-II](#). Provides detailed technical specifications of components and processes required for interoperability of PIV cards with personal authentication, access control, and PIV card management systems across the Federal government and the issuance of smartcards.

Power Supply. A source of operating power such as a generator, transformer, or battery including its circuits, terminations, and connections to the dependant system components.

Propellant-Activated Device. Any tool or special mechanized device or gas generator system that is activated by a propellant or releases or directs work through a propellant charge.

Protected Area. That portion of a premises that is covered by an alarm system.

Proximity Alarm System. See [Capacitance Alarm System](#).

Proximity Card. An identification card containing a microcircuit. When place in close proximity to a card reader, the card will activate the reader's circuitry and register its assigned unique code.

Radiation Detector. A small electronic device about the size of a pager (Personal Radiation Detector) or a hand held electronic device (Radiation Isotope Identification Device) or a large portal (Radiation Portal Monitor) that is capable of detecting gamma and neutron emissions from radioactive isotopes.

The Personal Radiation Detector (PRD) is worn on the Border Protection Officer's utility belt while he/she is on duty. The Radiation Isotope Identification Device (RIID) is used by Border Protection Officers to determine the exact source of a radiation alarm. The Radiation Portal Monitor (RPM) provides a passive, non-intrusive means to screen cars, trucks and other conveyances for the presence of radioactive and nuclear materials.

Refresher Briefing. The periodic reindoctrination on the national security information program provided to personnel with continuing authorized access to classified information.

Restricted Area. A room, office, building, or facility to which access is strictly and tightly controlled. Admittance to a restricted area is limited to personnel assigned to the area or persons who have been specifically authorized access to the area. Visitors to a restricted area and uncleared personnel must be escorted by personnel assigned to the area and all classified and sensitive information must be protected from observation, disclosure or removal.

REX. A request to exit device. See [Egress Button](#)

Risk. The possibility of suffering harm or loss.

Risk Analysis. An analytical tool used to minimize risk by applying security measures commensurate with the threats, vulnerabilities, and values of the asset(s) to be protected.

Risk Assessment. A detailed study of the vulnerabilities, threats, likelihood, loss or impact of loss and theoretical effectiveness of security measures.

Risk Management. The process of factoring the criticality of assets with the vulnerability to a threat, and determining the threshold of acceptable risk.

Screens. An array of wires or electrified screening that protects areas or openings, such as skylights and crawl spaces. It may use broken circuit or capacitance techniques to sense intrusion.

Security. Refers to the safeguarding of information classified Top Secret, Secret, or Confidential to prevent unlawful unauthorized dissemination, duplication or observation.

Security Liaison (SL). The individual responsible for coordinating compliance with the implementation of CBP security programs through the District Security Officer/Regional Security Officer and serve as the primary point of contact for all security issues in the their facilities.

Sensitive But Unclassified (SBU) Building Information. SBU includes but is not limited to paper and/or electronic documentation of the physical facility information. SBU is the formal designation for information that, by law or regulation, requires some form of protection but is outside the formal system of classification, in accordance with Executive Order 12958, Classified National Security Information as amended, and DHS MD 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information.

Sensitive Compartmented Information (SCI). SCI is classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled exclusively within formal control systems established by the Director of Central Intelligence.

Sensitive Compartmented Information Facility (SCIF). An accredited area, room, group of rooms, or installation where SCI may be stored, used, discussed, and/or electronically processed.

Small Arms Ammunition. Any shotgun, rifle or pistol cartridge and any cartridge for propellant-activated devices. This definition does not include military ammunition containing bursting charges or incendiary, tracer, spotting or pyrotechnic projectiles.

Special Access Program. Any program imposing access controls beyond those normally provided for access to Confidential, Secret, or Top Secret. Such programs include special clearances, investigative requirements, or special access lists of persons determined to require special access. Special access programs pertaining to intelligence activities, or intelligence sources or materials exercised by the Director of Central Intelligence.

Special Security Officer (SSO). An individual who is designated the responsibility for the secure operation of a SCIF and insuring the secure handling, storage, destruction and transmittal of foreign intelligence material.

Spring Latch. A beveled, spring loaded bolt of a rim, mortise, or cylindrical lockset that is retracted by a knob, lever, or key, and is depressed by a strike plate lip. The bolt is extended by the spring pressure.

Strongroom. A reinforced interior space enclosed by or separated from other similar spaces by four walls, a ceiling and a floor, constructed of solid building materials, and used for storage of classified materials.

Supervised Lines. Interconnecting lines in alarm systems that are electrically supervised against tampering. See also [Line Supervision](#).

Surreptitious Entry. The unauthorized entry into a facility or security container in a manner in which evidence of such entry is not discernable under normal circumstances.

Tamper Switch. A switch, usually mechanically operated, used to detect opening of alarm equipment.

Termination Briefing. The briefing provided to personnel upon termination of authorization for access to classified information and their acknowledgement of their continuing responsibilities by executing a Debriefing Acknowledgement.

Threat. Acts or conditions which may result in the compromise of information, loss of life, damage, loss or destruction of property or the disruption of the mission of an organization.

Threat Assessment. The analysis of an asset's vulnerability to its threats.

Top Guard. Anti-personnel device, usually of barbed or concertina wire, installed at the tops of fences and along roof edges.

Ultrasonic Detector. A device that senses motion in a protected area by a [Doppler](#) shift in the transmitted ultrasonic energy. The device operates by filling a space with a pattern of ultrasonic waves; the modulation of these waves by a moving object is detected and initiates an alarm signal.

Unauthorized Person. Any person who is not authorized to have access to specific classified information. Regardless of the degree of clearance, an individual is not authorized access to classified information of any degree without a demonstrated need-to-know.

Uninterruptible Power Supply (UPS). UPS systems provide backup power. They monitor the incoming power lines and provide continuous electrical current in the event of a change in voltage. The UPS provides a certain amount of battery backup.

Vault. A windowless enclosure of heavy, reinforced construction with walls, floor, roof and door(s) designed and constructed to delay penetration sufficiently to enable the timely arrival of response forces.

[RETURN TO TOP](#)

Vibration Detection. An alarm system that employs one or more contact microphones and vibration sensors, which are fastened to the surfaces of the area or object being protected to detect excessive levels of vibration. The contact microphone system consists of microphones, a control unit containing an amplifier and an accumulator, and a power supply. The unit's sensitivity is adjustable so that ambient noises or normal vibrations will not initiate an alarm signal.

Visitor. Any person who is not a DHS or CBP Federal employee or DHS or CBP contractor with current DHS or CBP suitability and issued a DHS or CBP [Photo Access Card \(PAC\)](#).

Volumetric Alarm. A system that detects movement through the interior of an alarmed area, as opposed to the detection of perimeter penetrations.

Vulnerability. The probability that a threat will result in the compromise of information, loss of life, damage, loss or destruction of property or the disruption of the mission of an organization.

Walk Test. A procedure of actually walking through the area protected by a motion detector to determine the limits of its coverage.

X-ray System. A device or system that inspects the contents of a package or container for concealed explosives or contraband. Some systems can only detect objects made of materials possessing high atomic numbers, such as steel, tin, aluminum, and iron. Other systems can detect materials with both high and low atomic numbers. Some systems have two monitors, one for objects with high atomic numbers and one for objects with low atomic numbers. Color systems presently available use only one monitor to view both types of materials. Specific colors are assigned to high and low atomic number materials. Such systems can detect and discriminate among plastics, metals, and explosives in firearms and bombs.

Zone. Large protected premises are divided into areas or zones, each having its own identification and/or annunciation.





ADDITIONAL CBP SECURITY LINKS

I. CBP INFORMATION SECURITY (INFOSEC)

[CBP Protection of Classified Information \(INFOSEC\)](#)

[Information Security/For Official Use Only \(INFOSEC/FOUO\)](#) - 12/03/2007

[CBP Courier Card](#)

[Awareness Training for Safeguarding Sensitive But Unclassified/For Official Use Only Information](#) - 11/29/2007

[Sensitive Security Information \(SSI\)](#)

[Controlled Unclassified Information \(CUI\)](#)

[Industrial Security](#) - 11/29/2007

[CBP Badge and Credential](#) - 12/14/2005

This information is available for requesting badges, credentials, and badge lucite preservation. Also contains the guidelines for reporting lost or stolen badges and credentials.

[RRB Crime Incidents](#) - 12/18/2007

II. CBP COMMUNICATIONS SECURITY (COMSEC)

CBP's Communication Security (COMSEC) program falls under the responsibility of the Security and Technology Policy Branch within the Office of Information and Technology. CBP's COMSEC Central Office of Record (COR) has day-to-day management responsibility for CBP's COMSEC program.

III. CBP COMSEC COR POINTS OF CONTACT

Keith Booker
CBP COMSEC COR Program Manager
Supervisory COMSEC
Desk: 540-542-2430
Blackberry: 571-271-9653
Fax: 540-542-2994
Keith.Booker@dhs.gov

Chuck Lamb
COMSEC Specialist
Desk: 540-665-5312
Blackberry: 202-528-9388
Fax: 540-542-2994
Charles.Lamb@dhs.gov

The Office of Information Technology (OIT) Network and Security Operations (NSO) and the Security and Technology Policy (STP) Branch spearheaded a newly formed COMSEC Working Group to unify all Communications Security (COMSEC) under an OIT sponsored centralized program. The COMSEC Working Group includes representation from all CBP COMSEC stakeholders to include Office of Intelligence and Operations Coordination (OIOC), Office of Internal Affairs (OIA), Office of Field Operations (OFO), Office of Border Patrol (OBP) and Office of Air & Marine (OAM). COMSEC services include identification of equipment to be procured, start-up of new secure communications equipment, inventory services, and coordination of service and maintenance. It is critical that CBP maintains its current system for transmitting time-sensitive classified communications from CBP Headquarters to the field offices. This working group was established to charter the CBP COMSEC program governance, structure and operational capabilities.

Communications Security (COMSEC) is the measures and controls taken to deny unauthorized individuals information derived from secure communications and to ensure the authenticity of such secure communications. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC.

[National Policy for the Destruction of COMSEC Paper Material](#)

[DHS Chief Information Security Officer \(CISO\) Page](#)

IV. THE OFFICE OF INFORMATION TECHNOLOGY (OIT)

Shall be responsible for managing CBP's Communications Security (COMSEC) program, accreditation of classified systems, providing Information Technology security training and responsible for CBP systems access requirements as defined in the [CBP Information Systems Security Policies and Procedures Handbook 1400-05C](#).

Though the COMSEC Account will not be authorized for open storage, the [DHS Management Directive \(MD\) No. 11046 Open Storage Area Standards for Collateral Classified Information \(issued 2/22/2005\)](#) be used in the certification process. This is in addition to verifying that the minimum physical security standards set forth in NSTISSI No. 4005 has been met for the room where the COMSEC Account will be established.

Physical security certification of the room where a COMSEC Account is located can only be approved by the Office of Internal Affairs. If Sensitive Compartmented Information (SCI) will be

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

in the COMSEC Account, then the request must be coordinated through the Office of Internal Affairs, to the DHS Office of Security for physical security certification of the room. The Office of Internal Affairs will coordinate the request for the physical security certification for a SCI level COMSEC Account room with the DHS Office of Security.

Request for physical security certification of COMSEC Account room is to be submitted to cbp.security@dhs.gov.

For securing a crypto card and or a secure telephone device in a government office, the COMSEC User must comply with the [DHS Secure Telephone User Guide, Attachment Q3 to the DHS MD 4300B](#).

Physical security certification of a private residence for securing a crypto card and or a secure telephone device can only be approved by the Office of Internal Affairs. If Top Secret is involved, then the request must be coordinated through the Office of Internal Affairs, to the DHS Office of Security for physical security certification of the residence.

Request for physical security certification of a private residence for securing a crypto card and or a secure telephone device is to be submitted to cbp.security@dhs.gov. Upon receipt of the request, the Office of Internal Affairs will provide the required documents.

V. CBP NATIONAL SECURITY SYSTEMS SECURITY

[CBP Office of Information and Technology](#)

VI. CBP OPERATIONS SECURITY (OPSEC)

[CBP OPSEC](#)

VII. CBP PERSONNEL SECURITY (PSD)

[CBP Security Clearances - Background Investigations](#)
[CBP Personnel Security Handbook 1400-07 2006](#)

Questions pertaining to Security can be directed to the IA Security Management mailbox cbp.security@dhs.gov or by calling 202-325-0110.





FOR OFFICIAL USE ONLY

BACK



**INFORMATION SECURITY: SAFEGUARDING CLASSIFIED
AND SENSITIVE BUT UNCLASSIFIED INFORMATION HANDBOOK**

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

TABLE OF CONTENTS

FOREWORD 745

1. CHAPTER 1: INTRODUCTION.....747

 1.1. POLICY..... 747

 1.2. AUTHORITIES..... 747

2. CHAPTER 2: RESPONSIBILITIES749

 2.1. THE COMMISSIONER, U.S. CUSTOMS AND BORDER PROTECTION (CBP) 749

 2.2. THE ASSISTANT COMMISSIONER, OFFICE OF INTERNAL AFFAIRS AS THE DESIGNATED CSO 749

 2.3. THE DIRECTOR, SECURITY MANAGEMENT DIVISION..... 749

 2.4. ASSISTANT COMMISSIONERS, DIRECTORS, AND OTHERS WITH EQUIVALENT AUTHORITY 749

 2.5. DESIGNATED SECURITY OFFICERS 749

 2.6. THE OFFICE OF INTERNAL AFFAIRS, PERSONNEL SECURITY DIVISION..... 749

 2.7. THE OFFICE OF INTELLIGENCE AND OPERATIONS COORDINATION..... 750

 2.8. THE OFFICE OF INFORMATION TECHNOLOGY (OIT)..... 750

 2.9. CBP SUPERVISORS AND MANAGERS..... 750

 2.10. CLASSIFIED DOCUMENT CUSTODIAN 750

 2.11. ALL PERSONNEL 750

3. CHAPTER 3: CBP SAFEGUARDING CLASSIFIED POLICY AND PROGRAM MANAGEMENT751

[RETURN TO TOP](#)

BACK

3.1. POLICY 751

3.2. INTERPRETATION 751

4. CHAPTER 4: SECURITY CLASSIFICATION 757

4.1. POLICY 757

4.2. CBP SECURITY CLASSIFICATION MANAGEMENT 757

4.3. ORIGINAL CLASSIFICATION AUTHORITY (OCA) 757

**4.4. CUSTOMS AND BORDER PROTECTION
OCA POSITIONS 757**

4.5. ORIGINAL CLASSIFICATION PROCESS 758

4.6. CLASSIFICATION LEVELS 759

4.7. CLASSIFICATION CATEGORIES 759

4.8. DURATIONS OF CLASSIFICATION UNDER EO 12958 760

**4.9. COMMUNICATING ORIGINAL
CLASSIFICATION DECISIONS 760**

4.10. CBP CLASSIFICATION GUIDES 760

4.11. CLASSIFICATION PROHIBITIONS 761

4.12. CLASSIFICATION BY COMPILATION 761

4.13. EXCEPTIONAL CIRCUMSTANCES 762

**4.14. RECLASSIFYING PREVIOUSLY
DECLASSIFIED INFORMATION 762**

4.15. RECORDS FOR ORIGINAL CLASSIFICATION ACTIONS 762

4.16. CLASSIFICATION CHALLENGES. 763

4.17. INFORMAL CLASSIFICATION CHALLENGES. 763

4.18. FORMAL CLASSIFICATION CHALLENGES 763

[RETURN TO TOP](#)

BACK

4.19. DERIVATIVE CLASSIFICATION..... 764

4.20. DERIVATIVE CLASSIFICATION AUTHORITY..... 764

4.21. DERIVATIVE CLASSIFICATION APPLICATIONS 764

4.22. RECORDS OF DERIVATIVE CLASSIFICATION ACTIONS..... 764

4.23. DERIVATIVE CLASSIFICATION
SPECIALIZED TRAINING 765

5. CHAPTER 5: DECLASSIFICATION 767

5.1. POLICY 767

5.2. DECLASSIFICATION AUTHORITY 767

5.3. EXTENSION OF CLASSIFICATION 768

5.4. EXEMPTION FROM DECLASSIFICATION (INFORMATION NOT
CONTAINED IN A FILE SERIES) 768

5.5. EXEMPTION FROM DECLASSIFICATION (INFORMATION
CONTAINED IN A SPECIFIC FILE SE-RIES)..... 769

5.6. ONSET OF AUTOMATIC DECLASSIFICATION 770

5.7. MANDATORY DECLASSIFICATION REVIEW 771

6. CHAPTER 6: MARKING CLASSIFIED INFORMATION 775

6.1. POLICY 775

**7. CHAPTER 7: ACCESS AND DISSEMINATION OF CLASSIFIED
INFORMATION 779**

7.1. POLICY 779

7.2. ACCESS AND DISSEMINATION RESTRICTIONS 780

7.3. CBP EMPLOYEE VISIT CERTIFICATION OF SECURITY
CLEARANCE 780

7.4. DISSEMINATION OF CBP CLASSIFIED INFORMATION. 781

[RETURN TO TOP](#)

FOR OFFICIAL USE ONLY

BACK

7.5. DISSEMINATION OF OTHER AGENCY INFORMATION 781

7.6. DISSEMINATION OF CLASSIFIED INFORMATION..... 781

8. CHAPTER 8: CUSTODY AND ACCOUNTABILITY 785

8.1. POLICY 785

8.2. CUSTODY DURING EMERGENCIES..... 785

8.3. ACCOUNTABILITY OF CLASSIFIED INFORMATION..... 786

8.4. ACCOUNTABILITY OF TOP SECRET INFORMATION 786

8.5. ACCOUNTABILITY OF SECRET AND CONFIDENTIAL INFORMATION 787

8.6. RECEIPTS FOR CLASSIFIED TRANSMISSION 787

8.7. CLASSIFIED MEETINGS AND CONFERENCES 788

8.8. REPRODUCTION OF CLASSIFIED MATERIAL 789

8.9. ANNUAL INVENTORY OF CLASSIFIED HOLDINGS 791

8.10. DESTRUCTION OF CLASSIFIED MATERIALS 791

8.11. END-OF-DAY SECURITY CHECKS 792

9. CHAPTER 9: STORAGE OF CLASSIFIED INFORMATION 793

9.1. POLICY 793

9.2. STANDARDS FOR STORAGE EQUIPMENT 793

9.3. NEW PURCHASES 793

9.4. MAINTENANCE 793

9.5. TOP SECRET INFORMATION STORAGE 794

9.6. SECRET INFORMATION STORAGE 794

9.7. CONFIDENTIAL INFORMATION STORAGE 795

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

FOR OFFICIAL USE ONLY

BACK

9.8. OPEN STORAGE..... 795

9.9. IDENTIFICATION OF SECURITY CONTAINERS..... 795

**9.10. PROTECTING CLASSIFIED COMBINATIONS
USING STANDARD FORM (SF) 700 796**

9.11. ACCESS TO CLASSIFIED COMBINATIONS..... 796

9.12. CHANGING COMBINATIONS 797

9.13. SECURITY CONTAINER CHECK SHEET..... 797

9.14. OPEN-CLOSED SIGNS 797

9.15. SECURITY CONTAINERS TAKEN OUT OF SERVICE. 797

10. CHAPTER 10: TRANSMISSION AND TRANSPORTATION 799

10.1. POLICY 799

10.2. METHODS OF TRANSMISSION OR TRANSPORTATION. 799

10.3. SHIPMENT OF FREIGHT 801

10.4. PREPARATION OF MATERIAL FOR TRANSMISSION. 801

10.5. ESCORT OR HAND-CARRYING OF CLASSIFIED MATERIAL. 802

10.6. COURIER TRAVEL BY COMMERCIAL AIR..... 802

**10.7. TRANSPORT OF CLASSIFIED MATERIAL
WITHIN AN ACTIVITY OR OFFICE..... 803**

10.8. RECEIPTS..... 803

11. CHAPTER 11: SECURITY VIOLATIONS AND INFRACTIONS 805

11.1. POLICY 805

11.2. DEFINITIONS 805

11.3. REPORTING SECURITY INCIDENTS..... 805

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

11.4. CLASSIFIED SPILLAGE 806

11.5. INCIDENTS INVOLVING SENSITIVE COMPARTMENT
INFORMATION (SCI) 807

11.6. PRELIMINARY INQUIRY 807

11.7. FORMAL INVESTIGATION 809

11.8. OVERSEAS SECURITY VIOLATIONS
AND INFRACTIONS 810

11.9. OTHER AGENCY SECURITY VIOLATIONS
AND INFRACTIONS 810

11.10. SANCTIONS 810

11.11. ANNUAL REPORTING REQUIREMENTS 811

12. CHAPTER 12: INDUSTRIAL SECURITY PROGRAM 813

12.1. CBP’S INDUSTRIAL SECURITY PROGRAM..... 813

12.2. PROCESSING REQUIREMENTS 818

13. CHAPTER 13: SAFEGUARDING SENSITIVE BUT UNCLASSIFIED
(FOR OFFICIAL USE ONLY) INFORMATION 821

13.1. POLICY 821

14. CHAPTER 14: SENSITIVE SECURITY
INFORMATION (SSI) 823

14.1. POLICY 823

14.2. RESPONSIBILITIES 823

14.3. CATEGORIES OF SSI 826

14.4. ORIGINAL DESIGNATION OF INFORMATION AS SSI 826

14.5. MARKING SSI 827

BACK

14.6. DURATION OF SSI AND SSI REVIEWS 828

14.7. CHALLENGING SSI 829

14.8. AUDITS AND INSPECTIONS 830

14.9. SHARING, DISSEMINATION AND ACCESS 830

14.10. STORAGE AND HANDLING 832

14.11. CBP SSI FOIA REVIEW PROCESS..... 832

14.12. TRANSMISSION 833

14.13. DESTRUCTION 834

14.14. INCIDENT REPORTING 834

14.15. PROGRAM STATUS REPORTING 835

15. CHAPTER 15: SECURITY EDUCATION AND AWARENESS 837

15.1. POLICY 837

15.2. RESPONSIBILITIES 837

15.3. SECURITY TRAINING 837

16. CHAPTER 16: COMPLIANCE REVIEWS AND SELF-INSPECTIONS 839

16.1. POLICY 839

16.2. RESPONSIBILITIES 839

16.3. COMPLIANCE REVIEW PROCEDURES 839

16.4. SELF-INSPECTIONS 840

16.5. UNANNOUNCED REVIEWS 840

16.6. EXTERNAL REVIEWS AND INSPECTIONS 840

[RETURN TO TOP](#)

17. APPENDIX A - SECURITY FORMS841



FOREWORD

U.S. Customs and Border Protection Safeguarding Classified and Sensitive But Unclassified Handbook.

U.S. Customs and Border Protection (CBP) are charged with securing America's borders to protect American people and our economy. CBP ensures border security against terrorist, other criminals and weapons of mass destruction, while facilitating legitimate trade and travel.

CBP achieves critical missions while working with critical information such as Classified National Security Information, For Official Use Only/Law Enforcement Sensitive Information and Sensitive Security Information.

This handbook supersedes Customs Issuance System (CIS) HB 1400-03, dated February 1991 and Immigration Naturalization Services, Security Officer Handbook.

Safeguarding classified and sensitive but unclassified information is vital to our mission and operations. I fully support the Office of Internal Affairs in their program oversight activities of CBP's Information Security Program.

Deputy Commissioner
U.S. Customs and Border Protection

1. CHAPTER 1: INTRODUCTION

1.1. POLICY

- 1.1.1. This security handbook implements the Executive Order 12958, as amended, Classified National Security Information and Department of Homeland Security Management Directives, 11000 series. It is applicable to all persons who are permanently or temporarily assigned, detailed to, employed or under contract with Customs and Border Protection (CBP). It establishes safeguarding, classifying, declassifying, and downgrading of official information requiring protection in the interest of national security.
- 1.1.2. This handbook also establishes safeguards for sensitive but unclassified information within CBP. DHS departmental policy states, that all sensitive but unclassified information generated within DHS and its components, that is not regulated by statute, shall be referred to as "For Official Use Only," (FOUO). [DHS MD 11042.1](#), provides specific guidance for the safeguarding of such information.
- 1.1.3. The provisions of this handbook set forth the minimum security standards and safeguards to ensure the protection of classified and sensitive but unclassified information within CBP.

1.2. AUTHORITIES

- 1.2.1. Executive Order 12333, as amended 46 F.R. 59941 (Dec 8, 1981); 68 F.R. 4075 (Jan. 23, 2003); 73 F.R. 45325 (July 30, 2008), United States Intelligence Activities
- 1.2.2. Executive Order 12829, as amended 58 F.R. 3470 (Jan 6, 1993); 58 F.R. 65863 (Dec 14, 1993), National Industrial Security Information.
- 1.2.3. Executive Order 12958, as amended, 68 F.R. 15315 (Mar 28, 2003), Classified National Security Information
- 1.2.4. Executive Order 13284, Amendment of Executive Orders, and Other Actions, in Connection with the Establishment of the Department of Homeland Security
- 1.2.5. 6 CFR §7, Department of Homeland Security, Classified National Security Information
- 1.2.6. 32 CFR §2001, Part Implementing Directive for E.O. 12958, as amended
- 1.2.7. 44 USC Chapters 21, 31, 33, Federal Records Act
- 1.2.8. 49 USC §114(s), Nondisclosure of Security Activities
- 1.2.9. 49 CFR §1.520, Protection of Sensitive Security Information, May 18, 2004
- 1.2.10. Homeland Security Act, Pub L. 107-296, 116 Stat 2135 (codified as amended in scattered sections of 6 USC §101 et seq).

[RETURN TO TOP](#)

1.2.11. 96-456, “Classified Information Procedures Act”

1.2.12. PL 107-71, 115, Stat. 597 (2001) “Aviation and Transportation Security Act”



2. CHAPTER 2: RESPONSIBILITIES

2.1. THE COMMISSIONER, U.S. CUSTOMS AND BORDER PROTECTION (CBP)

2.1.1. Shall designate the Assistant Commissioner, Office of Internal Affairs, as the Component Chief Security Officer (CSO).

2.2. THE ASSISTANT COMMISSIONER, OFFICE OF INTERNAL AFFAIRS AS THE DESIGNATED CSO

2.2.1. Shall serve as the principal advisor to the CBP Deputy Commissioner regarding CBP's Information Security Program;

2.2.2. Shall ensure sufficient resources are in place to implement and manage CBP's Information Security Program and the requirements of this handbook; and

2.2.3. Shall designate the Director, Security Management Division to implement and manage the CBP Information Security Program.

2.3. THE DIRECTOR, SECURITY MANAGEMENT DIVISION

2.3.1. Shall direct and administer CBP's Information Security Program under which information is classified, safeguarded, and declassified;

2.3.2. Shall issue any necessary written procedures required for the effective implementation of this handbook.

2.4. ASSISTANT COMMISSIONERS, DIRECTORS, AND OTHERS WITH EQUIVALENT AUTHORITY

2.4.1. CBP may choose to exceed the standards as cited within this handbook, but may not lessen them, per DHS MD 11044. If the choice is to exceed the minimum requirements, sufficient justification must exist to warrant any increased expenditures

2.4.2. Shall appoint in writing a Designated Security Officer (DSO) for their respective areas of responsibility to ensure procedures set forth in this handbook are followed.

2.5. DESIGNATED SECURITY OFFICERS

2.5.1. Shall provide assistance and support to regional CBP personnel and serve as a liaison to the Office of Internal Affairs for applicable matters relating to the implementation and compliance with the provisions of this handbook.

2.6. THE OFFICE OF INTERNAL AFFAIRS, PERSONNEL SECURITY DIVISION

2.6.1. Shall develop policy and procedures which implement and administer the

personnel security and suitability program for CBP; render employment suitability; and grant security clearances for access to Classified National Security Information, as defined in the CBP Personnel Security Handbook, HB 1400-07

2.7. THE OFFICE OF INTELLIGENCE AND OPERATIONS COORDINATION

2.7.1. Shall be responsible for managing CBP's Sensitive Compartmented Information (SCI) program and granting SCI access to CBP personnel.

2.8. THE OFFICE OF INFORMATION TECHNOLOGY (OIT)

2.8.1. Shall be responsible for managing CBP's Communications Security (COMSEC) program, accreditation of classified systems, provide Information Technology security training and responsible for CBP systems access requirements, as defined in the CBP Information Systems Security Policies and Procedures Handbook 1400-05C.

2.9. CBP SUPERVISORS AND MANAGERS

2.9.1. Shall ensure that they and those they supervise are aware of and comply with the applicable provisions of this handbook and promote and ensure compliance by staff members.

2.9.2. Shall appoint, in writing, a primary and alternate Classified Document Custodian (CDC) for those situations where classified information is stored and processed.

2.9.3. Shall ensure security education and awareness training is provided upon initial assignment of an employee, detailee, and contractor and reinforced periodically thereafter through routine office interaction, e-mail reminders, staff meetings and other office gatherings, which will contribute to an informed workforce.

2.10. CLASSIFIED DOCUMENT CUSTODIAN

2.10.1. Shall ensure the procedures set forth in Chapter 3 are followed.

2.11. ALL PERSONNEL

2.11.1. Shall be responsible for protecting classified and sensitive but unclassified information from unauthorized disclosure.

2.11.2. Shall be aware of, and comply with, the applicable provisions of this handbook and report to the appropriate officials any infractions or violations that affect the safeguarding of classified and sensitive but unclassified information.

3. CHAPTER 3: CBP SAFEGUARDING CLASSIFIED POLICY AND PROGRAM MANAGEMENT

3.1. POLICY

- 3.1.1. All CBP personnel are personally and individually responsible for providing proper protection of classified information under their custody and control. All officials within CBP who hold management or supervisory positions have a non-delegable responsibility for the quality, implementation, and management of the Information Security Program within their area of responsibility.
- 3.1.2. CBP personnel who create or handle classified information will be rated accordingly. Management of classified information shall be included as a critical element for CBP personnel serving as a Designated Security Officer (DSO) or Classified Document Custodian (CDC) whose duties primarily or collaterally involve the safeguarding of classified information.

3.2. INTERPRETATION

- 3.2.1. Questions concerning policies pertaining to classified national security information should be referred to the Office of Internal Affairs (IA), Security Management Division (SMD). The Director, SMD shall provide CBP interpretation of policies and procedures concerning the protection of classified national security information, and provide written guidance to CBP offices, as necessary.

1.3. PROGRAM POLICIES

- 3.3.1. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life. Our national interest requires that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Accordingly, classifying authorities, program managers, supervisors, and employees shall follow all applicable laws, including the provisions of EO 12958, as amended, subsequent orders and the provisions of this handbook to protect national security information.
- 3.3.2. DHS has delegated Original Classification Authority (OCA) up to the Top Secret level to the Commissioner, CBP and the Assistant Commissioner, Office of Intelligence and Operations Coordination (OIOC). No other CBP official is authorized to classify information at the Top Secret level.
- 3.3.3. CBP OCAs cannot re-delegate this authority, but it may be exercised by persons designated in writing to act in the absence of the OCA, provided they have the appropriate level of security clearance and training.
- 3.3.4. Derivative classification includes the classification of information based on

classification guidance or classified source material. With the appropriate security clearance, and as required by job, CBP personnel involved in the generation, extraction or summarization of information based on previously classified information are authorized to derivatively classified information.

- 3.3.5. E.O. 12958, as amended, states that authorized holders of information who, in good faith, believe that its classification status is improper, are encouraged and expected to challenge the classification status of the information in accordance with the procedures identified in this handbook. Authorized holders wishing to challenge the classification status of information shall follow those procedures outlined in 4.16-4.18 of this handbook.
- 3.3.6. Information that continues to meet the classification requirements of E.O. 12958, as amended, or any other applicable law or subsequent orders, requires continued protection. However, CBP generated classified information shall be declassified as soon as it no longer meets the standards for classification under any applicable law.
- 3.3.7. When classified information is transferred from another agency or DHS component in conjunction with a transfer of functions, and not merely for storage purpose, the receiving CBP office shall be deemed to be the originating office for purposes of downgrading and declassification.
- 3.3.8. Classified information generated by CBP must be reviewed for declassification upon receipt of a request by a United States citizen or permanent resident alien, a Federal agency, or a state or local government. A request for mandatory review of classified information shall be submitted in writing and describe the information with sufficient specificity to locate it with a reasonable amount of effort.
- 3.3.9. Assistant Commissioners, Directors, and alike shall appoint in writing, an individual with a Top Secret security clearance to serve as the Top Secret Control Officer (TSCO) within his or her office if the office processes information classified at the Top Secret level. The TSCO is responsible for protection, accountability, receiving, dispatching and overall control of all Top Secret information within his or her office.
- 3.3.10. Assistant Commissioners, Directors, Office Directors, Managers, and Supervisors must designate in writing an appropriately cleared employee to serve as the Classified Document Custodian (CDC) whenever classified information is handled and stored within his or her office.
- 3.3.11. Assistant Commissioners, Directors, Office Directors, Managers, and Supervisors must establish procedures for the control and accountability of classified (Top Secret, Secret and Confidential) information received. Procedures shall ensure movement of classified information can be traced, its dissemination limited, its retrieval is obtained promptly, its loss can be detected, and excessive holdings and reproduction are limited. Offices

- maintaining classified information must conduct an annual inventory, reviewing their classified holdings. The CDC must visually inspect each classified document upon initial receipt during the annual inventory to ensure that the document is completely intact, and accounted for by written evidence of proper disposition. Results of this inventory shall be kept locally on file.
- 3.3.12. No employee has a right to access classified information by virtue of title, position, or level of security clearance. An employee is only eligible for access to classified information provided that the employee has been determined to be trustworthy by the appropriate background investigation, adjudicated favorably, and access is essential to accomplish lawful and authorized Government purpose.
- 3.3.13. Classified information (in any form), to include extra copies, is not personal property and may not be removed from the Government's control by any departing employee. The CDC shall account for and transfer all classified information from the possession of the departing employee.
- 3.3.14. All Directors, Supervisors and Managers must ensure that only authorized persons obtain access to classified information; however, the final responsibility for determining whether an individual gains access to classified information rests with the individual who has possession, knowledge or control of the information and not with the prospective recipient. Classified information must be protected at all times by the holder of the information. Before classified information is disclosed, the holder must verify the recipient's identification and security clearance through their operating unit's servicing officer or security contact, determine the recipient's need to know, and advise the recipient of the classification level of the information.
- 3.3.15. Classified information may be transmitted by approved means both inside and outside of CBP's facilities; however, classified information may only be hand-carried aboard commercial aircraft when there is neither time nor other means available to properly transmit the information. Requests for permission to hand-carry classified information aboard a commercial aircraft shall be submitted, in writing, to the Office of Internal Affairs, Security Management Division as identified in Chapter 10 of this handbook.
- 3.3.16. CBP personnel may receive authorization from the Office of Internal Affairs to hand-carry classified information up to the Top Secret level within the United States and its territories, except by commercial aircraft. Authorization shall be requested for CBP personnel who are required and routinely carry classified material to facilities in the same geographical areas. To be an authorized courier, the employee must have valid justification to transport, hold an appropriate security clearance and possess a valid DHS Courier Authorization Card, as described in Chapter 10.8 of this handbook.
- 3.3.17. Classified information must be stored under conditions that will provide adequate protection against access by unauthorized persons. Whenever

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

classified information is not under the personal control and observation of a cleared person, it must be guarded by personnel with the appropriate security clearance or stored in a GSA-approved security container.

- 3.3.18. Certain security measures and controls must be in place for the storage of Top Secret material. The same applies to open storage. Storage for these purposes must be approved and accredited by the Office of Internal Affairs.
- 3.3.19. Classified documents must be destroyed in a manner sufficient to preclude recognition or reconstruction of the classified information. Assistant Commissioners, Office Directors and Division Directors shall ensure the proper destruction of classified information for classified information is stored and handled in their offices. Such procedures must be by approved destruction methods, adequate destruction records are maintained, and the destruction is properly witnessed as described in section 8.10 of this handbook.
- 3.3.20. Classified information shall not be discussed, or otherwise transmitted or processed, on any telecommunications equipment not approved and accredited by the Office of Information Technology (OIT) and Office of Internal Affairs (IA) accordingly. For further details, see the Information Systems Security Policies and Procedures Handbook HB 1400-05C.
- 3.3.21. All information security incidents, violations, or compromises must be reported. Any person who is aware of or suspects the unauthorized disclosure, mishandling, loss or compromise (in any form) of classified information must notify the Office of Internal Affairs, Joint Intake Center
- 3.3.22. CBP Office heads will be notified through official memorandum of security violations or infractions involving personnel within their office. Security violations or infractions committed shall be noted in the employee's evaluation. All reports and any information contained during an inquiry or investigation will be retained in the employees personnel security file. CBP personnel involved in security violations may be subject to U.S. Customs and Border Protection, Table of Offenses and Penalties. Personnel involved in security incidents may be subject to a re-examination of a granted security clearance.
- 3.3.23. The Designated Security Officer (DSO) will assist in the implementation and program management of the policies and procedures set forth in DHS MD 11041, Protection of Classified National Security Information Program Management.
- 3.3.24. Classified Contracts. CBP Offices entering into contractual agreements involving classified information shall adhere to the CBP National Industrial Security Program policy and procedures set forth in Chapter 12, CBP Industrial Security Program.
- 3.3.25. Reporting Requirements. CBP offices are required to participate in the

following recurring reports to ensure the efficiency and effectiveness of the CBP Information Security Program:

- Standard Form (SF) 311, Agency Security Classification Management Program Data Report, which reflects the status of an agency's classification management program. Each CBP office will submit a single report reflecting the classification and declassification actions taken during the preceding fiscal year. The Office of Internal Affairs will compile the information into one single report for submission to the DHS Chief Security Officer. The DHS Chief Security Officer will compile input from each DHS component for submission to the Information Security Oversight Office (ISSO). CBP Offices will submit report upon request by the Office of Internal Affairs.
- Lock Replacement Report. 32 CFR §§2001/2004, Section 2001.43, Classified National Security Information (Directive No. 1); Final Rule, requires the use of GSA approved equipment for the storage of classified information. Further, locks used on equipment for the storage of classified information must meet Federal Specification FF-L-2740-A. The referenced directive allows agencies until October 1, 2012, to meet the referenced standards.

3.3.26. CBP offices must develop a plan to replace equipment used for the storage of classified information that does not meet the standards referenced above and submit to the Office of Internal Affairs for review. CBP offices will submit a status of their replacement plan to the Office of Internal Affairs by April 4 each calendar year. The Office of Internal Affairs will compile into one single report for submission to the DHS Chief Security Officer:

- Cost Accounting Report. This report reflects the estimated cost expended for the protection of classified information for the current fiscal year. CBP offices will report any cost associated to the Office of Internal Affairs. Reports will be submitted upon request and with specific instructions. The Office of Internal Affairs will compile into one single report for submission to the DHS Chief Security Officer. The DHS Chief Security Officer will submit one agency report to the Information Security Oversight Office.
- Security Violations and Infractions. The Office of Internal Affairs must submit the total number of confirmed violations and infractions committed, by category, occurring within CBP in the preceding calendar year, by January 15 of each calendar year. The exceptions are incidents involving Communication Security (COMSEC) and Special Compartmented Information (SCI) which are reported through separate channels. The purpose of the report is to provide DHS-wide trend analysis for determining enhanced and focused educational and awareness needs.

3.3.27. Oversight and Compliance. The Office of Internal Affairs has overall responsibility for the oversight and compliance with the standards set forth

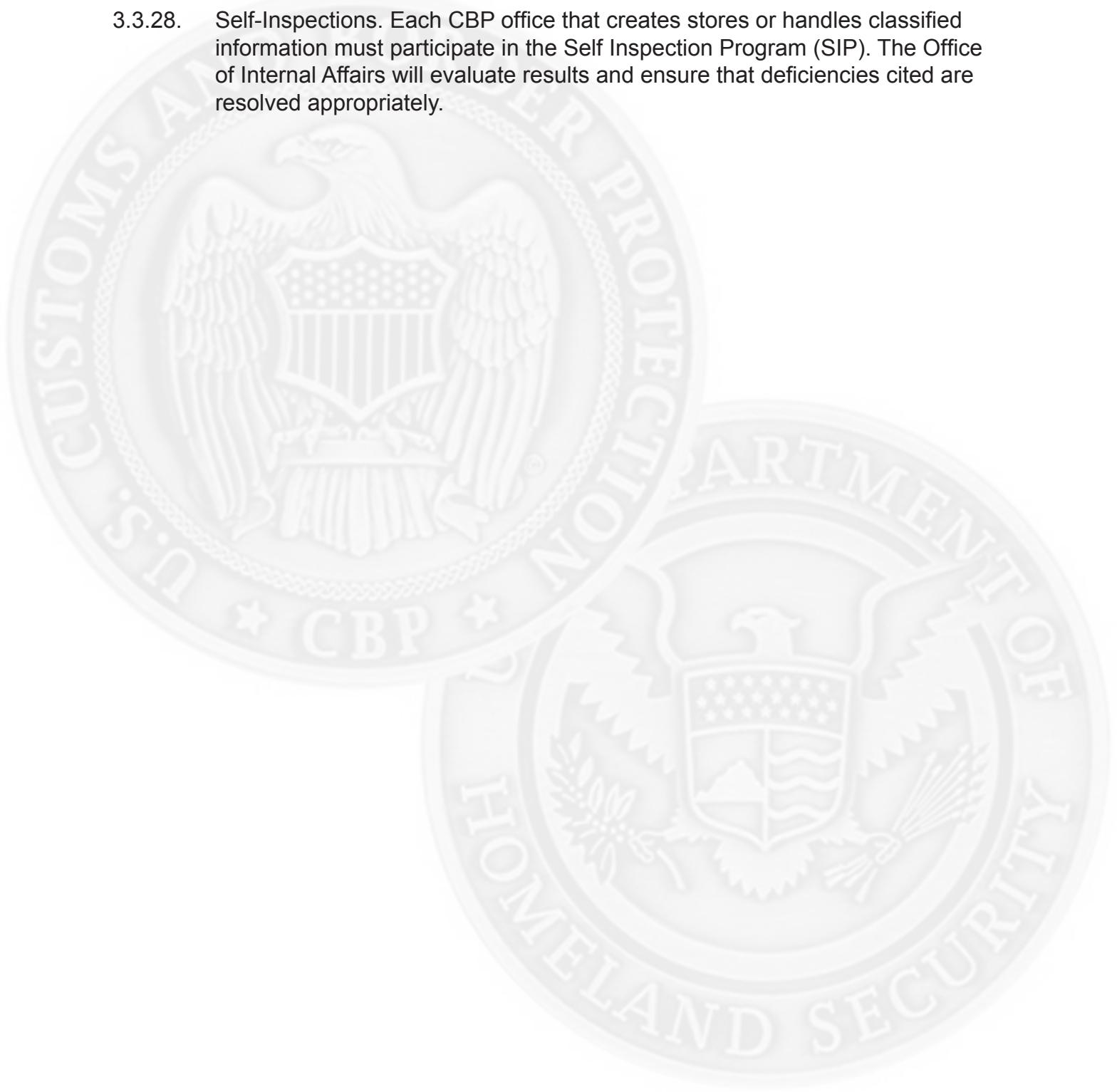
FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

in this handbook. As such, the Office of Internal Affairs will conduct periodic program reviews of CBP offices that store and handle classified information to assess compliance and provide guidance and assistance as necessary.

- 3.3.28. Self-Inspections. Each CBP office that creates stores or handles classified information must participate in the Self Inspection Program (SIP). The Office of Internal Affairs will evaluate results and ensure that deficiencies cited are resolved appropriately.



[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

4. CHAPTER 4: SECURITY CLASSIFICATION

4.1. POLICY

4.1.1. The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and potential loss of human life. Security classification shall be applied only to protect the national security and information may not be classified unless its disclosure reasonably could be expected to cause damage to the national security. Original classification decisions will be made in accordance with the guidance provided in E.O. 12958, as amended, any applicable DHS directives including MD 11044, and the provisions set forth in this chapter.

4.2. CBP SECURITY CLASSIFICATION MANAGEMENT

4.2.1. The integrity of Customs and Border Protection's classification system is dependent upon knowledge and judgment of CBP personnel involved in the oversight and implementation of programs that may involve the production of classified national security information.

4.2.2. The Office of Internal Affairs has program oversight of CBP's Classification Management process, polices and procedures set forth in this handbook, however further program coordination with the Office of Intelligence and Operations Coordination will occur accordingly.

4.2.3. CBP officials involved in the classification process shall comply with the standards cited in this handbook and ensure integrity of the system is maintained.

4.3. ORIGINAL CLASSIFICATION AUTHORITY (OCA)

4.3.1. An original classification authority (OCA) is written authorization to an official, either by the President, by agency heads, or other officials delegated by the President, to make an initial determination to classify information.

4.3.2. The Secretary of Homeland Security has been designated by the President as an OCA with authority to classify eligible information up to and including the Top Secret level. The Secretary can further delegate Top Secret original classification authority to additional DHS officials pursuant to EO 12958, as amended.

4.3.3. The DHS Chief Security Officer when designated by the Secretary as the "Senior Agency Official" may delegate Secret and Confidential original classification authority to additional DHS officials.

4.4. CUSTOMS AND BORDER PROTECTION OCA POSITIONS

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- 4.4.1. Customs and Border Protection officials who are delegated OCA by DHS will be officially announced in the form of a DHS management directive. CBP officials who have been delegated original classification authority cannot further delegate this authority. However, if an appropriately cleared individual is designated to act on behalf of a delegated OCA, that individual has the authority to classify eligible information.
- 4.4.2. Persons delegated OCA at a specified level are also authorized to classify information at a lower level.
- 4.4.3. CBP office heads may request OCA delegation where an operational need exists. Request for OCA delegations shall be submitted to DHS Office of Security through the Assistant Commissioner, Office of Internal Affairs using the DHS Form 1401-1 "Request for Original Classification Authority." OCA delegation requests shall be based on justification of a demonstrated and continuing need for such authority.
- 4.4.4. CBP Officials serving in OCA delegated positions:
- Shall be trained on OCA responsibilities, methods, and procedures, within sixty (60) days of occupying a delegated position. The Office of Internal Affairs is responsible for providing this training.
 - Are encouraged to consult with the Office of Internal Affairs for assistance when classifying information.
 - Shall communicate original decisions either through use of a classification guide and/or through markings placed directly on the materials.
 - Shall ensure record systems are designed and maintained to optimize the safeguarding of classified information, and to facilitate the declassification of records under the provisions of Chapter 5, Declassification, and as defined in EO 12958, as amended, when such information no longer meets the standards for continued classification.

4.5. ORIGINAL CLASSIFICATION PROCESS

- 4.5.1. Original classification is the initial determination that an item of information requires protection against unauthorized disclosure in the interest of nation security. Information may be originally classified under the terms of EO 12958, as amended if all of the following conditions are met.
- An Original Classification Authority (OCA) classifies the information;
 - The information is owned by, produced by or for, or is under the control of the U.S. Government; (for purposes of this handbook, "control" means the authority of CBP to regulate access to the information.)
 - The information falls within one or more of the categories of information listed in section 4.7 below as defined in EO 12958, as amended;
 - The OCA determines that the unauthorized disclosure of the information reasonably could be expected to cause in damage to the national security

which includes defense against transnational terrorism and the OCA is able to identify or describe the damage; and

- The OCA assigns a classification level as defined in Section 4.6.

4.6. CLASSIFICATION LEVELS

4.6.1. National security information that requires protection against unauthorized disclosure shall be classified by an original classification authority (OCA) at one of the following three levels.

- Top Secret shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
- Secret shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
- Confidential shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

4.6.2. At the time of the decision, there is no requirement for the classifying authority to prepare a written description of such damage; however, the classifying authority must be able to support the decision in writing, including identifying or describing the damage, should the classification decision become the subject of a challenge or access demand.

4.6.3. Except as otherwise provided by statute, no other terms shall be used to identify U.S. classified information e.g., “For Official Use Only,” “Sensitive But Unclassified.”

4.6.4. “For Official Use Only” or “Sensitive But Unclassified” information shall not be labeled with classified national security classification levels “Top Secret,” “Secret,” or “Confidential.”

4.7. CLASSIFICATION CATEGORIES

4.7.1. Information considered for classification must fall into one or more of the following categories (the numerical indicator preceding each category is the category identifier cited in Section 1.4 of EO 12958, as amended.):

- o 1.4(a) military plans, weapons systems, or operations;
- o 1.4(b) foreign government information;
- o 1.4(c) intelligence activities, (including special activities), intelligence sources or methods, or cryptology;
- o 1.4(d) foreign relations or foreign activities of the U.S., including

confidential sources;

- o 1.4(e) scientific, technological, or economic matters relating to national security, which includes defense against transnational terrorism;
- o 1.4(f) U.S. Government programs for safeguarding nuclear materials or facilities;
- o 1.4(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or
- o 1.4(h) weapons of mass destruction.

4.8. DURATIONS OF CLASSIFICATION UNDER EO 12958

4.8.1. At the time of original classification under EO 12958, as amended, the OCA will assign a date or event at which time the information will be downgraded and/or declassified. At the time of classification, original classifiers shall:

- Attempt to determine a specific date or event within ten years of the date of origination, upon which the information can be automatically declassified. If that is not possible, OCAs shall attempt to:
- Assign a date ten years (10) from the date of origination at which the information can be automatically declassified. Should the sensitivity of the information warrant classification beyond a 10-year period, they shall:

4.8.2. Assign a date no longer than 25 years from the date of origination at which the information will be automatically declassified, unless it is reclassified.

4.8.3. OCA cannot classify information beyond the 25 years unless such information has been specifically approved for exemption from declassification pursuant to EO 12958, as amended and Chapter 5, Declassification of this handbook. The only exception to this rule is when disclosure of the information could be expected to reveal the identity of a confidential human source or human intelligence source. In this instance, the “Declassify On” line may be marked 25X-Human. This marking is not authorized for use when the information pertains to non-human intelligence sources or intelligence methods.

4.9. COMMUNICATING ORIGINAL CLASSIFICATION DECISIONS

4.9.1. Classification decisions will be communicated either through publication of a security classification guide (see 4.10) or markings placed directly on the materials by the authorized OCA.

4.10. CBP CLASSIFICATION GUIDES

4.10.1. Classification guides are a documentary form of classification issued by an Original Classification Authority. The guide identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each element.

- 4.10.2. CBP offices and/or programs that develop classification guides will coordinate the development of such guides with the CBP, Office of Internal Affairs, Office of Intelligence and Operations Coordination, and DHS Office of Security.
- CBP classification guides will be prepared consistent with the standard DHS format. See EO 12958, Classified National Security Information, as amended, and DHS MD 11041 Protection of Classified National Security Information Program Management.
 - CBP classification guides must be coordinated through the DHS Office of Security prior to the appropriate CBP delegated OCA signing the CBP classification guides.
 - Final copies of CBP classification guides shall be submitted to the DHS Office of Security for file in the central DHS-wide classification guide repository.
- 4.10.3. Original classification authority is not required for individuals using classification guides. CBP personnel who generate information that requires classification based on the guide are authorized to “classify” the information by citing the applicable item in the guide and applying the classification level. This action is derivative classification from a classification guide.

4.11. CLASSIFICATION PROHIBITIONS

- 4.11.1. Information shall not be classified to:
- Conceal violations of law, inefficiency, or administrative error;
 - Prevent embarrassment to a person, organization, or agency;
 - Restrain competition; or
 - Prevent or delay the release of information that does not require protection
- 4.11.2. Classify basic scientific research information not clearly related to the national security.

4.12. CLASSIFICATION BY COMPILATION

- 4.12.1. Compilations of items of information that are individually unclassified may be classified in certain circumstances if the compilation reveals an additional association or relationship that meets the standards and criteria for classification under EO 12958, as amended; the additional association or relationship is not otherwise evident or revealed in the individual items of information; and the information is classified by an OCA. In this instance, the additional association or relationship is what is considered for classification, not the individual items of unclassified information. Careful consideration must be taken when determining the need for classification by compilation. When the determination is made that classification by compilation is necessary, the OCA must provide explicit instructions as to what elements of the compilation when combined, constitute classification and the additional association or

relationship that warrants the classification. CBP delegated OCAs, Office of Intelligence and Operations Coordination and/or the Office of Internal Affairs may provide assistance in making the determination of whether or not information should be classified by compilation.

4.13. EXCEPTIONAL CIRCUMSTANCES

4.13.1. When a CBP employee and/or contractor, develops information believed to require classification, the individual shall safeguard and mark the information in the manner prescribed according to its intended classification. Additionally, the notation, "TENTATIVELY CLASSIFIED PENDING AN ORIGINAL CLASSIFICATION DECISION" shall be prominently and conspicuously marked on the bottom of each page.

- A request for a classification decision will be submitted by a means approved for the level of classification, to the appropriate delegated CBP OCA. The OCA shall notify the sender of a classification determination within 30 days of receiving the request.
- When guidance is needed to determine the appropriate OCA with subject matter interest, contact the Office of Internal Affairs.

4.14. RECLASSIFYING PREVIOUSLY DECLASSIFIED INFORMATION

4.14.1. Information may be reclassified after it has been declassified and released to the public under proper authority. The following conditions will be met for CBP information that falls within this chapter.

- The Secretary of Homeland Security or Deputy Secretary personally endorses, in writing, that the reclassification action is in the best interest of national security and meets the standards and criteria for classification.
- The released information may be reasonably recovered and brought back under DHS control.
- The reclassification action is reported within 30 days to the Director, Information Security Oversight Office.

4.15. RECORDS FOR ORIGINAL CLASSIFICATION ACTIONS

4.15.1. Persons performing original classification actions shall maintain a record of each action taken. The records shall include the total number of documents originally classified by classification level and by declassification date.

- Records will be counted and reported by document not by page. For example, a newly created original classified document consisting of multiple pages and containing both SECRET and CONFIDENTIAL information is counted and reported as one original classified document at the SECRET level.
- Records will be submitted annually to the Office of Internal Affairs. The Office of Internal Affairs will submit one component report to the DHS

Office of Security as part of the annual reporting requirements defined in EO 12958, as amended, Chapter 3.3.24 of this handbook, and DHS reporting requirements policy, including MD 11044.

4.16. CLASSIFICATION CHALLENGES.

4.16.1. Authorized holders of classified information, who, in good faith, believe its classification status is improper, are encouraged and expected to challenge the classification status. Classification challenges shall be presented to the classifier of the information. Where necessary, assistance and/or anonymity in processing a classification challenge can be obtained by processing the challenge through the DHS Office of Security.

4.17. INFORMAL CLASSIFICATION CHALLENGES.

4.17.1. Classification challenges do not prohibit an authorized holder from informally questioning the classification of information through direct and informal contact with the classifier. When appropriate or when uncertainties exist over the classification status, holders of classified information are encouraged to make direct contact with the classifier to obtain clarification. When a change in classification results from an informal challenge, the challenger will ensure the official from whom the change was received is authorized to make such a change and a record of the change, to include the official's name, position, agency and date is maintained with a file copy of the document.

4.18. FORMAL CLASSIFICATION CHALLENGES

4.18.1. Formal challenges to classification shall be in writing and presented to an OCA having jurisdiction over the challenged information. Every effort should be made to keep the written correspondence unclassified. However, if the challenge includes classified information it shall be marked and safeguarded accordingly. The written correspondence shall sufficiently describe the information being challenged and can consist of only questions as to why the information is classified and why it is classified at a particular level.

- Individuals submitting a classification challenge shall not be subject to retribution of any kind for bringing such actions. Anonymity can be requested by processing the challenge through the Office of Internal Affairs or DHS Office of Security.
- The OCA receiving the challenge shall provide a written response with a classification/declassification decision to the challenger within sixty (60) days of receipt.
- The individual submitting the challenge has a right to appeal the decision to the Interagency Security Classification Appeals Panel established by EO 12958 §5.3, as amended. The Office of Internal Affairs will assist in appeals as needed.
- Challenged information remains classified and shall be protected at its

highest level of classification until a final classification determination is made by an appropriate OCA.

4.19. DERIVATIVE CLASSIFICATION

4.19.1. Unlike original classification, derivative classification is incorporating, paraphrasing, restating, reproducing or generating in new form, information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on guidance provided in a security classification guide.

4.20. DERIVATIVE CLASSIFICATION AUTHORITY

4.20.1. Delegated authority is not required to perform a derivative classification action. Unless restricted by Assistant Commissioners, Directors and alike of a CBP Office, any CBP employee with the appropriate level of security clearance and the need to perform derivative classification as part of their official government duties is authorized to do so.

4.21. DERIVATIVE CLASSIFICATION APPLICATIONS

4.21.1. Personnel performing derivative classification shall follow the guidance noted below:

- Respect and forward original classification markings cited on the source or in a security classification guide into the newly created document.
- Apply all applicable classification markings, declassification instructions, and handling on the newly created material.
- Attach a listing of classified source(s) to the official file or record copy.

4.21.2. Questions on the classification markings as they appear on the source or in a security classification guide will be referred to the originator. Questions can also be addressed to the Office of Internal Affairs or the Office of Internal Affairs, Security Liaison and Representative, which will coordinate with the originator.

4.22. RECORDS OF DERIVATIVE CLASSIFICATION ACTIONS

4.22.1. Personnel performing derivative classification actions shall maintain records of each action taken. Records shall include the total number of documents derivatively classified by classification level.

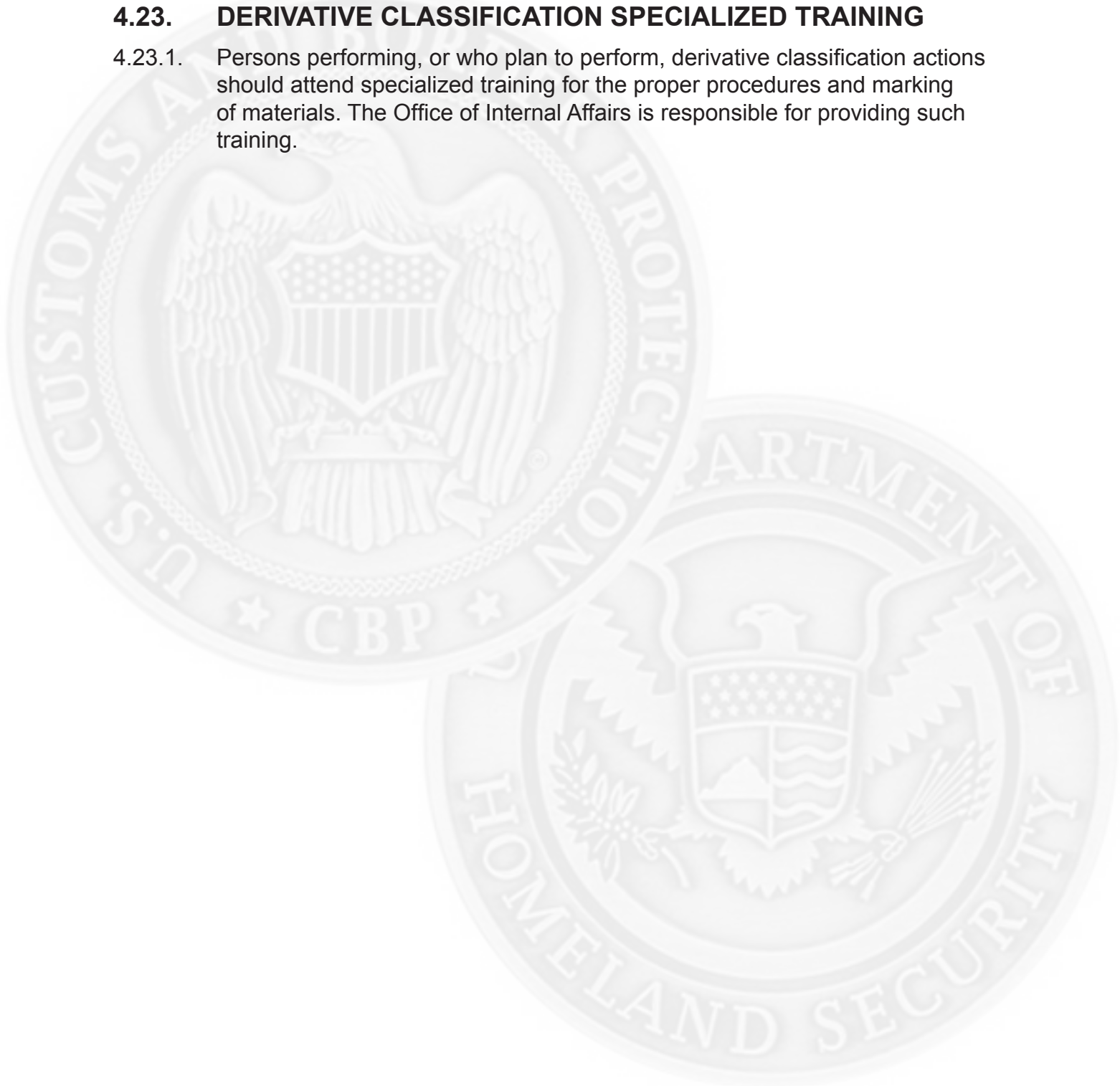
4.22.2. Records for classification actions will be counted and reported by document-not by page. For example, a newly created derivatively classified document consisting of multiple pages and containing both SECRET and CONFIDENTIAL information is counted and reported as one derivatively classified document at the SECRET level.

4.22.3. Records will be maintained by fiscal year and submitted annually to the Office

of Internal Affairs. The Office of Internal Affairs will submit one component report to the DHS Office of Security as part of the annual reporting requirements defined in EO 12958, as amended.

4.23. DERIVATIVE CLASSIFICATION SPECIALIZED TRAINING

- 4.23.1. Persons performing, or who plan to perform, derivative classification actions should attend specialized training for the proper procedures and marking of materials. The Office of Internal Affairs is responsible for providing such training.



5. CHAPTER 5: DECLASSIFICATION

5.1. POLICY

- 5.1.1. Information that continues to meet the classification requirements of Executive Order 12958, Classified National Security Information, requires continued protection; all Customs and Border Protection information to include legacy Customs and Immigration and Naturalization information shall be declassified as soon as it no longer meets the standards for classification under this executive order.
- 5.1.2. CBP personnel shall coordinate with the CBP Records Manager before reviewing records in their holdings to ensure that appropriate procedures are established for maintaining the integrity of the records and that the National Archives and Records Administration (NARA) receives accurate information about CBP declassification actions when records are transferred to NARA.
- 5.1.3. CBP senior officials who have reason to believe that the public interest in disclosure of information outweighs the need for continued classification shall refer the matter to the Office of Internal Affairs, who will further coordinate with the appropriate original classification authority or DHS Senior Official.
- 5.1.4. None of the provisions cited in this directive apply to information classified in accordance with the Atomic Energy Act of 1954, as amended (Restricted Data and Formerly Restricted Data).

5.2. DECLASSIFICATION AUTHORITY

- 5.2.1. Information may be declassified or downgraded by:
- The Secretary of Homeland Security;
 - The DHS Chief Security Officer as defined in DHS MD 8100.3;
 - Officials who have been delegated Original Classification Authority, their current successor in function, or a supervisory official of either;
 - Officials who have been delegated declassification authority, in writing by the Secretary or DHS Senior Agency Official; and
 - CBP Declassification Authorities identified by appropriate delegation order.
- 5.2.2. CBP officials with declassification authority shall develop and issue declassification guides to facilitate effective review and declassification of CBP information (which includes legacy the U.S. Customs Service and the Immigration and Naturalization Service information) not previously covered by a classification or declassification guide, and for information exempt from automatic declassification.
- 5.2.3. Declassification Authority is not required for simply canceling or changing classification markings in accordance with declassification or downgrading instructions cited on a document, directions found in a security classification

guide or declassification guide, or instructions received from an original classification or declassification authority as defined below.

5.3. EXTENSION OF CLASSIFICATION

- 5.3.1. If an original classification authority with jurisdiction over the information does not extend the classification of information that has been assigned a specific date or event for declassification, the information is automatically declassified upon the occurrence of the date or event.
- 5.3.2. If an original classification authority has assigned a date or event for declassification that is less than 25 years from the date of classification, an original classification authority with jurisdiction over the information may extend the classification duration of such information for a period not to exceed 25 years from the date of origination.
- 5.3.3. Decisions to extend classification must take into account the potential difficulty of notifying holders of the extension; including the possible inability to ensure continued, uniform protection of the information. Officials who make a determination to extend a declassification date are responsible for notifying holders of the information of the decision and providing a new date and instructions for declassification.
- 5.3.4. For information in records determined to have permanent historical value, successive extensions of classification may not exceed 25 years from the date of the information's origin.

5.4. EXEMPTION FROM DECLASSIFICATION (INFORMATION NOT CONTAINED IN A FILE SERIES)

- 5.4.1. Circumstances may arise where the safeguarding of classified information may be extended beyond the 25-year period and exempt from automatic declassification. The following information may be exempt from automatic declassification as defined below, if approved pursuant to 5.4.2.
 - Reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;
 - Reveal information that would assist in the development or use of weapons of mass destruction;
 - Reveal information that would impair U.S. cryptologic systems or activities;
 - Reveal information that would impair the application of state of the art technology within a U.S. weapon system;
 - Reveal actual U.S. military war plans that remain in effect;
 - Reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine

ongoing diplomatic activities of the United States;

- Reveal information that would clearly demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees from whom protection services, in the interest of the national security, are authorized;
- Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or
- Violate a statute, treaty, or international agreement.

5.4.2. For CBP information that falls within one or more of the categories in [Chapter 5.4.1](#), exemption requests shall be endorsed by the CBP Commissioner and submitted through the DHS Chief Security Officer to the DHS Secretary. Exemptions endorsed by the Secretary will be submitted to the Information Security Oversight Office for approval. Submissions shall be made no earlier than five (5) years, and no later than 180 days, before the information is scheduled for automatic declassification. Requests should have the following information:

5.4.3. Description of the specific information to be exempted;

- Explanation why the information must remain classified beyond the 25-year period; and
- Except for the identity of a confidential human source or human intelligence source, a specific date or event upon which the information will be declassified.

5.5. EXEMPTION FROM DECLASSIFICATION (INFORMATION CONTAINED IN A SPECIFIC FILE SERIES)

- Specific file series may be exempt from the 25-year automatic declassification provisions of the EO 12958, as amended. Such exemption requests shall be endorsed by the CBP Commissioner and submitted through the DHS Chief Security Officer, to the DHS Secretary. The DHS Secretary shall notify the President, through the Assistant to the President for National Security Affairs and the Information Security Oversight Office, of any specific file series proposed for exemption from 25-year automatic declassification. Submissions shall be made no earlier than 5 years, and no later than 180 days, before the information is scheduled for automatic declassification. In addition to the specific exemption cited above, submissions shall include:
 - Description of the file series;
 - Explanation of why the information within the file series must remain classified beyond a 25-year period; and

- o Except for the identity of a confidential human source or human intelligence source, a specific date or event upon which the information will be declassified.

5.5.1. Information that falls within the file series in Section 5.4.4 shall not be subject to automatic declassification unless the DHS Secretary specifically decides to remove the series from the exempted category. Information exempted from automatic declassification at 25 years remains subject to the mandatory and systematic declassification review provisions of this handbook.

5.6. ONSET OF AUTOMATIC DECLASSIFICATION

5.6.1. The following provisions shall apply to the onset of automatic declassification:

- Classified records within an integral file block that are otherwise subject to automatic declassification under this chapter, shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.
- If a CBP office purposes to exempt a specific file series of records from automatic declassification, based on Section 5.4.2, the head of the office shall submit the request for change to CBP Office of Internal Affairs for an assessment. The Office of Internal Affairs will forward the request to the DHS Office of Security and the Director of the Information Security Oversight Office, before the records are subject to automatic declassification. The Secretary or the DHS Chief Security Officer may delay automatic declassification for up to five (5) additional years for classified information contained in microforms, motion pictures, audiotapes, videotapes, or comparable media that make a review.
- If a CBP office purposes to exempt a specific file series of records from automatic declassification, based on Section 5.4.2, the head of the office shall submit the request for change to CBP Office of Internal Affairs for an assessment. The Office of Internal Affairs will forward the request to the DHS Office of Security and the Director of the Information Security Oversight Office, before the records are subject to automatic declassification. The Secretary or the DHS Chief Security Officer may delay automatic declassification for up to three (3) years for classified records that have been referred or transferred to DHS by another agency less than three (3) years before automatic declassification would otherwise be required.
- If a CBP office purposes to exempt a specific file series of records from automatic declassification, based on Section 5.4.2, the head of the office shall submit the request for change to CBP Office of Internal Affairs for an assessment. The Office of Internal Affairs will forward the request to the Director of the Information Security Oversight Office, the Secretary or DHS Chief Security Officer may delay automatic declassification for up to three (3) years from the date of discovery of classified records that

[RETURN TO TOP](#)

were inadvertently not reviewed prior to the effective date of automatic declassification.

- o Information contained in records not determined to be permanently valuable, and not scheduled for disposal or retention by the National Archives, is not subject to automatic declassification. CBP retention and destruction requirements apply.

5.7. MANDATORY DECLASSIFICATION REVIEW

- 5.7.1. Any individual may request a review for declassification of information classified under EO 12958, as amended, or its predecessor orders. Such requests shall be sent to the Department of Homeland Security, Director, Departmental Disclosure, Privacy Office, Washington D.C. 20528.
- 5.7.2. Information originated by the incumbent President; the incumbent President's White House Staff; committees, commissions, or boards appointed by the incumbent President, or other entities within the Executive Office of the President that solely advise and assist the incumbent President are exempt from the provisions of this chapter.
- 5.7.3. Responsibilities
- The Disclosure Office shall serve as the central processing point for all mandatory review requests concerning DHS information. The Disclosure Officer will promptly, but no later than thirty days from receipt, forward mandatory review requests to the applicable DHS organizational element(s) having primary jurisdiction over the requested information. The Disclosure Officer will provide the requester with an acknowledgment of receipt of the request.
 - Customs and Border Protection shall promptly process any request received. The CBP FOIA Office shall receive such requests and properly coordinate with the Office of Internal Affairs. Information reviewed shall be declassified if it no longer meets the standards for classification established by Executive Order 12958, as amended, and this handbook. Information that is declassified shall be released to the requester unless withholding is appropriate under applicable law (for example, the Freedom of Information Act or the Privacy Act of 1974).
- 5.7.4. Processing Mandatory Review Requests
- The request must sufficiently describe the document or material with enough specificity to allow it to be located by CBP personnel with a reasonable amount of effort. When the description of the information in the request is deficient, the FOIA Office shall solicit as much additional identifying information as possible from the requester. If the information or material requested cannot be obtained with a reasonable amount of effort, the FOIA Office shall provide the requester, through the DHS Disclosure Office, with written notification, of the reasons why no action will be taken

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

and of the requester's right to appeal.

- Requests for review of information that has been subjected to a declassification review request within the preceding two years shall not be processed. The DHS Disclosure Officer will notify the requester of such denial.
- Requests for information exempted from search or review under Sections 105C, 105D, or 701 or the National Security Act of 1947 (50 USC 403-5c, 403-5e, and 431), shall not be processed. The DHS Disclosure Officer will notify the requester of such denial.
- If documents or material being reviewed for declassification under this chapter contain information that has been originally classified by another government agency, the reviewing activity shall notify the Disclosure Officer. Unless the association of that organization with the requested information is itself classified, the DHS Disclosure Officer will then notify the requester of the referral.
- CBP may refuse to confirm or deny the existence, or non-existence, of requested information when the fact of its existence, or non-existence, is warrants protection.
- CBP shall make a final determination on requests received as soon as practicable but within one year from receipt. When information cannot be declassified in its entirety, CBP will make reasonable efforts to redact those portions that still meet the standards for classification and release those declassified portions of the requested information that constitute a coherent segment.
- The Office of Internal Affairs shall notify the DHS Disclosure Officer of the determination made in the processing of a mandatory review request. Such notification shall include the number of pages declassified in full; the number of pages declassified in part; and the number of pages where declassified was denied.
- The DHS Disclosure Officer shall maintain a record of all mandatory review actions for reporting in accordance with applicable federal requirements.

5.7.5. Processing Appeals

- The mandatory declassification review system shall provide for administrative appeal in cases where the review results in the information remaining classified. The requester shall be notified of the results of the review and of the right to appeal the denial of declassification. To address such appeals, the DHS Disclosure Office will convene a DHS Classification Appeals Panel (DHS/CAP). The DHS/CAP will, at a minimum, consist of representatives from the DHS Disclosure Office, the DHS Office of Security, the DHS Office of General Counsel, and a representative from CBP, if CBP information is involved.

[RETURN TO TOP](#)

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

- If the requester files an appeal through the DHS/CAP, and the appeal is denied, the requester shall be notified of the right to appeal the denial to the Interagency Security Classification Appeals Panel (ISCAP).

5.7.6. Foreign Government Information

- The declassification agency is the agency that initially received or classified the information. When foreign government information is being considered for declassification or appears to be subject to automatic declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that would prevent its declassification at that time. The declassifying agency or the Department of State, as appropriate, should consult with the foreign government prior to declassification.

5.7.7. Freedom of Information Act and Privacy Act Requests

- If a requester submits a request under both the mandatory declassification review provisions cited in this handbook and the Freedom of Information Act (FOIA), 5 USC §552, the requester shall be advised to elect one process or the other. If the requester fails to elect one or the other, the request will be treated as a FOIA request.

5.7.8. Systematic Declassification Review

- CBP shall conduct systematic declassification review for classified information that is exempted from automatic declassification which:
 - Contain information that has been identified to have significant value for historical or scientific research or for promoting the public welfare; and
 - Have reasonable likelihood of being declassified upon review.
- CBP personnel shall contact the Office of Internal Affairs for further systematic declassification review guidance.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

6. CHAPTER 6: MARKING CLASSIFIED INFORMATION

6.1. POLICY

- 6.1.1. A uniform security classification system requires that standard markings be applied to classified information. At the time of original classification, all national security information shall be marked in a manner appropriate to the medium involved. This chapter sets forth the requirements described by the Information Security Oversight Office Directive No. 1 and 32 CFR §2001, et seq.
- 6.1.2. The DHS standard security classification guide template also prescribes the markings that shall be uniformly and conspicuously applied to ensure the classified status of the information, the level of protection required, and the duration of the classification. See DHS MD 11041, Appendix 1 for further information.
- 6.1.3. Overall Markings. Documents shall be marked with the highest classification level (Top Secret, Secret or Confidential) of information contained in the document. The marking shall be printed or stamped in bold letters at the top and bottom of the outside front cover (if there is one), on the title page (if there is one), on the first page, and on the outside back cover (if there is one).
- 6.1.4. Page Marking. Each interior page is typed or stamped at the top and bottom according to the highest classification of the contents of the page, when appropriate, or according to the overall classification of the document. The three authorized classification designations (Top Secret, Secret or Confidential) may be used in conjunction with approved Intelligence Community compartmented information code words.
- 6.1.5. Portion Marking
- Each subject line, title, paragraph, subparagraph, section (i.e. classified diagram, map, drawing, etc.) or similar portion of a classified document shall be marked to show the level of classification of that portion or to indicate that it is unclassified. Classification of portions of a document must be shown by placing the appropriate classification symbol immediately before or after the portion. In marking portions, the parenthetical symbols, “(TS)” for Top Secret, “(S)” for Secret, “(C)” for Confidential, and “(U)” for Unclassified will be used.
 - The Director of the Information Security Oversight Office (ISOO) may grant and revoke waivers of the foregoing portion marking requirement. A request for such a waiver must be made through the Office of Internal Affairs to DHS Office of Security. The written request must identify the information or class of documents for which the waiver is sought and a declaration that the circulation of the document and its potential as a source for derivative classification determinations will be kept to a

[RETURN TO TOP](#)

minimum. The increased administrative burden of portion marking may not be used as a sole justification for the waiver.

- 6.1.6. At the time of original classification the information shown in the example below shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner.
- 6.1.7. One of the three classifications, Top Secret, Secret or Confidential as defined in [Chapter 4.6](#) of this handbook.
- 6.1.8. The identity, by name or personal identifier and position, of the original classification authority and the agency and office of origin, if not otherwise evident:
- Example:
Classified By: Assistant Commissioner, Office of Intelligence
U. S. Customs and Border Protection
Reason: 1.5 (g) Vulnerabilities or capabilities of systems, installations, instructions

- 6.1.9. A concise reason for classification which, at a minimum, cites the applicable classification category as defined in [Chapter 4.6](#).

- Example

Classified By: Commissioner,
U.S. Customs and Border Protection

- When the reason for classification is not apparent from the content of the information (e.g., classification by compilation) the classifier shall provide a more detailed explanation of the reason for classification.
- 6.1.10. Declassification Instruction. Note: the X1 through X8 exemption categories formerly used to exempt information from 10-year declassification can no longer be used. The duration of the original classification decision shall be placed on the “Declassify On” line. All classified materials shall have a declassification date and/or instruction. One of the following instructions shall apply:
- A date or event for declassification less than 10 years, or if unable to identify such a date or event;
 - A date 10 years from the date of the document for declassification;
 - A date greater than 10 and less than 25 years from the date of the

document; or

- A date 25 years from the date of the document.

6.1.11. The following information may be exempt from automatic declassification as defined below, if approved pursuant to 5.4.2.

- Reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;
- Reveal information that would assist in the development or use of weapons of mass destruction;
- Reveal information that would impair U.S. cryptologic systems or activities;
- Reveal information that would impair the application of state of the art technology within a U.S. weapon system;;
- Reveal actual U.S. military war plans that remain in effect;
- Reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;
- Reveal information that would clearly demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees from whom protection services, in the interest of the national security, are authorized;
- Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or
- Violate a statute, treaty, or international agreement.

6.1.12. Derivative Classification Markings

6.1.13. The Information Security Oversight Office Directive No.1 “Marking Classified Information Pamphlet” sets forth the uniform security classification system for standard markings that are applied to classified information, original or derivative.

6.1.14. The DHS Standard Security Classification Guide, also describes the markings that shall be uniformly and conspicuously applied to classified information.

7. CHAPTER 7: ACCESS AND DISSEMINATION OF CLASSIFIED INFORMATION

7.1. POLICY

- 7.1.1. Federal employees are not automatically granted access to classified information. An employee is eligible for access to classified information only when the employee has been determined to be trustworthy by an appropriate background investigation and access is essential to the accomplishment of lawful and authorized government purposes.
- 7.1.2. As defined in the Personnel Security Handbook, HB 1400-07, CBP Form 6100 is used to request security clearances for CBP personnel.
- 7.1.3. Each head of CBP offices, supervisors, or program managers, must ensure that only authorized persons obtain access to classified information. No employee has the right to gain access to classified information solely by virtue of title, position, or level of security clearance. Before classified information is disclosed, the holder must verify the recipients' identification and security clearance through the Office of Internal Affairs, Personnel Security Division and/or CBP personnel, e.g., designated security liaisons and/or other liaisons that have been authorized by the Office of Internal Affairs, Personnel Security Division to verify personnel security clearances through CBP's official security clearance database.
- 7.1.4. CBP personnel who are granted security clearances shall receive such notification from the Office of Internal Affairs, Personnel Security Division, receive a briefing on the safeguarding and handling of classified information, must sign the SF-312 Classified Information Nondisclosure Agreement, and the Foreign Contact Non-disclosure agreement. All forms must be submitted to the Office of Internal Affairs, Personnel Security Division, prior to the formal granting of a security clearance.
- 7.1.5. The Office of Internal Affairs, Director, Personnel Security Division, shall suspend, cancel or revoke a security clearance when the security clearance or access is no longer consistent with the interests of national security.
- 7.1.6. Upon termination of a security clearance, the holder shall receive a formal security debriefing describing the continuing responsibility to protect the national security information to which the individual had access. The debriefing section of the SF-312 Nondisclosure Agreement shall be completed upon the debriefing. The Office of Internal Affairs and/or the servicing regional Security Officer may conduct the security debriefing. The debriefing acknowledgment form shall be sent to the headquarters Office of Internal Affairs, Personnel Security Division for file.
- 7.1.7. As defined in the National Industrial Security Manual, contractors and

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

consultants working in the federal government may not be given access to classified material without the proper processing of a classified contract and the execution of a DD-254. To obtain classified contract and DD-254 processing refer to the CBP National Industrial Security Chapter 12.2, Processing Requirements. Section 7.3 provides the security clearance verification process for CBP contractors/consultants.

7.1.8. Contractors and consultants may be granted access to classified material in the custody of CBP after Section 7.1.7 is executed accordingly and the Office of Internal Affairs, Personnel Security Division has verified the applicable contractors hold the appropriate security clearance through Defense Security Service (DSS).

7.1.9. As defined in the Personnel Security Handbook, HB 1400-07, all CBP contractors and consultants are required to undergo a Background Investigation (BI) to determine suitability for contractor employment. This is not the same as receiving a security clearance for access to classified information. CBP program offices that require contractors and/or consultants to access classified information are required to be in compliance with Section 7.1.8 .

7.1.10. Classified information (in any form), to include extra copies, is not personal property and may not be removed from the Government's control by any departing employee or contractor. Designated Security Officer, and other designated security liaison appointments and/or positions shall ensure all debriefed personnel have accounted for all classified information in their possession and transferred it to an authorized custodian.

7.2. ACCESS AND DISSEMINATION RESTRICTIONS

7.2.1. Classified information may be discussed and disclosed under the following conditions:

- The recipient of the classified information has a current security clearance at the appropriate level and the security clearance has been verified per the Personnel Security Handbook, HB 1400-07.
- The holder of the classified information has validated the recipient's need-to-know; and
- discussion must be held in an appropriately cleared Federal Government or contractor facilities to preclude unauthorized disclosure of classified information.
- The recipient has the means to protect the information in accordance to EO 12958 and other applicable DHS, CBP policies, through retention, storage or destruction.

7.3. CBP EMPLOYEE VISIT CERTIFICATION OF SECURITY CLEARANCE

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

7.3.1. CBP employees who have a need to certify their security clearance information to another government agency or contracting facility must initiate the [CBP Form 6101](#), Classified Visit Request Security Clearance Certification as defined in the Personnel Security Handbook, HB 1400-07. Some agencies or government facilities require the use of their own form for visits to their facilities. The individual coordinating the security clearance certification should verify the method acceptable to other agencies prior to the visit. For policy regarding outside CBP employee visit certification of security clearance refer to Section 7.6.10.

7.4. DISSEMINATION OF CBP CLASSIFIED INFORMATION.

7.4.1. Each CBP Office head, Director, or Program Manager is responsible for providing specific procedures for dissemination of classified information originated by his or her office. Procedures must include but not be limited to the guidance cited in Section 7.2.1 and Sections 7.5-7.7.6.11 and must otherwise be consistent with this Directive.

7.5. DISSEMINATION OF OTHER AGENCY INFORMATION

7.5.1. Also commonly known as the “Third Agency Rule.” Classified information originated by another agency and furnished to DHS and DHS components shall not be further distributed outside of DHS without the prior consent of the originating agency. Unless limitations have been imposed by the originator, this restriction does not apply to further distribution to authorized personnel within DHS and components of DHS, or distribution to cleared contractors who require the information in performance of a DHS contract.

7.6. DISSEMINATION OF CLASSIFIED INFORMATION

7.6.1. Outside the Executive Branch

- Classified information can be made available to persons outside the Executive Branch provided that such information is necessary for performance of a function for which the U.S. Government will derive a benefit or advantage, and that such release is not prohibited by the originating department or agency.

7.6.2. Judicial

- The CBP Chief Counsel will be consulted whenever a litigation request or demand is made upon CBP personnel for official CBP information for testimony concerning such information. The personnel upon whom the request or demand was made shall immediately notify the Office of Chief Counsel or servicing regional Associate or Assistant Chief Counsel. The CBP Office of Chief Counsel will consult with the DHS Office of the General Counsel accordingly with all requests. Classified information entered into the Judicial System shall be handled in accordance with the Classified Information Procedures Act (PL 96-456). Justices of the U.S.

Supreme Court and Judges of the U.S. Courts of Appeals and District Courts do not require an investigation and determination of eligibility for access to classified information. All other members must be appropriately investigated and granted a security clearance.

7.6.3. Congress

- Access to classified information or material by Congress, its committee, members, and staff representatives shall be coordinated with the CBP Office of Congressional Affairs. The CBP Office of Congressional Affairs will further coordinate with the DHS Office of Legislative Affairs. Any CBP employee testifying before a Congressional committee in executive session, in relation to a classified matter, shall obtain the assurance of the committee that the individuals present have a security clearance commensurate with the highest classification of information that may be discussed. Members of Congress, by virtue of their elected positions, do not require an investigation and determination of eligibility for access to classified information. All other congressional staff members and other associated officials must be appropriately investigated and granted a security clearance.

7.6.4. State, Local, Tribal, and Private Sector Officials

- State Governors, by virtue of their elected positions, do not require an investigation and determination for eligibility for access to collateral classified information. Other State, Local, Tribal and Private Sector Officials must be appropriately investigated and granted a security clearance by DHS or other Federal government agencies.

7.6.5. Foreign Nationals

- U.S. Intelligence information and classified information may be shared with foreign nationals only when consistent with U.S. national security and foreign policy objectives and when an identifiable benefit can be expected for the United States. For requirements of sharing of such information with foreign nationals and security clearance verification, refer to the CBP Office of Intelligence and Operations Coordination who further coordinates with the DHS Foreign Disclosure Office.

7.6.6. Representatives of the Government Accountability Office (GAO)

- Representatives of the GAO may be granted access to classified information when such information is relevant to the performance of the statutory responsibilities of that office. Certifications of security clearances, and the basis thereof, shall be accomplished pursuant to arrangements between GAO and CBP Office of Internal Affairs.

7.6.7. Government Printing Office (GPO)

- Documents and material of all classification may be processed by the GPO, which protects the information in accordance with the guidelines

prescribed in the Executive Order, 12958, as amended, Classified National Security Information.

7.6.8. Historical Researchers

- Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to classified information provided that a CBP Original Classification Authority (OCA), with classification jurisdiction over the information, accomplishes the following:
 - Makes a written determination that such access is clearly consistent with the interests of National Security in view of the intended use of the material to which access is granted, and certifies that the requester has been found to be trustworthy based on such investigation as determined by the DHS CSO.
 - Limits such access to specific categories of information over which CBP has classification jurisdiction, and to any other category of information for which the researcher obtains the written consent of a CBP or other DHS component OCA, or non-DHS Department or Agency that has classification jurisdiction over information contained in or revealed by the document, within the scope of the proposed historical research.
 - Maintains custody of the classified material at a DHS installation or activity, or authorizes access to documents in the custody of the National Archives and Records Administration.
 - Obtains the researcher's agreement to safeguard the information and to submit any notes and manuscripts for review by CBP or non-DHS departments or agencies with classification jurisdiction, for a determination that no classified information is contained therein. This information shall be included in a non-disclosure agreement, which shall be executed by the researcher as a condition of access.
 - Issues an authorization for access valid for not more than two years from the date of issuance.

7.6.9. Former Presidential Appointees

- Persons who previously occupied policy-making positions, to which the President appointed them, may not remove classified information upon departure from office. Such material must remain under the secure control of the U.S. Government. Such persons may be authorized access to classified information they originated, received, reviewed, signed, or that was addressed to them while serving as such an appointee, upon approval of the Secretary, Deputy Secretary or Chief Security Officer in consultation with the Office of the General Counsel. The approving official shall:
 - Make a written determination that such access is clearly consistent

with the interest of national security in view of the intended use of the material to which access is granted, and by certifying that the requester has been determined to be trustworthy based on such investigation as determined by the CSO.

- o Limit access to specific categories of information over which DHS has classification jurisdiction and to any other category of information for which the former appointee obtains the written consent of a non-DHS Department or Agency that has classification jurisdiction over information contained in or revealed by documents within the scope of the proposed access.
- o Retain custody of the classified material at a DHS installation or activity, or authorizes access to documents in the custody of the National Archives and Records Administration.
- o Obtain the former Presidential appointee's agreement, through the execution of a non-disclosure agreement, to safeguard the information and to submit any notes and manuscripts for review by DHS or non-DHS departments or agencies with classification jurisdiction for a determination that no classified information is contained therein.

7.6.10. Security Clearance Certification CBP Visit Notification

- For personnel visiting CBP facilities for meetings/projects where classified information is shared, security clearance verification shall be submitted from the Security Office of the parent organization to the Office of Internal Affairs (IA), Personnel Security Division (PSD). CBP personnel shall not disclose any classified information to visitors until notification from Internal Affairs/ Personnel Security Division (IA/PSD) that security clearance has been verified.

7.6.11. Emergency Release of Classified Information

- In an emergency situation, in which there is an imminent threat to life or defense of the homeland, the Secretary of Homeland Security has delegated the authority to release such information in the custody of CBP to the Commissioner, U.S. Customs and Border Protection. Under these conditions the Commissioner shall follow the provisions of the Department of Homeland Security Delegation of Emergency Authority to Disseminate Classified Information, DHS Delegation No. 12001.

8. CHAPTER 8: CUSTODY AND ACCOUNTABILITY

8.1. POLICY

8.1.1. Any person who has possession of, or is charged with responsibility for classified information must protect and account for that information. The following measures shall be applied to properly protect classified information:

- While in use, classified information shall not be left unattended, unless stored properly in accordance with this handbook.
- Before granting access to classified material, all CBP personnel must verify security clearance information per Chapter 7 of this handbook.
- An office that receives classified information (in any form) and has no authorized storage equipment available must either return the classified information to the sender, arrange with another office to properly store the information, or destroy it by an approved method as defined in Section 8.10.
- Custodian of classified information must ensure that persons who do not possess an appropriate security clearance and need-to-know do not access classified information.
- Classified information must be appropriately stored in a GSA-approved security container at all times when not in use.

8.1.2. Classified information must be covered with the appropriate GSA Standard Form (SF) cover sheet (SF-703, Top Secret; SF-704, Secret; or SF-705, Confidential).

8.2. CUSTODY DURING EMERGENCIES

8.2.1. In the event of fire, natural disaster, civil disturbance, terrorist activities, hostile action, or an evacuation of office space, classified information shall be protected by placing it in a GSA-approved security container and/or safe or by proper destruction.

8.2.2. Each program office shall prepare a general plan for the protection and destruction of classified information in the event of an emergency, as detailed in 8.2.1. Such plans should be forwarded to the Office of Internal Affairs and/or the Designated Security Officer (DSO) for review and approval, as appropriate.

- The plan should include the priority of safeguarding and destruction, persons responsible for the destruction, and the recommended place and method of destruction.
- The classified destruction plan shall be distributed to all cleared personnel working with classified information. The DSO, and/or other designated security liaison positions shall ensure that personnel are briefed on the

[RETURN TO TOP](#)

responsibilities of the plan.

8.3. ACCOUNTABILITY OF CLASSIFIED INFORMATION

8.3.1. In order to control and account for classified information, each CBP Office where classified information is generated and received must designate either a DSO and/or a CDC. CBP personnel who are designated in these positions shall ensure that the movement of classified information can be traced, dissemination is limited, prompt retrieval of information can be obtained, the loss of information can be detected, and excessive holding and reproduction are limited. However CBP personnel who serve in a security liaison position are not personally accountable for other CBP personnel who handle classified information.

8.4. ACCOUNTABILITY OF TOP SECRET INFORMATION

8.4.1. Each CBP office and/or program office that has requested and received approval from the Office of Internal Affairs to store Top Secret information is required to appoint an appropriately cleared CBP employee to serve as the Top Secret Control Officer (TSCO).

- Top Secret information within the National Capital Region will continue to be stored within the Sensitive Compartmented Information Facility (SCIF).

8.4.2. The TSCO appointment shall be made in writing, with a copy forwarded to the Office of Internal Affairs.

8.4.3. The TSCO is responsible for receiving, disseminating, and maintaining control and accountability of Top Secret information within their program office.

8.4.4. The TSCO is required to account for all Top Secret information using DHS Form 11000-03, Document Control Register Top Secret National Security Information.

- Each Top Secret document will be assigned a Document Control Number (DCN) and entered under the applicable Top Secret Control Account (TSCA).
 - o The DCN will consist of the office identifier, or other coding information, indicating the specific office possessing the document, the calendar year, and a sequential number indicating the number of documents generated/received within the calendar year.
 - o Information annotated on the DHS Form 11000-03 shall be unclassified. If the title of the document is classified, then it is recommended the DHS Form 11000-03 identify the document through the Top Secret DCN.
- When a Top Secret document is transmitted internal or external to CBP, the TSCO will coordinate the transmission. A Classified Document Record of Transmittal, DHS Form 11000-11.1, is required for the transmission.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- o Each Top Secret document in the TSCA will have attached to it a Top Secret Signature Record, DHS Form 11000-04. Each person having access to the Top Secret information will sign and date the form indicating they had access.
- o The TSCO shall maintain a copy of the DHS Form 11000-11.1 and DHS Form 11000-04.
- o If a signed receipt is not received within 30 days, the TSCO shall follow up with a second receipt or contact the recipient to determine the status.

8.4.5. Reproduction of Top Secret information. Reproduction of Top Secret Information will be coordinated with the TSCO.

- The DHS Form 11000-03 shall reflect any additional copies of reproduced Top Secret information.

8.4.6. Top Secret Information Annual Inventory. No later than December 31 of each year, a hands-on inventory of Top Secret material maintained in a Top Secret Control Account will be conducted. Inventory records will be maintained on file and submitted to the Office of Internal Affairs no later than January 31 of each year.

8.5. ACCOUNTABILITY OF SECRET AND CONFIDENTIAL INFORMATION

8.5.1. Except as required by the originator or as specified for certain categories of SECRET and CONFIDENTIAL information, there is no requirement to maintain accountability records or inventories for SECRET or CONFIDENTIAL information. However, Assistant Commissioners, Directors, and alike may mandate the use of accountability records within their respective offices at their discretion.

8.6. RECEIPTS FOR CLASSIFIED TRANSMISSION

8.6.1. When transport or transmission of classified information occurs external to a program office, the custodian of the information is responsible for the proper transmission in accordance with Chapter 10 of this handbook and obtaining signed receipts as set forth below.

8.6.2. Transmission of Top Secret information requires a receipt, DHS Form 11000-11.1 and coordination with the assigned Top Secret Control Officer as defined in Section 8.4.4.

8.6.3. A receipt is required for the transmission of SECRET and CONFIDENTIAL information internal or external to CBP.

8.6.4. Pending Receipts for Classified Transmission

- Receipts of classified information shall be received in a timely manner. The holder or Classified Document Custodian shall maintain a suspense

copy of all document receipts for classified material transferred external to CBP. If a signed receipt is not received within 30 days, then a follow-up receipt shall be mailed to the organization that received the mailed document. If a signed receipt is still not received within two weeks, the sender or Classified Document Custodian must contact the organization to determine the status of the classified material.

8.7. CLASSIFIED MEETINGS AND CONFERENCES

8.7.1. Meetings and conferences that involve classified information present special vulnerabilities to unauthorized disclosure. CBP Senior Managers shall limit:

- In-house gatherings and other impromptu meetings. For in-house gatherings and other impromptu meetings where classified information will be discussed, it is incumbent upon the host or sponsor of the meeting to ensure appropriate security measures are in place as defined below:
 - The meeting is held in an area under the secure control of a U.S. Government agency, or at an appropriately cleared U.S. contractor facility.
 - Ensure that all electronic equipment maintained in the room capable of transmitting signals outside the room, is powered off and disconnected from electrical outlets.
 - Conduct a sound attenuation test to ensure normal conversational tone from inside the room cannot be heard intelligibly from outside the room, pay particular attention to vents, ducts, and other openings. If public address or other amplification systems are used, conduct the test with these systems on and off.
 - Assign and post cleared host office personnel at exterior doors and hallways to keep the room's perimeter under surveillance and prevent passers-by from stopping and listening.
 - Limit the number of room entrances and access controls prior to or during the meeting to prevent access by unauthorized persons.
 - Control access to the room to prohibit those without proper authorization and security clearance from attending. Use an attendee roster if applicable, and have sufficient backup host office personnel available, as needed.
 - Ensure the security clearances of attendees are at least equal to the level of classified information to be disclosed and verify security clearance of participants in accordance with Chapter 7.3 of this handbook and the CBP Personnel Security Handbook, HB 1400-07.
 - Verify the identity of each participant via U.S. Government photo identification or similar documentation.
 - When notifying personnel or presenters of a classified meeting, inform them of the highest level of classified information to be presented/

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

discussed and when multiple presentations are given, the specific classification (or unclassified status) of each presentation.

- o Announcements of classified meetings shall be unclassified and shall not describe the specific classified subjects that are to be presented.
- o Ensure security protection for the room is maintained during breaks.
- o Comply with all security safeguards for classified information.
- o At the conclusion of the meeting, conduct an inspection of the room to ensure no classified materials have been left behind.

8.7.2. The dissemination of classified information to large audiences increases security risks and may involve substantial costs to provide adequate security. The number of meetings involving the dissemination of classified information must be limited; and those that are conducted shall only be authorized when the head of each office, determines in writing the:

(a) Conduct of the classified conference serves a specific U.S. Government purpose.

(b) The use of other prescribed channels for dissemination of classified information does not accomplish the purpose.

(c) The location selected for the meeting is under the secure control of a U.S. Government Agency or a U.S. contractor having an appropriate facility clearance.

(d) Adequate security procedures have been developed and can be implemented as defined in Section 8.7.1.

(e) Classified sessions shall be held only at a U.S. Government facility or a U.S. contractor facility where adequate physical security and procedural controls have been approved in accordance with the Physical Security Handbook.

(f) A physical security assessment of the selected facility and/or a Technical Surveillance Countermeasure (TSCM) survey may be conducted if deemed necessary by the Office of Internal Affairs.

8.8. REPRODUCTION OF CLASSIFIED MATERIAL

8.8.1. Documents and other materials containing classified information shall be reproduced only when necessary to accomplish the mission of the organization or for compliance with applicable statutes or directives and shall be kept to a minimum. This section outlines the security precautions necessary to protect classified information from possible compromise as a result of copier use. New technology available for copiers increases security vulnerabilities. Security measures must be in place to prevent: unauthorized

individuals from gaining access to copies of classified information, the misuse of copiers by authorized personnel, and information retention through latent or residual images on the machines or electronic memory is prevented. At a minimum, the copier security requirements below must be in place before any reproduction of classified information.

8.8.2. Copiers within Customs and Border Protection must first be designated and “approved” before being used for the reproduction of classified information. The Office of Internal Affairs, coordinating with the Office of Information Technology or the servicing Information Systems Security Officer, is designated as the approval authority. Determination of approved copiers must be based upon the following:

- Machines with unacceptable risks, such as machines that are connected to an unclassified LAN, equipped with remote diagnostics, equipped with an internal memory, or in some other way retain images, will not be approved for classified reproduction.
- Physical location of the copier. Approved machines must be located in locked or secured areas to deny access to unauthorized users. If no locked or secure area is available, the copier shall be located away from high traffic areas where unauthorized persons are situated. The location must allow continuous monitoring of the copier by office personnel during work hours.

8.8.3. After designation of a copier as “approved” it will be affixed with a GSA Standard Form (SF) label (SF-707, Top Secret; SF-708, Secret; or SF-709, Confidential) indicating the classification level it is approved to copy. Copiers not approved for classified information will have SF-710, Unclassified label applied to serve as a reminder to users not to copy classified information on this machine. Additionally, the Office of Internal Affairs, or DSO will issue a classified copier equipment approval letter which will be posted next to the copier. The letter at a minimum will identify: the machine(s) that is approved, the classification level that it is approved to copy, the location of the copier and the point of contact in the office. The point of contact will be required to coordinate with the Office of Internal Affairs or DSO when potential problems arise, or when there are incidents of possible compromise.

- Copies of the letters must be sent to the Office of Internal Affairs, headquarters for filing.

8.8.4. Accountability of Classified Information. Records must be maintained to show the accountability of certain classified information.

- The reproduction of Top Secret must be coordinated with the TSCO and accounted for in accordance with the procedures defined above in 8.4.4.
- Unless otherwise restricted by special dissemination or reproduction limitations, Secret and Confidential document reproduction accountability logs are not required but recommended.

8.8.5. Copier Security Procedures. The following are procedures for reproducing classified information.

- Reproduction of classified information is done on an approved copier machine. Refer to Section 8.8.2.
- Cleared individuals (security clearance) will remain at the copier until classified reproduction is complete.
- Before leaving the copier, cleared individuals must check the copier for any copies or originals that may be left in or around the copier.

8.8.6. Additional copies not needed or rejected copies must be destroyed in accordance with the procedures in Section 8.10.

- If the copier malfunctions and the copy or original cannot be retrieved, the Office of Internal Affairs and/or the DSO shall be notified to ensure that the copier is removed from approved service until the certification of the malfunction has been properly cleared.
- Scheduled Maintenance. The Office of Internal Affairs and/or DSO shall be notified prior to a scheduled service visit and arrange for a cleared individual to be present. Any documents, image retaining drum sheets, or memory chips removed from the machine must be collected by a cleared individual and submitted to the Office of Internal Affairs or DSO. No maintenance person shall be allowed to service any reproduction equipment used for the reproduction of classified materials without a cleared escort.

8.9. ANNUAL INVENTORY OF CLASSIFIED HOLDINGS

8.9.1. CBP offices maintaining classified information must conduct an annual inventory and review their classified holdings to reduce the amount necessary for operational and program purposes. All classified documents shall be reviewed upon initial receipt and during the annual inventory. The inventory shall include a review to determine possible downgrade, declassification or destruction of classified holdings. For documents that meet the requirements for downgrading or declassifying, refer to Chapter 5, Declassification, of this handbook. Documents which are no longer required for operational purposes must be disposed of in accordance with the provisions of the Federal Records Act and CBP records retention policy. For classified information that meets the requirements for destruction, refer to Section 8.10.

8.10. DESTRUCTION OF CLASSIFIED MATERIALS

8.10.1. When no longer needed as identified in Section 8.9.1, classified information shall be destroyed completely to preclude recognition or reconstruction of the classified information. Methods and equipment approved for destroying classified information include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition or pulverizing. The most common

method for Customs and Border Protection offices is destroying through use of a cross-cut shredder, see Sections 8.10.2 and 8.10.3. The use of strip-cut shredders, or other types of shredders not approved by NSA, as well as tearing into small pieces, or cutting up, are not acceptable means for destroying classified information.

- 8.10.2. Only National Security Administration (NSA) approved cross-cut shredders that produces a residue particle size that does not exceed 1/32-inch in width by 1/2-inch in length will be used for the destruction of all classified information.
- 8.10.3. Where maintenance is performed on such machines that involves rebuilding the shredder blade assembly, or where new shredders are purchased for the destruction of classified information, the replacement or new purchase must comply with CNSS Policy No. 16, National Policy for the Destruction of COMSEC Paper Material, and be equipment listed on the NSA Evaluated Products List (EPL) of High Security Cross-Cut Shredders. A copy of the EPL can be obtained from the Office of Internal Affairs and/or the DSO.
- 8.10.4. Technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media may be obtained from the Office of Internal Affairs.

8.11. END-OF-DAY SECURITY CHECKS

- 8.11.1. Each CBP office that receives, stores and/or processes classified information shall establish a system of security checks at the close of each working day to ensure that all classified information has been returned to the appropriate GSA-approved security container and is properly secured. Each office is also required to visibly display the Standard Form (SF) 701 Security Activity Checklist to ensure:
- All desk and counter tops are free of classified information and secured properly;
 - All COMSEC material is secured; and
 - All SF-702 Security Container Check Sheet information has been noted accordingly.

9. CHAPTER 9: STORAGE OF CLASSIFIED INFORMATION

9.1. POLICY

- 9.1.1. Classified national security information will be afforded a level of protection against unauthorized access and disclosure that is commensurate with its level of classification. When classified information is not under the personal control and observation of a cleared person, it must be guarded by personnel with the appropriate security clearance or stored in a locked General Services Administration (GSA) approved security container. Any person(s) having access to and possession of classified information is responsible for meeting the accountability and storage requirements prescribed in this handbook.
- 9.1.2. Classified information shall be secured under conditions adequate to prevent access by unauthorized persons. The requirements specified in this handbook represent the minimal acceptable security standards. Weapons, sensitive or valuable items such as funds, jewels, precious metals, or seized items, such as drugs, shall not be stored in the same container used to safeguard classified information. Security requirements for Sensitive Compartmented Information Facilities (SCIFs) are established by the Director of Central Intelligence through the Director of Central Intelligence Directives (DCIDs) or Intelligence Community Directives (ICDs). Current holdings of classified material shall be reduced to the minimum required for mission accomplishment. For more information regarding SCIFs at U.S. Customs and Border Protection (CBP), refer to the CBP Office of Intelligence and Operations Coordination (OIOC).

9.2. STANDARDS FOR STORAGE EQUIPMENT

- 9.2.1. GSA establishes and publishes minimum standards, specifications, and supply schedules for security containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information.

9.3. NEW PURCHASES

- 9.3.1. New purchases of GSA approved security containers or combination locks for GSA approved security containers, vaults, doors, and secure rooms shall conform to Federal Specification FF-L-2740A. Existing non-FF-L-2740A mechanical combination locks will not be repaired. If they should fail, they will be replaced with locks meeting FF-L-2740A standards.

9.4. MAINTENANCE

- 9.4.1. Maintenance performed on GSA-approved security containers must be in accordance with Federal Standard 809A, Neutralization and Repair of GSA-Approved Containers. When repairs to a GSA-approved security container affect its original integrity, the GSA-approved label shall be removed and the

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

container will no longer be authorized for the storage of classified information. For maintenance or repair issues for security containers, contact the Office of Internal Affairs and/or the designated security office.

9.5. TOP SECRET INFORMATION STORAGE

9.5.1. Before CBP Offices are allowed the storage of Top Secret information or materials within their facilities, a written request must be forwarded to the Office of Internal Affairs, Security Management Division for review and approval. Approvals and denials will be made based on the review of physical security measures and proposed supplemental controls.

9.5.2. Top Secret Information shall be stored in a GSA-approved security container. One or more of the following supplemental controls must also be in place:

- The location that houses the security container is subject to continuous protection by cleared guard or duty personnel;
- Cleared guard or duty personnel shall inspect the security container once every two hours;
- An Intrusion Detection System (IDS) is in place with cleared personnel arriving within 15 minutes of the alarm annunciation;
- A Security-In-Depth system, as determined by the CBP Physical Security Handbook Appendix 8.9, Intrusion Detection Systems, when the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740A; or
- A modular vault or a secure room constructed in accordance with the CBP Physical Security Handbook and equipped with an IDS, with cleared personnel responding within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth, or a 5-minute alarm response time if it is not.

9.5.3. Storage of Top Secret information in the National Capital Region will continue to be stored in the SCIF.

9.6. SECRET INFORMATION STORAGE

9.6.1. Secret Information shall be stored by one of the following methods:

- In the same manner as prescribed for Top Secret Information;
- In a GSA-approved security container or vault without supplemental controls; or
- In a non-GSA-approved container having a built-in combination lock or in a non-GSA-approved container secured with a rigid metal lock bar and a GSA-approved padlock (policy valid until October 1, 2012). When stored in a non-GSA approved container, one or more of the following supplemental controls must be in place:
 - The location that houses the security container must be subject to

continuous protection by cleared guard or duty personnel;

- o Cleared guard or personnel shall inspect the security container once every four hours; or
- o An Intrusion Detection System (IDS), approved by the Office of Internal Affairs, with a thirty-minute response time to the alarm location.

9.7. CONFIDENTIAL INFORMATION STORAGE

9.7.1. Confidential information shall be stored in the same manner as prescribed for Top Secret or Secret, without the supplemental controls.

9.8. OPEN STORAGE

9.8.1. Approval of open storage will be considered when the volume of material or operational necessity of the mission dictates. Only the Office of Internal Affairs, Security Management Division can authorize approvals; refer to DHS MD 11046 Open Storage Area Standards for Collateral Classified Information, and the Physical Security chapter of this handbook.

9.8.2. Sensitive Compartmented Information (SCI) shall only be stored in accordance with specifications and requirements of the Director, Central Intelligence Agency. The Department Homeland Security (DHS), Special Security Programs has oversight in accrediting DHS facilities for the storage of SCI.

9.8.3. The Office of Intelligence and Operations Coordination (OIOC) is the only CBP office authorized to receive and store SCI within CBP. Any requests for additional facilities for the storage of SCI must be approved by the Assistant Commissioner of OIOC. OIOC further coordinates with DHS for SCI facility accreditations.

9.8.4. For the storage requirements for sensitive but unclassified information e.g., "For Official Use Only"/"Law Enforcement Sensitive," refer to Chapter 13, Safeguarding Sensitive But Unclassified Information..

9.9. IDENTIFICATION OF SECURITY CONTAINERS

9.9.1. There shall be no external mark revealing the level of classified information stored in a security container.

9.9.2. Each security container must be marked accountability and ready identification. This can be accomplished in a variety of ways, including use of the existing property control number.

9.9.3. An internal or local system shall be established by which each security container in use (other than vaults/secure areas) can be easily identified by a consecutive number, without regard to physical location of the container.

9.9.4. Identification numbers will be fixed to the container where it will be conspicuously visible.

9.10. PROTECTING CLASSIFIED COMBINATIONS USING STANDARD FORM (SF) 700

- 9.10.1. Combinations to security containers, vaults or other areas approved for storage must be recorded on the SF-700, Security Container Information. The SF 700 must be completed accurately and reflect all pertinent information such as container's location, description/type, personnel with access to the combination, etc..
- 9.10.2. Knowledge of combinations shall be limited to the minimum number of persons necessary for operating purposes.
- Combinations shall not be recorded on calendars, rolodex, in desk drawers, in key-locked cabinets, in wallets, stored at home, etc. Combinations to security container storing classified information that are recorded on anything other than the required SF 700, Part 2A, will be considered a security violation.
- 9.10.3. When completed, the SF 700 shall be separated into its three parts;
- Part 1 shall be affixed to the inside of the security container, closest to the lock and visible when the container is open.
 - Part 2A, containing the written combination, will be sealed inside part 2.
 - Part 2, shall be stored in a separate security container as listed below;
 - CBP Headquarters and facilities located within the National Capital Region shall forward the SF-700, Part 2 to the CBP Office of Internal Affairs, Security Management Division headquarters,
 - CBP field offices shall forward the SF-700, Part 2 to the Director of the appropriate Office, Sector Headquarters, and/or sector or regional offices.
- 9.10.4. An SF 700 containing the combination of a container, vault, or secure room used for storage of classified information or material shall be afforded protection equal to that given to the highest level of classified information stored in the container. Therefore, the standards cited in this handbook and the requirements identified in DHS MD 11047 shall be strictly enforced for the transmission of those SF 700s.
- 9.10.5. An SF 700 must be completed for each lock, especially containers that have multiple locks and marked with the highest classification level that the security container is approved to store.

9.11. ACCESS TO CLASSIFIED COMBINATIONS

- 9.11.1. Only appropriately cleared and authorized employees shall have access to classified combinations. The number of employees with access shall be kept

to a minimum. Contact information shall be annotated on the SF 700 in case the container is ever found open and unattended.

9.12. CHANGING COMBINATIONS

9.12.1. Combinations to security containers shall be changed by the Office of Internal Affairs or by appropriately cleared government personnel.

9.12.2. Combinations shall be changed:

- When first placed in to use;
- Whenever an individual knowing the combination no longer requires access to it, unless other sufficient controls exist to prevent access to the lock;
- When the combination has been subject to actual or possible compromise;
- Every two years, if none of the above has occurred.
- When taken out of service, built-in combination locks shall be reset to the standard combination 50-25-50 and combination padlocks shall be reset to the standard combination 10-20-30.

9.13. SECURITY CONTAINER CHECK SHEET

9.13.1. A SF 702, Security Container Check Sheet, shall be placed on the exterior of each security container to record every time the container is opened, closed, and double-checked. Each opening and closing shall be recorded using the initials of the individual conducting the action and the time of the opening or closing. The “Checked By” column will be used every day that the office is occupied to conduct work. This is done to ensure that an individual who failed to complete the “Opened By” and “Closed By” blocks did not leave the security container open accidentally. The “Guard Check” column is optional. The individual who conducts the end-of-day double-check of the container must ensure that the container is properly locked and secured by pulling on the handles of the drawers and then spinning the combination dial at least four rotations in the same direction. Although it is not always possible, the person conducting the end-of-day double-check of the security containers should not be the same person who opened and closed the security container during the duty day. This procedure provides an additional security measure to ensure that classified information in the office is protected. Supervisors are responsible for establishing procedures to ensure that the requirements in this chapter are met.

9.14. OPEN-CLOSED SIGNS

9.14.1. Reversible OPEN-CLOSED (or OPEN-SECURED) signs should be used on all classified security containers each time they are locked or unlocked as a visual reminder.

9.15. SECURITY CONTAINERS TAKEN OUT OF SERVICE.

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

- 9.15.1. Security containers no longer used for the storage of classified information may be transferred to other areas where they are needed or stored as surplus. Prior to removing any container, the container shall be thoroughly searched to ensure all classified information has been removed. Areas to be searched include: between, behind and beneath the container and behind, under, and on the sides of all drawers. The person who conducts the search must declare the container empty by placing a written statement on the outside front of the container indicating the date of the inspection, the person who conducted the inspection, and the office that last used the container. In addition, prior to removing any security container with a built-in combination dial, the combination shall be reset to the standard combination of 50-25-50. The written statement on the outside of the container shall identify that the combination has been reset. The security contact must remove and destroy Part 1 of the SF-700 located inside the control drawer. No security container shall be relocated or taken out of service without first notifying the Office of Internal Affairs (IA) and/or the DSO.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

10. CHAPTER 10: TRANSMISSION AND TRANSPORTATION

10.1. POLICY

- 10.1.1. Classified information shall be transmitted and received pursuant to the standards cited in this handbook and in a manner that ensures tampering can be detected, inadvertent access is precluded, and timely delivery to the intended recipient is assured. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized to receive the information, aware of the transmission, and have the capability to properly safeguard it. Under no circumstances will classified information be transmitted by any means other than the approved methods described in this handbook.
- 10.1.2. Requests to waive requirements cited in this handbook will be submitted in writing through the Office of Internal Affairs to the DHS Chief Security Officer. Waiver requests must include sufficient justification to support the request and identify compensatory measures that will be implemented to mitigate deficiencies.

10.2. METHODS OF TRANSMISSION OR TRANSPORTATION.

- 10.2.1. Top Secret information shall be transmitted by:
- Direct contact between appropriately cleared persons.
 - Secure telephone equipment (STE) or Secure Fax keyed to the Top Secret level.
 - Defense Courier Service (DCS) or other authorized government agency courier service.
 - Department of State Courier System (also known as a diplomatic pouch).
 - Electronic means over NSA-approved cryptographic communications system(s).
- 10.2.2. Secret and Confidential information shall be transmitted by any of the following means:
- Any of the methods approved for transmitting Top Secret.
 - U.S. Postal Service Registered Mail.
 - U.S. Postal Service Express Mail. When using U.S. Postal Service Express Mail, the Waiver of Signature and Indemnity block (Item 11-B), on the U.S. Postal Service Express Mail Label shall not be executed. Additionally, street-side collection boxes shall not be used.
 - Commercial carriers or cleared commercial messenger services cleared for such purpose under the National Industrial Security Program (NISPOM).
 - On an exceptional basis and when an urgent requirement exists for overnight delivery within the U.S. and its territories, the current holders of

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

the General Services Administration (GSA) contract for overnight delivery of information for the Executive Branch may be used. The list of current holders of the GSA contract will be updated and published periodically by DHS Office of Security. Use of these services is under exceptional circumstances only and shall not be used for routine transmission of classified information. When using these services, the following conditions apply:

- o Classified Communications Security (COMSEC) Information/ Equipment, North Atlantic Treaty Organization (NATO), and Foreign Government Information shall not be transmitted in this manner.
- o The use of street-side collection boxes is prohibited.
- o Carrier personnel shall not be notified that the package contains classified information.
- o Material shall be packaged for transmission as cited in this handbook.
- o The outer address label may contain the personal name of the intended recipient.
- o The release signature block on the receipt label shall not be executed.
- o The sender is responsible for verifying the proper mailing address and ensuring that an authorized person will be available to accept delivery.
- o Packages should be shipped only on Monday through Thursday and not on the eve of a federal holiday unless prior arrangements have been made to ensure a cleared person will be available to accept delivery.

10.2.3. Under no circumstances will Top Secret information be transmitted via the U.S. Postal Service or any other uncleared commercial delivery service. When it is necessary to transmit Top Secret material, the Top Secret Control Officer (TSCO) shall ensure that the methods and procedures used comply with the requirements of this handbook. Questions concerning the transmission of Top Secret information, which are not covered in this handbook, shall be referred to the Special Security Officer (SSO) for the National Capital Region. For CBP offices located outside the NCR, contact the Office of Internal Affairs or designated security liaisons.

10.2.4. Transmitting classified information to a U.S. Government facility located outside of the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, Commonwealth of the Northern Mariana Islands, Guam, and any other territory or possession of the United States, shall be by methods commensurate with the level of classified information being transmitted. U.S. Registered Mail through Military Postal Service facilities may be used to transmit Secret and Confidential information provided that the information does not at any time pass out of the control of a U.S. citizen and does not pass through a foreign postal system.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- 10.2.5. Transmission of classified information to foreign governments will be approved in accordance with CBP and DHS foreign disclosure policies and procedures.

10.3. SHIPMENT OF FREIGHT

- 10.3.1. Transmitting bulk classified material will be performed by qualified, cleared carriers that are authorized to transport material via a Protective Security Service (PSS) under the Department of Defense Industrial Security Program. This may be done only within the United States when the size, bulk weight, and nature of the shipment make other methods impractical.
- 10.3.2. Observation is not required while the shipment is stored in an aircraft or ship in connection with air or sea transport provided the shipment is in a compartment that is not accessible to unauthorized persons or is loaded in specialized shipping containers, including closed cargo containers. The container or compartment must be sealed to prevent access without detection.
- 10.3.3. Cleared operators, officers of ships or pilots of aircraft who are U.S. citizens may be designated as escorts if control and surveillance of the cargo is maintained 24 hours a day. The escort shall protect the shipment at all times through personal observation, placing the shipment in protected storage or other measures designed to prevent inspection, tampering, pilferage or unauthorized access.
- 10.3.4. All additional control notices imposed by an Original Classification Authority must be honored when transmitting & transporting classified national security information.

10.4. PREPARATION OF MATERIAL FOR TRANSMISSION.

- 10.4.1. Envelopes or Containers. All classified information physically transmitted outside CBP facilities shall be enclosed in two layers, both of which conceal the contents, prevent inadvertent opening, and would provide reasonable evidence of tampering. When envelopes are used, they shall be sealed with reinforced tape.
- The inner enclosure shall clearly identify the name of the intended recipient, the address of both the sender and the recipient, the highest classification level of the contents, and any appropriate warning notices.
 - The outer enclosure shall clearly identify the office of the recipient (personal names shall not be used), and the address of both the sender and the recipient. There will be no markings on the outside envelope to indicate that the contents are classified. Intended recipients shall be identified by name only on the inner envelope. The following exceptions apply:
 - If the classified information is an internal component of a packable item

of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information;

- o If the classified information is an item of equipment that is not reasonably packable and the shell or body is classified, it shall be concealed with an opaque enclosure that will hide all classified features;
- o Specialized shipping containers, including closed cargo transporters or diplomatic pouch, may be considered the outer enclosure when used; and
- o When classified information is hand-carried outside a facility, a locked briefcase or similar locking container may serve as the outer enclosure.

10.4.2. The Office of Internal Affairs may approve the use of specialized shipping containers that are secured with high security padlocks and equipped with an electronic seal that would provide evidence of surreptitious entry is of sufficient construction to provide evidence of forced entry, and are handled by the carrier to ensure that the container is protected until its delivery is completed.

10.5. ESCORT OR HAND-CARRYING OF CLASSIFIED MATERIAL.

10.5.1. Courier authorizations shall be issued to individuals who must hand-carry classified information outside of, and beyond the perimeter of a building or compound, and will be processed through and approved by the Office of Internal Affairs. Requests for courier authorization will be submitted to the Office of Internal Affairs, Security Management Division on DHS Form 11000-2, Courier Authorization Request. The individual's security clearance level must be equal to or exceed the level of material being carried. Designated couriers are required to review the DHS Guidance for Classified Couriers briefing pamphlet and must sign and return an acknowledgement receipt.

- A one-time courier letter shall be issued when the designated courier is required to hand-carry classified information on an infrequent basis within the local commuting area. Such letters shall have an expiration date not to exceed 30 days from the date of issue.
- A permanent courier card shall be issued when the designated courier is required to frequently and routinely handcarry classified information within the local commuting area. Such cards shall have an expiration date not to exceed two (2) years from the date of issue. The DHS Form 11000-01, Classified National Security Information Courier Card, may be used for this purpose.

10.6. COURIER TRAVEL BY COMMERCIAL AIR

10.6.1. Transporting classified material aboard commercial aircraft is discouraged, but will only be approved by the Office of Internal Affairs, in instances of great urgency, and only when the material cannot be transmitted by other means.

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

- 10.6.2. The request, with justification, will be submitted to the Office of Internal Affairs using the DHS Form 11000-2. The justification section will clearly state that the courier will be transporting classified information via commercial air.
- 10.6.3. If information technology equipment, e.g., a laptop computer, computer media, etc., containing classified information is to be transported, it must be encrypted prior to transport. Refer to DHS National Security Systems Handbook for additional information.
- 10.6.4. The CBP Office of Internal Affairs will approve or disapprove the request based on the justification provided.
- 10.6.5. If approved, a courier authorization letter (see sample at Attachment D) shall be prepared and issued by the CBP Office of Internal Affairs.

10.7. TRANSPORT OF CLASSIFIED MATERIAL WITHIN AN ACTIVITY OR OFFICE

- 10.7.1. If required to transport classified material from one building to another via a public street or road, courier authorization is required, and the material shall be packaged in accordance with the requirements of this directive.
- 10.7.2. If required to transport classified material within the same building or compound, an appropriate cover sheet (SF 703, Top Secret; SF 704, Secret; and SF 705, Confidential) shall be affixed to the document and the document shall be placed in an unmarked envelope or folder to avoid undue attention. Courier authorization is not required.

10.8. RECEIPTS.

- 10.8.1. Receipts for Top Secret, Secret, and Confidential materials transmitted or transferred outside of CBP are required. DHS Form 11000-11, Document Record of Transmittal or a similar transmittal form may be used for this purpose.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

11. CHAPTER 11: SECURITY VIOLATIONS AND INFRACTIONS

11.1. POLICY

11.1.1. Programs and safeguards established for the identification and protection of classified information are necessary to assure U.S. National Security. Incidents involving the mishandling of classified information must be promptly and thoroughly investigated to determine the cause, assess and mitigate potential damage, and implement measures to prevent recurrence.

11.2. DEFINITIONS

11.2.1. Security Infraction: Any knowing, willful, or negligent action contrary to the requirements of Executive Order 12958, as amended, and its implementing directives, that does not rise to the level of a Security Violation. A Security Infraction is usually a minor incident or administrative error in the safeguarding of classified information that does not result in the compromise of such information or in which the likelihood of such compromise is remote.

11.2.2. Security Violation: Any knowing, willful or negligent action: (1) that could reasonably be expected to result in an unauthorized disclosure of classified information; (2) to classify or continue the classification of information contrary to the requirements of Executive Order 12958, as amended, and its implementing directives; and/or (3) to create or continue a special access program contrary to the requirements of Executive Order 12958, as amended.

11.3. REPORTING SECURITY INCIDENTS

11.3.1. Security incidents shall be reported promptly, but no later than the next business day from the time of discovery. All security incidents involving the mishandling of collateral classified must be recorded on the DHS Form 11000-10 "Record of Security Violation" and reported to the Office of Internal Affairs, Joint Intake Center. Depending on the incident, a preliminary inquiry or formal investigation will be conducted by the Office of Internal Affairs. This includes incidents where CBP employees knowingly, willfully or by negligent action could reasonably expect that an unauthorized disclosure of classified information may have occurred. Examples of reportable security incidents include:

- Any knowing, willful or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information.
- Any knowing, willful or negligent action to classify or continue the classification of information contrary to the requirements of E.O. 12958, as amended, and its implementing directives.
- Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of E. O. 12958, as amended.
- Any incident involving computer, telecommunications equipment or media

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

that may result in disclosure of classified information to unauthorized individuals. Or an incident that will result in unauthorized modification, destruction of classified system data, the loss of classified computer system processing capability or loss/theft of classified computer system media.

- Any incident involving the processing of classified information on computer equipment that has not been specifically approved and accredited for that purpose by an authorized official.
- Any incident involving the transmission/transportation of classified information by an unapproved method. Or any evidence of tampering with a shipment, delivery or mailing of packages containing classified information.
- Any incident in which classified information is not stored by an approved means.
- Any incident in which classified information is inadvertently revealed to or released to a person that is not authorized access.
- Any incident in which classified information has been destroyed by unauthorized means.
- Any incident in which classified information has been reproduced without authorization or contrary to specific restrictions imposed by the originator or on equipment that has not been specifically approved and accredited for that purpose.
- Any other incident in which classified information is not safeguarded or handled in accordance with prescribed procedures.

11.3.2. Refer to Section 11.4 for security incidents involving classified spillages. Refer to Section 11.5 for incidents involving Sensitive Compartmented Information (SCI) and incidents within a Sensitive Compartmented Information Facility (SCIF).

11.4. CLASSIFIED SPILLAGE

11.4.1. Classified spillage is the accidental, inadvertent or intentional introduction of classified information into unclassified information technology (IT) systems not specifically certified and accredited for classified use, or certified and accredited at a level lower than that of the classified information introduced into it. Any IT incident could pose a significant, negative impact to the confidentiality, integrity, and availability of CBP IT systems.

11.4.2. Reporting a Classified Spillage. Classified spillages must be reported immediately to a supervisor and the CBP Computer Security Incident Response Center (CSIRC) in accordance with OIT HB 1400-05C.

11.4.3. Users must take no action to delete, disturb or further disclose spilled information, such as deleting an email that contains classified information or a

classified attachment or printing hard copies off of a printer.

- 11.4.4. Specific information regarding a spill shall itself be classified at the same level of the classification of the information spilled until confirmation is received that the spilled information has been effectively eradicated from the IT system or the potential for compromise has been otherwise neutralized. Specific information means information sufficient to allow a dedicated intruder or curiosity seeker to search for and access the spilled material.
- 11.4.5. The CSIRC is responsible for forwarding incident reports to the Office of Internal Affairs, Joint Intake Center for preliminary inquiry or investigation.

11.5. INCIDENTS INVOLVING SENSITIVE COMPARTMENT INFORMATION (SCI)

- 11.5.1. Incidents involving SCI, Special Access Program (SAP) information and all other incidents within a SCIF shall be reported to the Office of Intelligence and Operations Coordination (OIOC), Special Security Officer (SSO).

11.6. PRELIMINARY INQUIRY

- 11.6.1. Upon notification of an alleged security incident, the CBP Office of Internal Affairs and/or DSO shall initiate a preliminary inquiry. The person conducting the preliminary inquiry shall serve as the Inquiry Official. The Inquiry Official shall have the authority to conduct interviews and obtain statements from personnel knowledgeable about the incident. Personnel involved in the inquiry process are required to cooperate with Inquiry Officials. Failure to cooperate can result in sanctions as defined in the U.S. Customs and Border Protection, Table of Offenses and Penalties.
- 11.6.2. A preliminary inquiry and corresponding Report of Inquiry (ROI) shall be completed within 30 work days from date of initiation. Where an inquiry cannot be completed within 30 work days, the Inquiry Official shall include a statement in the Report of Inquiry justifying the delay.
- 11.6.3. A preliminary inquiry shall be conducted to determine:
- Whether a security violation or infraction did or did not occur;
 - Time, date, and location of the alleged incident;
 - Whether there was an actual compromise or suspected compromise of classified information;
 - Identification of the classified information involved;
 - The person(s) responsible for and involved in the security violation or infraction;
 - The cause of the security violation or infraction.;
 - The actions taken to minimize damage or neutralize the potential for compromise;

FOR OFFICIAL USE ONLY

[BACK](#)

[RETURN TO TABLE OF CONTENTS](#)

- Recommendations to prevent recurrence of similar security incidents, to include additional training, procedural changes and/or administrative or disciplinary action;
- 11.6.4. If the security incident involves the improper transmission of classified information to CBP from an outside agency, the Inquiry Official shall notify the security official of the sending office or agency who shall pursue the matter further in accordance with the sending agency's regulations. For classified spillage incidents, the CBP CSIRC will conduct damage control of the affected CBP automated systems to remove any trace of the classified information.
- 11.6.5. If the security incident involves the improper transmission of classified information to CBP from another DHS component, CBP shall notify the appropriate security official of the sending Component or office who shall pursue the matter further.
- 11.6.6. If the preliminary inquiry reveals an actual compromise or a suspected compromise of classified information, the Inquiry Official shall request that the OCA with jurisdiction over the information conduct a damage assessment.
- 11.6.7. If CRP originated classification information was originated by a CBP, OCA is compromised, the preliminary inquiry report and request for damage assessment will be forwarded to the Office of Internal Affairs Assistant Commissioner for processing (see MD 11049 for DHS components).
- 11.6.8. If another government agency's information is compromised a copy of the preliminary inquiry report and request for damage assessment will be forwarded to the applicable government agency. A copy of the preliminary inquiry report and request for damage assessment will be forwarded to the Office of Internal Affairs.
- 11.6.9. If the originator of the information cannot be determined, the preliminary inquiry report will be forwarded to the DHS Office of Security/Administrative Security Division (OS/ASD). OS/ASD will attempt to determine the originator of the information and process the damage assessment request. If OS/ASD cannot determine the originator, OS/ASD shall seek guidance from the Information Security Oversight Office (ISOO).
- 11.6.10. If the incident involves the inadvertent disclosure of classified information to a person not authorized access, then the person who received the information will be asked to sign an Inadvertent Disclosure Statement. If the person refuses to sign the Inadvertent Disclosure Statement, the information on the form will be read orally to the person, in the presence of a witness, and the form will be annotated to reflect the individual's refusal to sign; both the Inquiry Official and the witness will sign the form. This information will be included in the preliminary inquiry report.
- 11.6.11. The completed preliminary inquiry report shall be sent from the Office of Internal Affairs, Assistant Commissioner to the Assistant Commissioner's,

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Office Directors and alike with jurisdiction where the security incident occurred and responsibility over the person(s) involved, for further action as appropriate.

- 11.6.12. If the preliminary inquiry report contains classified information, it will be handled and marked accordingly. At a minimum, the preliminary inquiry report will be marked and handled as “For Official Use Only (FOUO).”
- 11.6.13. Persons who are suspected or found to have committed a security incident shall be afforded the opportunity to provide a written statement disputing the facts or identifying mitigating circumstances. Such written statements shall be included as an attachment to the preliminary inquiry report.
- 11.6.14. A copy of the preliminary inquiry report shall be retained by the Office of Internal Affairs. Where a person(s) is suspected or found to have committed a security violation or infraction, a copy of the preliminary inquiry report and all other supporting documentation shall also be included in the individual’s personnel security file.
- 11.6.15. Reports pertaining to contract employees shall be provided to the applicable Contracting Officer’s Technical Representative or equivalent Federal employee having oversight of the contract. In addition, further reporting relative to contractors shall be made in accordance with the National Industrial Security Program (NISP) directives.
- 11.6.16. Preliminary inquiry and/or subsequent inquiry report will be sufficient to close the incident if it determines that:
- The loss or compromise of classified information has not occurred or its likelihood is remote;
 - The compromise of classified information has occurred but there is no indication of knowing, willful, or negligent behavior or significant security weaknesses;
 - There is no evidence of employee misconduct, criminal behavior, or espionage;
 - No additional information will be gained by conducting a formal investigation.

11.7. FORMAL INVESTIGATION

- 11.7.1. The decision to conduct a formal investigation in lieu of or subsequent to a preliminary inquiry shall be made by the Assistant Commissioner, Office of Internal Affairs.
- 11.7.2. Upon determination that a formal investigation is appropriate, the Office of Internal Affairs, Investigative Operations Division will conduct the investigation accordingly. Should the DHS Office of Inspector General (OIG), the Federal Bureau of Investigation (FBI) or another agency assume investigative responsibility, CBP will coordinate all further actions with that investigative

agency.

11.7.3. Reports of Investigations may be forwarded to the DHS, Office of Security.

11.8. OVERSEAS SECURITY VIOLATIONS AND INFRACTIONS

11.8.1. Security incidents occurring at overseas locations are under the purview of the Department of State (DOS). If a security incident is observed by CBP personnel at an overseas location, the DOS Regional Security Officer(s), United States Marine Corps (USMC) Security Guard(s) or other designated person(s) shall be notified.

11.8.2. Security incidents occurring at overseas locations involving CBP personnel are reported by DOS using an Optional Form (OF) 117, "Notice of Security Violation" through the DHS Office of Security.

11.8.3. Upon receipt of OF 117, IA/SMD shall forward the notice, with a cover letter, to the INFOSEC Branch for conducting a preliminary inquiry.

11.9. OTHER AGENCY SECURITY VIOLATIONS AND INFRACTIONS

11.9.1. CBP personnel who observe or learn of a security incident committed by a visiting or detailed employee or contractor of another agency shall follow the guidelines provided in Section 11.6 for reporting and conducting a preliminary inquiry or formal investigation.

11.9.2. The Office of Internal Affairs, Assistant Commissioner shall send a memorandum to the security office of the visiting or detailed individual's agency with a description of the incident.

11.10. SANCTIONS

11.10.1. When an individual is found to be responsible for the commission of a security violation or infraction, he/she may be subject to administrative, disciplinary or criminal sanctions as defined in the U.S. Customs and Border Protection Table of Offenses and Penalties. The type of sanctions imposed shall be under the purview and authority of appropriate supervisory/management officials and based on several considerations, including the following:

- Severity of the incident;
- Intent of the person committing the security violation or infraction;
- Extent of training the person(s) has received; and
- Frequency of which the individual has been found responsible in the commission of other such security violations or infractions.

11.10.2. Sanctions may include, but are not limited to, verbal or written counseling, reprimand, suspension without pay, removal, suspension or revocation of security clearance, loss or denial of access to classified information or termination of classification authority or criminal penalties.

11.10.3. These sanctions will be assessed in accordance with established policies and

[RETURN TO TOP](#)

procedures established in the U.S. Customs and Border Protection Table of Offenses and Penalties.

- 11.10.4. Where a proposed sanction associated with the unauthorized disclosure of classified information is in excess of a reprimand, the official imposing the sanction shall first coordinate with the Office of the Chief Counsel (OCC), for legal review, prior to imposing the sanction. Further, where a criminal violation has occurred that will result in a criminal prosecution, the investigating agency shall coordinate with OCC, which shall coordinate with the Department of Justice, as appropriate.

11.11. ANNUAL REPORTING REQUIREMENTS

- 11.11.1. No later than January 15, CBP shall submit to DHS Office of Security a consolidated report reflecting the security violations and infractions that occurred during the preceding calendar year. This report shall consist of the total number of confirmed CBP security violations and infractions; a brief synopsis of the circumstances for each (i.e., improper storage, improper destruction or improper transmission etc); and remedial actions. Incidents involving COMSEC and SCI, which are reported through other channels, and shall not be included in this report. This report will be used to assess trends and determine the need for enhanced and focused education and awareness programs. The Office of Internal Affairs is responsible for providing this report.

12. CHAPTER 12: INDUSTRIAL SECURITY PROGRAM

12.1. CBP'S INDUSTRIAL SECURITY PROGRAM

- 12.1.1. This chapter sets forth the policies and procedures for the Department of Homeland Security, U.S. Customs and Border Protection's (CBP) participation in the National Industrial Security Program (NISP). Established by E. O. 12829 on January 6, 1993, the National Industrial Security Program provides for the protection of classified information as defined by E. O. 12958, as amended and the Atomic Energy Act of 1954.
- 12.1.2. The NISP serves as a single, integrated, cohesive program for the protection of classified information when not in U.S. Government possession. Under the NISP, contractors are mandated to protect all classified information to which they have been given access or custody by the U.S. Government.
- 12.1.3. DHS formalized its use of the industrial security services of the Department of Defense (DoD), as a user agency of the NISP, by Memorandum of Agreement dated August 22, 2003. As a result of the agreement, DoD is authorized to act for and on behalf of DHS in rendering security services for the protection of classified information released to or within industry by DHS. DHS participates in the NISP to ensure that any classified information released to or accessed by industry, in connection with DHS contracts, grants, or related activities, is properly safeguarded in accordance with Executive Order 12958.
- 12.1.4. Participation in the NISP allows DHS to use the Defense Security Service (DSS) to conduct investigations for contractor facilities and personnel security clearances, and to monitor the contractor's compliance with safeguarding requirements. All facility and personnel security clearances granted by DoD will be accepted by DHS to establish eligibility for access to classified information. Contractors granted an interim facility and personnel security clearance, such as an interim TOP SECRET, will only be eligible for access to DHS classified information at the SECRET level. Upon completion by DSS of all investigative requirements, that facility shall be considered eligible for access to classified information, or contract award, at the appropriate level granted by DSS.
- 12.1.5. DSS issues and maintains facility security clearances and personnel security clearances, as required, for DHS contractors. DSS inspects and monitors contractors who require or will require access to classified information. The Defense Industrial Security Clearance Office (DISCO), a field element of DSS, issues personnel security clearances under the authority of the NISP.
- The Chief Security Officer (CSO) as the Senior Agency Official (SAO) will direct and administer DHS' Industrial Security Program.
 - The Chief, Administrative Security Division, under the direction and authority of the CSO/SAO, delegated the authority to administer

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

FOR OFFICIAL USE ONLY

[BACK](#)

[RETURN TO TABLE OF CONTENTS](#)

implementation and management of the Industrial Security Program within CBP to the Assistant Commissioner, Office of Internal Affairs.

- The Assistant Commissioner of the Office of Internal Affairs shall delegate the authority to administer implementation and management of the Industrial Security Program within CBP to the Security Management Division (SMD).
- The Director, Internal Affairs, Security Management Division shall delegate management of the Industrial Security Program within the Information Security Branch and ensure cooperation among relevant CBP offices.
- CBP IA/SMD/Information Security Branch Chief shall:
 - Serve as the CBP official responsible for management, implementation, and oversight of the Industrial Security Program within CBP.
 - Provide assistance and guidance to contracting and program personnel relating to the security requirements of any procurement action involving classified or sensitive information and provide assistance and guidance to committee control officers relating to processing requests for security clearances for members of Federal Advisory Committees and facility security clearances under the NISP.
 - Process requests for verification of facility security clearances for prospective contractors or employers of advisory committee members and process paperwork for facility clearance sponsorship.
 - Assist the program office, Office of Finance, and contracting officer's technical representative (COTR) in the development of security classification guidance.
 - Represent CBP in all NISP matters within DHS, boards, committees, etc.
 - Review and approve the DD Form 254, Contract Security Classification Specification, and provide a completed copy to the Office of Finance, DSS, and DHS Office of Security. The approved form will be returned to the Office of Finance for inclusion in the contract or solicitation. For contracts involving Sensitive Compartmented Information (SCI), IA/SMD will review the DD 254 to ensure the correct information is provided, but the DHS Administrative Security Division will provide oversight and final approval for the DD 254 and contracts.
 - Review amendments, modifications, etc., with security implications where changes affect the security posture of the contract.
 - Provide training to contract officers/specialists, COTRs, and program area representatives, as needed.
 - In regards to visit authorization requests, verify contractors are working on classified contracts.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

FOR OFFICIAL USE ONLY

[BACK](#)

[RETURN TO TABLE OF CONTENTS](#)

- Office of Finance shall:
 - Ensure that all solicitations and contracts under their oversight comply with the policies and procedures identified in this directive, in addition to the requirements of the Federal Acquisition Regulation regarding safeguarding classified information.
 - Review all proposed solicitations to determine whether access to classified information may be required by offerors, or by a contractor prior to and/or during the contract performance.
 - Ensure that the classified acquisition is conducted as required by the NISP or CBP procedures, as appropriate.
 - Inform contractors and subcontractors of the security classifications and requirements assigned to the various documents, materials, tasks, subcontracts, and components of the classified contract.
 - Ensure the statement work or other pertinent documentation contains the appropriate clauses to include, the Security Requirements Clause, 52.204.2, (for classified contracts), the HSAR Clause, 3052.204-71, Contractor Employee Access (for all contracts), and the Suitability Statement.
 - Verify that all performance specifications are identified in the statement of work.
- COTR shall:
 - Monitor the Contractor's compliance with contractual security requirements.
- CBP Program Manager shall:
 - Consider security requirements at the earliest possible stage in the procurement process, to include the conduct of security risk analyses on classified acquisitions.
 - Work with Internal Affairs on generating the DD 254 and properly identifying all security requirements as stated in the Statement of Work.
 - Ensure classification guide is provided to Office of Finance when the requirement is to generate classified information.
 - Issue a DD Form 254 whenever the security requirements change or additional classification guidance is found necessary.
 - Issue a final DD Form 254 if additional disposition instructions are needed for any classified information the contractor may possess which pertains to the departmental contract.
- Office of Internal Affairs, Personnel Security Division (PSD) shall:
 - Verify that all contractors who are required to have security clearances do so.
 - Verify that all contractor visit requests are tied to a classified contract

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

prior to certifying security clearances.

- o Ensure that Internal Affairs/Security Management Division and COTR are notified of negative responses (i.e. contractor does not have a required security clearance) regarding contractor security clearances.
- Office of Information Technology (OIT)
 - o Notify CBP/IA of contractors who are no longer working on a classified contract.

12.1.6. Security Clearances.

- To ensure that classified information entrusted to private industry is properly safeguarded, CBP requires that contractors who will require access to classified information in the completion of their contractual responsibilities, be processed for security clearances in accordance with the requirements stipulated in the NISPOM.
- Individuals employed by a contractor will be cleared through DSS/DISCO. The cleared contractor is required to have a designated facility security officer (FSO) through whom requests for personnel security clearances are submitted to DISCO. The FSO will provide the Office of Internal Affairs, Security Management Division and Office of Finance with an updated status report of security clearance actions required, pending, and approved as required. The FSO is also responsible for submitting visitor authorization requests on all cleared employees. Contractor personnel must have security clearances commensurate with the level of access required for performance under the contract. CBP has no role in the processing or granting of security clearances to industry personnel.
- For consultants who are working on an interagency agreement, the consultant's agency shall provide the consultants' security clearance. The consultant and the component office head will execute a Security Agreement which will include the consultant's responsibilities and any accesses required. A DD 254 is not needed. If the individual will require access to SCI and does not currently have access, a justification from the individual will need to be sent to the Facility Security Officer in the form of a nomination letter. The Facility Security Officer will put together a package and submit it to the CBP Special Security Officer for processing, as well as provide a copy of the Security Agreement to DHS, Office of Security. DHS Office of Security will be provided a copy of the Security Agreement.
- For independent consultants, HR notifies Internal Affairs that they are bringing a consultant on board and sends a copy of the Consultant Agreement to Internal Affairs. Internal Affairs completes the Security Agreement and sends it and the Non-Disclosure agreement to the hiring office for signatures. The signed Security agreement and Non-Disclosure Agreement are kept on file.

12.1.7. Facility Security Clearance.

- Any firm or business under contract with CBP, which requires access to classified information, will require a facility security clearance commensurate with access required. Additionally, any firm or business entity that requires access to classified information to prepare a response to a Request for Proposal, Request for Bid, etc., and/or in performance of a classified Department contract, will require a facility security clearance.
- Firms that do not possess a facility security clearance, or the requisite level of facility security clearance, will be sponsored for a DoD facility security clearance when a determination has been made by the government contracting officer that the contract effort will require access to classified information. Facility security clearance sponsorship requests will be made by the CBP Program office and shall be submitted to Internal Affairs, for processing to DSS. Facility security clearances for sub-contracts shall be sponsored and processed by the prime contractor in accordance with the NISPOM.
- Facility security clearances for sub-contracts shall be sponsored and processed by the prime contract in accordance with the NISPOM.
- DSS will conduct a risk assessment for all contracts that require contractors to store, process, or access CBP information, systems, or property at their facility to:
 - Identify countermeasures.
 - Ensure identified countermeasures are implemented prior to the contractor gaining control of CBP material.
- Physical Security oversight for cleared contractor facilities, those with access to NSI, will be provided by the cognizant DSS office.
- DHS Office of Security will provide oversight in regards to Sensitive Compartmented Information (SCI) and Special Access Programs (SAP).

12.1.8. Contract Security Classification Specification (DD Form 254)

- In order to activate DSS services and obligate the contractor to the provisions of the NISPOM, CBP offices will include in all classified contracts and classified contract solicitations, a DD Form 254. The DD Form 254 is the primary vehicle for relaying contract specific security classification guidance to the contractor and shall, therefore, in Section 13 of the form, identify a published Security Classification Guide applicable to the contract effort, or the classification will be based on existing classified information from which the contractor shall derive and apply classification guidance. Where the source(s) is identified as a security classification guide(s), the contractor shall be provided access to, or a copy of, the applicable guide(s).
- A DD Form 254 is required and will be completed only for contracts that

require access to classified information.

- The Statement of Work or other documentation used to describe the services or supplies that will be provided by the contract will be provided to the Office of Internal Affairs to assist in verifying the DD Form 254.
- The contract, Statement of Work, or other documentation shall contain the FAR Security Clause 52.204.2 which states that a Government contracting officer made a determination that the contract issued will require access to classified information by the contractor or his or her employees in the performance of the contract. In addition, the DHS HSAR Clause 3052.204-70 mandates that contractors requiring unescorted access to government facilities, access to sensitive information, or access to government information technology resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract. This requirement shall be prescribed for all CBP classified contracts, and will be applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other government Contracting Activity Programs that require access to classified information by a contractor. In addition, such documentation shall also identify the classification level, Top Secret, Secret, or Confidential.
- The Office of Internal Affairs will return the approved DD Form 254 to the CBP Office of Finance for inclusion in the contract or solicitation. The Office of Internal Affairs will distribute a copy of the DD Form 254 to DSS and DHS Office of Security. DSS will conduct investigations and issue the personnel security clearance(s) for the contract employees. DSS will provide security oversight functions in coordination with the Contractor's Facility Security Officer, with the exception of "carve out" contracts requiring access to SAPs. DHS, Office of Security, Special Security Programs Division will provide oversight for contracts involving access to SCI and SAP information.
 - In some instances, it may be necessary to include classified information in a DD Form 254. In those cases, the documentation must be protected in a manner approved for classified information, as identified in Chapter 9.5 of this handbook.

12.2. PROCESSING REQUIREMENTS

- 12.2.1. For each classified contract, the contract solicitation must include a statement that the contractor will require access to classified information and/or will generate classified information in the performance of the contract.
- All classified contracts require verification of facility security clearances by Office of Internal Affairs.
 - The contract, statement of work, or other documents will contain a security clause stating that a Government contracting officer made a determination

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

that the contract will require access to classified information by the contractor in the performance of the contract.

- The DD Form 254 is reviewed to ensure that all of the security requirements captured in the Statement of Work are also identified in the DD Form 254.

12.2.2. Classified Visits

- CBP is to accept visit authorization letters only when they are submitted in accordance with, and contain the information as required by, Chapter 6 of the NISPOM.
- All classified visits by contractors require advance notification to the office hosting the visit. Requests must be in writing and can be submitted by mail, facsimile, or teletype, no hand-carried visit requests shall be accepted. CBP has final approval authority for the proposed visit. CBP need not notify a requester that a visit has been approved if sufficient advance notice of the visit was provided. If CBP disapproves a visit, the requester must be promptly notified.
- The number of classified visits shall be held to a minimum. CBP must determine that the visit is necessary and requires access to classified information in order to approve a classified visit.
- Visitors are not to take notes; make records of classified discussions; discuss classified information on non-secure phones; or take photographs in areas where classified information might be recorded, unless given permission by the hosting organization.
- CBP offices are to ensure that access to classified information higher than the level of the visitor's security clearance certified in the visit authorization letter is not granted.
- Classified visit requests will require certification from the Office of Internal Affairs, Personnel Security Division.

12.2.3. International Security Agreement

- International Security Agreements with foreign governments address security controls, protection, and assurance for safeguarding classified information. These agreements establish the "government-to-government" principle, signifying that signatory governments each have legal responsibility over the others' classified information at all times. All agreements will be in accordance with Chapter 10 of the NISPOM.
- DHS Office of Security shall be responsible for the administration and oversight of classified material to be exported (any disclosure or transfer of technical data to a foreign national), the permanent and temporary import of classified information, and compliance by cleared U.S. contractors involved with NATO, foreign governments, or foreign contractors. DHS maintains a record of cleared U.S. contractors involved with foreign

entities and related activities. Any offices and contractors desiring to enter into international agreements will report their intentions to DHS Office of Security. The report shall contain:

- o Name of Country
- o Name and address of government entity issuing contract
- o Contract/RFP number
- o Name of U.S. contractor/name of any subcontractors involved
- o Contract/RFP issue and response date
- Contractors are still required to report their activities to DSS per the NISPOM.

12.2.4. DHS Office of Security shall use this report to issue proper guidance to CBP and contractors to ensure compliance with governing export control laws: the Export Administration Regulation and the Arms Export Control Act, before executing any agreement with a foreign interest that involves access to DHS classified information by a foreign national. Contractors are still required to comply with foreign ownership, control, or influence (FOCI) requirements per the NISPOM. Prior to the execution of such agreements, review and approval are required by the State Department and release of the classified information must be approved by DHS. Failure to comply with Federal licensing requirements may render a contractor ineligible for a facility security clearance.

13. CHAPTER 13: SAFEGUARDING SENSITIVE BUT UNCLASSIFIED (FOR OFFICIAL USE ONLY) INFORMATION

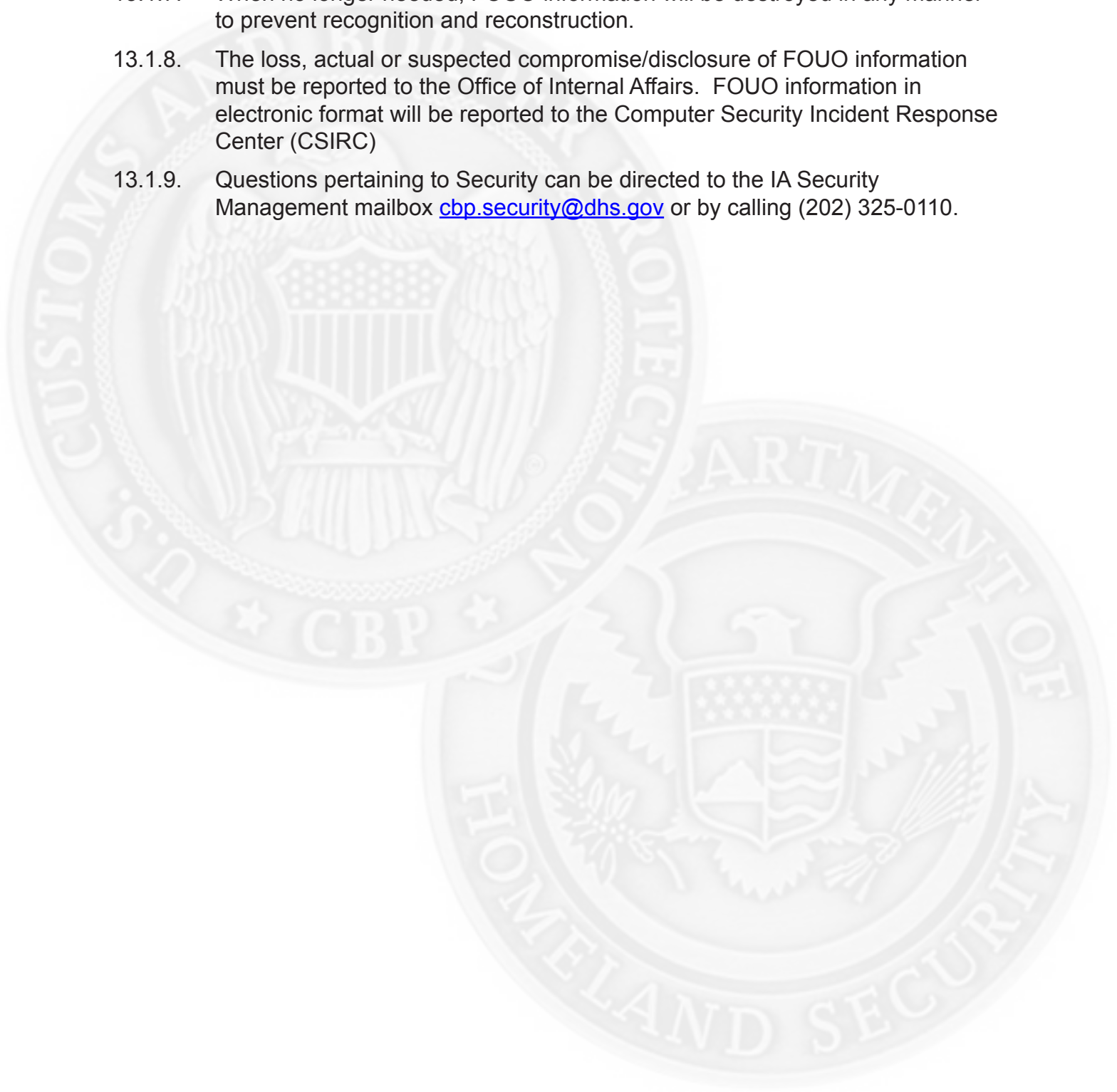
13.1. POLICY

- 13.1.1. FOUO is the designator used within DHS to identify Sensitive but Unclassified information with the DHS community that is not otherwise specifically described and governed by statute or regulation and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. For example, information designated as Protected Critical Infrastructure Information (PCII) and Sensitive Security Information (SSI) are governed by separate guidance issued by the responsible program office. Any DHS employee, detailee, or contractor can designate information as FOUO provided it meets the sensitivity threshold defined in [DHS MD 11042.1](#) (Safeguarding Sensitive But Unclassified (For Official Use Only) Information) and falls within one of the types of information listed in the MD as FOUO. Officials occupying supervisory or managerial position are authorized to designate other information, not listed in the MD and originating under their jurisdiction as FOUO. Access to FOUO information is based on a "need-to-know" as determined by the holder of the information.
- 13.1.2. Other government agencies and international organization may use different terminology to identify sensitive information, such as Limited Official Use (LOU) and Official Use Only (OUO). In most instances, this information is equivalent to FOUO information and should be protected as such.
- 13.1.3. Information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. At a minimum, prominently mark on the bottom of each page "FOR OFFICIAL USE ONLY".
- 13.1.4. FOUO information will be sent by U.S. Postal Service first class mail or an accountable commercial deliver service and may be entered into an inter-office mail system, provided it is afforded sufficient protection to prevent unauthorized access (e.g., sealed in an envelope).
- 13.1.5. FOUO information in electronic form shall:
- not be entered or posted on any public website,
 - not to be sent to personal e-mail accounts,
 - be stored or processed on encrypted thumb or jump drives, and
 - be transmitted over secure communications systems or encrypted if transmitted over unclassified or "open" communications
- 13.1.6. When unattended, FOUO materials will, at a minimum, be stored in a locked file cabinet, locked desk drawer, a locked overhead storage compartment,

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- or similar locked compartment. An FOUO coversheet will be used when removed from storage.
- 13.1.7. When no longer needed, FOUO information will be destroyed in any manner to prevent recognition and reconstruction.
 - 13.1.8. The loss, actual or suspected compromise/disclosure of FOUO information must be reported to the Office of Internal Affairs. FOUO information in electronic format will be reported to the Computer Security Incident Response Center (CSIRC)
 - 13.1.9. Questions pertaining to Security can be directed to the IA Security Management mailbox cbp.security@dhs.gov or by calling (202) 325-0110.



14. CHAPTER 14: SENSITIVE SECURITY INFORMATION (SSI)

14.1. POLICY

14.1.1. As defined in 49 C.F.R. §1520.5, Sensitive Security Information (SSI) is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which DHS, the Transportation Security Agency (TSA), or CBP has determined would (1) constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file); (2) reveal trade secrets or privileged or confidential information obtained from any person; or (3) be detrimental to the security of transportation. In addition, CBP Directive, 1450.021, May 13, 2008 establishes the Customs and Border Protection (CBP) policy regarding the recognition, identification, and safeguarding of Sensitive Security Information (SSI).

14.2. RESPONSIBILITIES

14.2.1. The following entities and CBP Offices have a significant role in the oversight and management of CBP's SSI Program:

- DHS and TSA:
 - DHS has program oversight responsibility for promulgation of Department-wide policy governing the recognition, identification, and safeguarding of SSI. The DHS Chief Security Officer coordinates with the Director of TSA/SSI Office the development of any security classification guide that may identify information that requires protection of SSI. The Assistant Secretary for TSA serves as the authority for implementation, management, and oversight of SSI, pursuant to 49 USC §114(s). The TSA SSI Office assists in the promulgation of regulations and procedural guidance for the implementation and management of SSI, and serves as the approval authority for publication of CBP SSI guidance and procedures, CBP Directive 1450.021. The TSA SSI Office Director also works in coordination with the DHS Office of Security to establish, provide guidance for, and approve processes and programs for the audit, oversight, and inspection of the management and practical application of SSI to include reviews of SSI records for consistent and appropriate application and use of SSI.
- Commissioner for U.S. Customs and Border Protection (CBP) shall:
 - Administer implementation and management of SSI within CBP through written appointment of a Government official to serve as the SSI Program Manager for CBP. The appointed SSI Program Manager, Office of Internal Affairs (IA), Security Management Division (SMD), shall represent CBP on the DHS SSI Oversight Committee. Copies of

[RETURN TO TOP](#)

the appointment record shall be forwarded to the Director of the TSA SSI Office and the DHS Chief Security Officer.

- o Ensure appointment of at least one employee in each office that generates or accesses SSI to serve as SSI Coordinator, and grant each Coordinator authority to make determinations that records generated by CBP are appropriately marked SSI.
- o Ensure that periodic and random reviews are conducted for effective management and practical application, consistent and appropriate application and use of SSI, and notify the DHS Office of Security about these reviews. Such reviews shall assess compliance with regulations, policies, procedures, and guidance governing SSI recognition, identification, and safeguarding. The DHS Office of Security may also conduct SSI reviews within CBP, as it deems appropriate.
- o Where necessary, develop and implement supplemental internal SSI procedures and guidance specific to the management and administration of SSI within CBP. Supplemental procedures and guidance shall be approved by the Director of the TSA SSI Office, in coordination with the DHS Office of Security prior to implementation.
- o Ensure that when a lawful request to publicly release a record containing information determined to be SSI is received, the record is reviewed in a timely manner to determine whether any information contained in the record meets the criteria for continued SSI protection under applicable law and regulation. Portions that no longer require SSI protection shall be released subject to applicable laws and regulations, including §§§§552 and 552a of Title 5, United States Code. Any records containing SSI originating from another DHS Component shall be referred to the appropriate Component for review and response. Any information originally designated as SSI pursuant to 49 C.F.R. §§1520.5(b)(9)(iii) or 1520.5(b)(16) shall be referred to the Assistant Secretary for the Transportation Security Administration.
- The Office of Policy and Planning (OPP) shall:
 - o Serve as the liaison with external audit groups such as the Office of the Inspector General (OIG) and the Government Accounting Office (GAO) to coordinate CBP responses to external audit reports and reviews that contain potential CBP SSI.
- CBP SSI Program Manager shall:
 - o Serve as the CBP official responsible for management, implementation, and oversight of SSI within CBP.
 - o Represent CBP on the DHS SSI Oversight Committee.
 - o Conduct self-inspections of CBP for effective management and practical application of SSI, and consistent and appropriate application and use of SSI. Self-inspections shall be conducted in accordance with

FOR OFFICIAL USE ONLY

[BACK](#)

[RETURN TO TABLE OF CONTENTS](#)

MD 11056.1 or the DHS Security Operating Manual.

- o Ensure appointment of an appropriate number of office-level SSI Coordinators in order to effectively implement and manage SSI within the respective offices.
- o Maintain an up-to-date record of all CBP SSI Coordinators and provide a copy to the Director of the TSA SSI Office on a semi-annual basis.
- o Develop CBP-specific SSI identification and procedural guidance as necessary to implement and manage SSI.
- CBP SSI Coordinator shall:
 - o Facilitate the administration and oversight of SSI within their applicable office.
 - o Assist office personnel in the appropriate use and application of SSI and make determinations that records generated by that office are appropriately marked SSI.
 - o Conduct self-inspections of their respective office for effective management and practical application of SSI and consistent and appropriate application and use of SSI.
 - o Ensure training of office personnel who access and/or generate SSI.
 - o Keep abreast of SSI policies and procedures and maintain liaison with the CBP SSI Program Manager.
- DHS Oversight Committee is:
 - o Chaired by the Director of the TSA SSI Office, with membership consisting of the DHS Chief Security Officer and Component SSI Program Managers.
 - o Used as a forum for the discussion of policies and procedures related to the implementation, management, and oversight of SSI within DHS and an exchange of information related to lessons learned and best practices.
- CBP employees, contractors, consultants, and other CBP Covered Persons (i.e. airport operator, aircraft operator, anyone with a transportation-related responsibility) to whom access to SSI is granted shall:
 - o Be aware of and comply with the recognition, identification, disclosure restrictions, and safeguarding requirements for SSI as outlined in DHS MD 11046.1, 49 CFR §1520 and any other approved implementing regulations, directives, procedures, and guidance.
 - o Be aware that divulging SSI without proper authority could result in enforcement or corrective action.
 - o Participate in training sessions presented to communicate the requirements for recognizing, identifying, and safeguarding SSI.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

14.3. CATEGORIES OF SSI

- 14.3.1. Security Programs including amendments, comments, guidance and Contingency Plans
- Security Directives (SDs) or orders
 - Information Circulars under, and any comments, instructions, or implementing guidance pertaining thereto.
 - Performance specifications, test objects and test procedures
 - Vulnerability assessments directed, created, held, funded, approved by, or provided to DOT or DHS
 - Security inspection or investigation information
 - Threat information against transportation held by Government
 - Security measures: specific details of aviation or maritime security measures
 - Security screening information (aviation or maritime)
 - Security training materials created for aviation or maritime security training purposes
 - Identifying information of certain transportation security personnel
 - Critical aviation or maritime infrastructure asset information
 - Systems security information of IT systems: security procedures, inspections, vulnerability information
 - Confidential business information related to aviation or maritime security
 - Research and development information
 - Other (as determined by TSA)

14.4. ORIGINAL DESIGNATION OF INFORMATION AS SSI

- 14.4.1. The DHS Secretary, the Assistant Secretary for the TSA, and the Director of the TSA SSI Office are authorized, under 49 C.F.R. §1520.5(b)(16), to designate information as SSI, which is not otherwise categorized as SSI under 49 CFR §§1520.5(b)(1) through (15).
- This designation authority also includes a determination to protect detailed information about screening locations in accordance with 49 C.F.R. §1520.5(b)(9)(iii). No other officials shall have the authority to designate information as SSI that is not otherwise covered under 49 CFR §§1520.5(b)(1) through (15).
- 14.4.2. If information is identified or developed that would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information obtained from any person, or be detrimental to the security of transportation if publicly disclosed, but is not otherwise categorized as SSI under 49 C.F.R. §§1520.5(b)(1) through (15), it shall be transmitted through

the CBP SSI Program Manager, IA/SMD to the Director of the TSA SSI Office, for review and determination as to whether or not the information warrants protection as SSI. Such information shall be marked and protected as SSI on an interim basis in accordance with policies and procedures issued or approved by the TSA SSI Office, pending a final assessment by the Director of the TSA SSI Office.

- 14.4.3. A record shall be maintained of each original SSI designation made. The record shall include the date, title or subject of the document, and a detailed synopsis of the information. A copy of the record and the information to be protected shall be transmitted to the TSA SSI Office within 30 days following designation. Whenever possible, to maintain consistency, such designations should be done in consultation with the TSA SSI Office prior to designation.
- 14.4.4. Information designated as SSI shall be marked in accordance with 49 C.F.R. §1520.13. To the extent practicable, the front page, title page, and/or the first page shall include the notation “Designated SSI Pursuant to 49 C.F.R. §1520.5(b)(16),” or, “Designated SSI Pursuant to 49 C.F.R. §1520.5(b)(9) (iii),” as applicable. Where the official marking is not otherwise evident, the additional notation “Designated by (name and position of authorized official)” shall be added.
- 14.4.5. Once information is properly designated as SSI under 49 C.F.R. §§1520.5(b) (9)(iii) or 1520.5(b)(16), the designation must be communicated to appropriate parties with a need-to-know.

14.5. MARKING SSI

- 14.5.1. A CBP covered person shall mark information as SSI if it meets the criteria for SSI as cited in 49 C.F.R. §1520.5(b) and MD 11056.1. Mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of (1) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover; (2) Any title page; and (3) Each page of the document. In addition, the protective marking “SENSITIVE SECURITY INFORMATION and the following limitation statement will be identified:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR §15 and §1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR §15 and §1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR §15 and §1520.

- 14.5.2. Where there is doubt as to the applicability of an SSI category, the information shall be marked as SSI on an interim basis and submitted to the applicable

office SSI Coordinator or CBP SSI Program Manager for final assessment. If the information is believed to warrant protection as SSI but is not governed by a category of information under 49 C.F.R. §§1520.5(b)(1) through (15), the SSI Program Manager shall refer the information as cited in MD 11056.1, VI.C.3 or the DHS Administrative Security Operating Manual.

14.5.3. Information meeting the SSI criteria shall be marked in accordance with 49 C.F.R. §1520.13. Additionally, the following markings shall be applied:

- Subjects, titles, paragraphs, subparagraphs, charts, graphs, and similar portions (portion markings) need not be portion marked unless (1) the record contains other types of information that requires portion marking, e.g., classified information; or (2) the information is to be transmitted outside of DHS to Congress, or Congressional Committees. All SSI records submitted by DHS to Congress or Congressional Committees must be portion-marked. When used, such portion markings shall be reviewed by the CBP SSI Program Manager prior to dissemination. The parenthetical abbreviation (SSI) shall be used.
- Portion markings will be applied to unclassified portions of a record within a classified record that contain SSI. The parenthetical abbreviation (SSI) shall be used.

14.6. DURATION OF SSI AND SSI REVIEWS

14.6.1. Information designated or appropriately marked as SSI will remain SSI unless determined releasable by the Assistant Secretary for the Transportation Security Administration, the Commandant of the United States Coast Guard (USCG), the Director of the TSA SSI Office, or other authorized officials, in accordance with policies and procedures issued or approved by the TSA SSI Office.

14.6.2. SSI information that is over three years old or older will be subject to release upon request, unless the DHS Office of Security, TSA SSI Office, or CBP SSI Program Manager determines that one of the following conditions applies:

- The information is incorporated in a current transportation security directive, security plan, contingency plan, or information circular.
- The information contains current information in one of the following SSI categories: equipment or personnel performance specifications; vulnerability assessments; security inspection or investigative information; threat information; security measures; security screening information; security training materials; identifying information or designated transportation security personnel; critical aviation or maritime infrastructure asset information; systems security information; confidential business information; or research and development information
- The information is otherwise exempt from disclosure under applicable law, i.e. the Privacy Act

- If the SSI does not fall under a category cited in MD 11056.1 or the DHS Administrative Security Operating Manual, then the request for release may only be denied in whole or in part, if the Secretary or the Assistant Secretary for the Transportation Security Administration, makes a written determination that identifies a rational reason why the information must remain SSI. Such written determination shall be provided to the party that made the request within twenty (20) business days after the determination has been made. Additionally, each written determination shall be provided to the Committees on Appropriations of the Senate and House of Representatives as part of the annual reporting requirement.

- 14.6.3. Pursuant to 49 C.F.R. §1520.5(c), the Director of the TSA SSI office shall coordinate with the USCG and the DHS SSI Oversight Committee to develop and implement policy and procedures relating to the loss of an SSI designation from information that no longer meets the criteria set forth in 49 C.F.R. §1520.5(a).
- 14.6.4. In accordance with 49 C.F.R. §1520.15(a) and (b), the CBP SSI Program Manager or other authorized CBP offices may review and redact SSI records upon requests for public release under the Freedom of Information Act (FOIA) in accordance with policies and procedures issued or approved by the Director of the TSA SSI office and Chapter 14.10, CBP SSI FOIA Review Process in this handbook.
- 14.6.5. CBP offices may also redact SSI records in response to other requests, in accordance with MD 11056.1 or the DHS Administrative Security Operating Manual, and policies and procedures issued or approved by the Director of the TSA SSI office.

14.7. CHALLENGING SSI

- 14.7.1. Any authorized holder of SSI who believes the information has been improperly or erroneously marked as SSI is encouraged to challenge the marking. Such challenges may be done either formally or informally.
- 14.7.2. Informal challenges may be made directly by the holder of the information to the person that applied the SSI marking who shall reevaluate the marking against the criteria cited in 49 C.F.R. §1520.5(b)(1) through (15) and implementing guidance published or approved by the Director of the TSA SSI Office.
- 14.7.3. A formal challenge may be submitted in writing to the person that applied the SSI marking through the applicable office SSI Coordinator and the CBP SSI Program Manager, IA/SMD to the TSA SSI Office, or the DHS Office of Security. An appeal of the decision made by the recipient of the challenge may be filed with the Director of the TSA SSI Office. A further appeal of the decision made by the Director of the TSA SSI Office may be made to the Assistant Secretary for TSA. The decision of the Assistant Secretary for the

TSA shall be final.

- 14.7.4. Individuals submitting a challenge shall not be subject to retribution for bringing such actions. Anonymity may be requested from any of the reviewers listed above, and the reviewers shall honor a challenger's request for anonymity and fully consider and appropriately process the challenge.

14.8. AUDITS AND INSPECTIONS

- 14.8.1. Nothing in this policy shall diminish the authority of the Office of Inspector General to conduct audits, inspections, or investigations, in accordance with the Inspector General Act of 1978, as amended, 5 USC App. 3, and DHS Management Directive 0810.1 or DHS Administrative Security Operating Manual.
- 14.8.2. The DHS Office of Security may conduct periodic oversight and compliance reviews of SSI within DHS, as it deems appropriate.
- 14.8.3. The Director of the TSA SSI office shall develop, issue, and approve policies, procedures, and guidance for the implementation and management of self-inspection CBP programs that access or generate SSI. The TSA SSI Office shall create, publish and approve appropriate guidance and checklists to facilitate the conduct of self-inspections by SSI Program Managers and SSI Coordinators. The DHS Office of Security shall also provide a means to monitor and track self-inspection program implementation.
- 14.8.4. The CBP SSI Program Manager, IA/SMD, shall conduct a self-inspection of the program at least once every eighteen (18) months. The results of self-inspections conducted pursuant to MD 11056.1 or the DHS Administrative Security Operating Manual shall be reported to the TSA SSI Office within thirty (30) days after completion. Discrepancies cited during the self-inspection shall be reconciled in a timely manner, and the SSI Program Manager, IA/SMD or the TSA SSI Office will take remedial action as needed.
- 14.8.5. SSI Coordinators shall conduct a self-inspection of their applicable office SSI program at least once every 12 months. The results of self-inspections conducted shall be reported to the CBP SSI Program Manager, IA/SMD within 30 days after completion. Discrepancies cited during the self-inspection shall be reconciled in a timely manner, and the SSI Coordinator or the SSI Program Manager will take remedial action as needed.
- 14.8.6. Self-inspections shall assess compliance with regulations, policies, procedures, and guidance governing SSI recognition, identification, and safeguarding.

14.9. SHARING, DISSEMINATION AND ACCESS

- 14.9.1. SSI shall not be disseminated in any manner (orally, electronically, visually, or in any other manner) to unauthorized personnel. The Assistant Secretary for TSA may determine in writing that information which might otherwise be

considered SSI may be released publicly in the interest of public safety or in furtherance of transportation security under 49 C.F.R. §1520.5(b). Under 49 C.F.R. §1520.15(e), the Assistant Secretary for TSA, and under 49 C.F.R. §1520.9(a)(2), the Assistant Secretary for TSA and the Commandant of the USCG, may also determine in writing that specific SSI may be released to non-covered persons (e.g., individuals not within the definition provided at 49 C.F.R. §1520.7), in accordance with policies and procedures issued or approved by the TSA SSI Office.

14.9.2. In addition to other requirements cited previously and in 49 C.F.R. §1520, access to SSI is based on a need-to-know as determined by the holder of the information. Where there is uncertainty as to a person's need-to-know, the holder of the information will request dissemination instructions from his or her next-level supervisor or the originator of the information. Need-to-know is determined in accordance with 49 C.F.R. §1520.11 and procedures issued or approved by the TSA SSI Office. Under 49 C.F.R. §1520.11(a), a DHS covered person has a need-to-know specific SSI in the following circumstances:

- When the person requires access to specific SSI to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT;
- When the person is in training to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT;
- When the information is necessary for the person to supervise or otherwise manage individuals carrying out transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT;
- When the person needs the information to provide technical or legal advise to a covered person regarding transportation security requirements of Federal law; or
- When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements.
- Pursuant to 49 C.F.R. §1520.11(b), a Federal employee has a need-to-know SSI if access to the information is necessary for performance of the employee's official duties, on behalf or in defense of the interests of the Federal, State, local or tribal government, or a person acting in the performance of a contract or grant from DHS or DOT has a need-to-know SSI if access to the information is necessary to performance of the contract or grant.
- Pursuant to 49 C.F.R. §1520.11(d), for some specific SSI, DHS may make a finding that only specific persons or classes of persons, whose official duties, on behalf or in defense of the interests of the Federal, State, local

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

or tribal government, have a need-to-know, in accordance with procedures issued or approved by the Director of the TSA SSI Office.

- 14.9.3. A security clearance is not required for access to SSI. However, in accordance with 49 C.F.R. §1520.11(c), TSA or USCG may make an individual's access to SSI contingent upon satisfactory completion of a security background check or other procedures and requirements for safeguarding SSI. The TSA SSI Office must approve any SSI background check or processing requirements or procedures developed by the USCG or CBP.
- 14.9.4. SSI shall be shared with other agencies, state, tribal, or local governments and law enforcement officials, provided a need-to-know has been established in accordance with 49 C.F.R. §1520.11, and the information is shared in support of transportation security or in the furtherance of a coordinated and official governmental activity.
- 14.9.5. In accordance with 49 C.F.R. §§1520.11(b)(1) and 1520.15(c), SSI shall be shared with Congress, Congressional Committees, the Comptroller General (Government Accountability Office), the Office of Inspector General, and other similar entities acting within their official governmental capacities.

14.10. STORAGE AND HANDLING

- 14.10.1. When unattended, SSI will, at a minimum, be stored in a locked container or in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an authorized area where access is controlled by a guard, cipher lock, or card reader. Additional guidance can be obtained through the CBP Program Manager, IA/SMD or the TSA SSI Office.
- 14.10.2. Information Technology (IT) systems that store SSI will be certified and accredited for operation in accordance with Federal and DHS standards. Consult the DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A, or additional guidance published by the TSA SSI Office for more detailed information.
- 14.10.3. When removed from an authorized storage location and persons without a need-to-know are present, or where casual observation would reveal SSI to unauthorized persons, measures such as an unmarked folder, envelope, or SSI cover sheet shall be used to prevent unauthorized or inadvertent disclosure.

14.11. CBP SSI FOIA REVIEW PROCESS

- 14.11.1. All Freedom of Information Act (FOIA) requests submitted to the CBP FOIA Office must be reviewed for the presence of SSI. If the FOIA Office determines that a record responsive to a FOIA request may contain SSI, it will

be forwarded to the SSI Program Manager, IA/SMD for a full review.

14.11.2. Procedures

- Any person who receives a FOIA request must submit it to the CBP FOIA Office for processing.
- The FOIA Office will process the request by gathering records and preparing an appropriate response while maintaining an awareness of what constitutes SSI.
- The FOIA Office will identify SSI in all records it receives and the response it prepares.
- If the FOIA Office determines that any records it reviews contain SSI, those records will be forwarded to the SSI Program Manager, IA/SMD for review and determination.
- The SSI Program Manager will identify all SSI material in records it receives from the FOIA Office and prepare a visibly redacted version of the record, removing SSI material.
- The visibly redacted version of the record will be returned to the FOIA Office for further processing.

14.11.3. Information designated as SSI qualifies for exemption from disclosure under the FOIA.

14.11.4. If a record contains both SSI and non-SSI material, only the non-SSI material may be disclosed in response to a FOIA request.

14.11.5. If there is disagreement about the existence of SSI material, the issue will be presented to a review committee consisting of a representative from the FOIA Office, the SSI Program Office, and the Office of Chief Counsel. The SSI Program Office will make the final decision.

14.12. TRANSMISSION

14.12.1. When transmitting SSI, the SSI marking must be applied to the transmittal document (letter, memorandum, or fax). The transmittal document must contain, if applicable, a disclaimer noting that it is no longer SSI when it is detached from the SSI material it is transmitting (transmittal e-mails do not need to contain this disclaimer), and a warning that if received by an unintended or different recipient, the sender must be notified immediately.

14.12.2. When discussing or transmitting SSI to another individual(s), CBP Covered Persons must ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid need-to-know. In addition, CBP Covered Persons must ensure that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise accessing the information.

14.12.3. SSI shall be mailed in a manner that offers reasonable protection of the sent

materials and sealed in such a manner as to prevent inadvertent opening and show evidence of tampering.

14.12.4. SSI may be mailed by U.S. Postal Service First Class Mail or an authorized commercial delivery service such as DHL or Federal Express.

14.12.5. SSI may be placed into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.

14.12.6. Electronic Transmission

- Transmittal r-controlled or -sponsored encrypted or otherwise protected portals (applications or data networks), such as the Homeland Security Information Network (HSIN), USCG HomePort, or TSA's WebBoards. Such posting shall be in accordance with guidance published or approved by the TSA SSI Office, CBP Program Manager, IA/SMD and appropriate IT security offices.

14.13. DESTRUCTION

14.13.1. In accordance with 49 CFR. §1520.19, SSI will be destroyed when no longer needed and its continued retention is not otherwise required under the National Archives Records Administration (NARA) records retention laws and regulations. Destruction may be accomplished as follows:

- "Hard Copy" materials will be destroyed by shredding, burning, pulping, or pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.
- Electronic records may be deleted in accordance with policies or procedures issued or approved by the TSA SSI Office and CBP Program Manager, IA/SMD and in accordance with NARA records retention policies. Electronic storage media (compact discs, personal computers, etc.) shall be sanitized appropriately by overwriting or degaussing. Contact the CBP Program Manager, IA/SMD or IT security personnel for additional guidance.
- Paper products containing SSI will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

14.14. INCIDENT REPORTING

14.14.1. The loss, compromise, suspected compromise, or unauthorized disclosure of SSI must be reported to the CBP SSI Program Manager, IA/SMD to the DHS Office of Security or the TSA SSI Office. Incidents involving SSI in DHS IT systems will be reported to the CBP Computer Security Incident Response Center in accordance with IT incident reporting requirements. The TSA SSI Office shall, in coordination with the DHS SSI Oversight Committee, develop, publish or approve procedures for reporting, mitigating, and investigating

incidents involving the improper handling, suspicious or inappropriate requests for, or unauthorized disclosure of SSI.

- 14.14.2. CBP shall have its own delegated authority, pursuant with DHS Delegation 8100.3, to pursue enforcement action of violations of the SSI regulation in accordance with 49 CFR §1520.17, other applicable statutes and regulations, and procedures issued or approved by the TSA SSI Office.

14.15. PROGRAM STATUS REPORTING

- 14.15.1. No later than January of each year the CBP SSI Program Manager shall report, through the TSA SSI Office to the DHS Office of Security, the total number of SSI records that were generated as SSI in their entirety for the preceding calendar year. SSI in their entirety means any record, the entire content of which the creator of the record believes to be SSI. Any record that the creator of the record believes contains a combination of SSI and information that is not SSI is not considered SSI in its entirety and therefore not reportable. DHS Office of Security shall compile this information into a single report for submission to the House and Senate Committees on Homeland Security no later than January 31 of each calendar year.

15. CHAPTER 15: SECURITY EDUCATION AND AWARENESS

15.1. POLICY

15.1.1. A security program is most effective when employees practice security daily. The Office of Internal Affairs, Security Management Division is responsible for the Security Education and Awareness as it pertains to Administrative Security i.e. safeguarding of classified and sensitive but unclassified information, Physical Security, Counterintelligence and OPSEC. Refer to [Chapter 17](#) for specified security training descriptions and method of delivery.

15.2. RESPONSIBILITIES

15.2.1. The Director, Security Management Division has overall responsibility for CBP's Administrative Security Education and Awareness training as defined in [Chapter 17](#) and ensures CBP personnel who have not fulfilled the required training requirements are restricted from unescorted access to CBP areas and/or from access to classified information until the requirements are met.

15.3. SECURITY TRAINING

15.3.1. Security training will encompass the fundamentals of how to properly safeguard classified and sensitive but unclassified information. The overall intent of training is to provide CBP personnel with the basic knowledge required to work effectively with critical information to:

- Ensure that each employee who creates, processes, or handles classified information has a satisfactory knowledge and understanding of classification, safeguarding, and declassification policies, procedures, and practices;
- Increase uniformity among personnel when handling classified and sensitive but unclassified information;
- Reduce improper classification, safeguarding, transmission, and disclosing incidents; and
- Foster motivation to attend security education and awareness training activities.

15.3.2. Training methods may include on-site briefings provided by the Office of Internal Affairs (IA), security liaison and/or web base delivery.

15.3.3. Security Orientation Training:

- All CBP employees, detailed personnel, and contractors are required to attend Security Orientation Training within the first 30 days of assignment. This training covers the basics on protection, reporting emergencies, theft, misconduct and protection of information.

15.3.4. Initial Security Training "Safeguarding Classified National Security

[RETURN TO TOP](#)

Information.”

- As defined in Executive Order 12958, as amended, all CBP personnel who have undergone a complete favorable background investigation for access to classified and require a security clearance as defined in [Chapter 7.1](#) are required to have Initial Security Training on the proper safeguarding of classified information prior to being granted a final security clearance. Individuals shall receive a comprehensive briefing to inform them of their safeguard and security responsibilities for the protection of Classified National Security Information and penalties associated with the mishandling of this information. At this time personnel will also be required to execute the Standard Form (SF) 312, Classified Information Nondisclosure Agreement, and the Department of Homeland Security, Customs and Border Protection Reporting Foreign Contacts Form. The Office of Internal Affairs, Personnel Security Division is responsible for providing this training.

15.3.5. Refresher Security Training “Safeguarding Classified National Security Information.”

- All CBP personnel who have been granted a security clearance are required to undergo annual refresher training on the safeguarding and handling of classified information as defined in Executive Order 12958, as amended. This training is required to ensure the individual’s continued access to classified information.

16. CHAPTER 16: COMPLIANCE REVIEWS AND SELF-INSPECTIONS

16.1. POLICY

- 16.1.1. This handbook is designed to ensure proper and adequate security services to CBP personnel while safeguarding and protecting critical information from unauthorized disclosure such as theft, sabotage or mishandling. Unauthorized disclosure of classified and sensitive but unclassified information threatens our national security. Security compliance, which may consist of self-inspections, security surveys, assessments, assistance visits, compliance reviews and unannounced spot checks are conducted to ensure compliance with laws, Executive Orders, Federal regulations, and CBP policies.
- 16.1.2. This chapter provides an overview of compliance reviews conducted by the Office of Internal Affairs and ongoing standards for the Self-Inspection Program (SIP) as it relates to the safeguarding of classified and sensitive but unclassified information.

16.2. RESPONSIBILITIES

- 16.2.1. The Director, Security Management Division is responsible for ensuring that all CBP offices comply with established security laws, regulations, and policies. Compliance review teams, which conduct compliance surveys, inspections, assessments, and spot checks, carry out this function.

16.3. COMPLIANCE REVIEW PROCEDURES

- 16.3.1. Compliance reviews and frequency of the reviews are based on CBP office program needs and the magnitude of security activity to include the (SIP) results. Compliance review teams will conduct reviews of CBP offices that handle and store classified information biannually.
- 16.3.2. The compliance review team will provide an in-brief prior to the commencing of the review and provide an exit briefing at the conclusion of the review.
- 16.3.3. Compliance reviews are not limited to the protection of critical information and may include physical, personnel and operational security practices. Reviews may include information listed below and information contained in Section 19.4, Self-Inspections:
- A review of internal procedures and processes for the safeguarding of classified and sensitive but unclassified information;
 - Interviews with office personnel;
 - A review of access and control records;
 - A review of safes/security containers; and
 - A review of a sampling of classified and sensitive but unclassified documents processed and/or stored.

BACK

[RETURN TO TABLE OF CONTENTS](#)

- 16.3.4. The compliance review team will prepare a draft report that documents preliminary findings and recommendations. A final report will be provided to the relevant CBP program activity through the appropriate CBP Office head.

16.4. SELF-INSPECTIONS

- 16.4.1. CBP offices are required to conduct self-inspections for the safeguarding of classified and sensitive but unclassified information on an annual basis. The Office of Internal Affairs, Security Management Division receives and analyzes SIP results in this area.

16.5. UNANNOUNCED REVIEWS

- 16.5.1. The Office of Internal Affairs may conduct an unannounced review of a CBP program office without the benefit of advance notification. An unannounced review is conducted when issues or circumstances arise, which raise concerns relative to the effective and efficient management of classified or sensitive but unclassified information within a CBP program office.

16.6. EXTERNAL REVIEWS AND INSPECTIONS

- 16.6.1. CBP offices may be subject to reviews and inspections from outside entities such as the DHS Chief Security Office, DHS Office of Inspector General or the National Archives Records Administration, Information Security Oversight Office.

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

17. APPENDIX A - SECURITY FORMS

SECURITY FORMS

- DHS 11000-1(08-03): Classified National Security Information Courier Card
- DHS 11000-02: Courier Authorization Request
- DHS 11000-3(08-03): Document Control Register
- DHS 11000-4(08-03): Top Secret Signature Record
- DHS 11000-5: DHS Personnel Security Data Verification Request
- DNS 11000-6: Non-Disclosure Agreement
- DHS 11000-8: Disclosure Record
- DHS 11000-9: Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act
- DHS 11000-10: Record of Security Violation
- DHS 11000-11,1: Document Record of Transmittal
- DHS 11000-13: Visitor Processing Information
- DHS 11000-14: Identification Access Control Card Request
- DHS 11000-15: Courier Service Request
- DHS 11000-16: DHS Employee Credential Request Form
- DHS 11000-17: Request for Security Clearance for Access to Classified Information
- DHS 11000-18: Classified Document Certification of Destruction
- DHS 11041-1: Request for Delegation of Original Classification Authority
- DHS 11042-1: For Official Use Only (FOUO) Labels
- DHS 11043-1: Notification of Foreign Travel
- DHS 11053-5: Foreign Contact Form
- SF-312: Classified Information Nondisclosure Agreement (01/00)
- SF-700: Security Container Information (08/85)
- SF-701: Activity Security Check Sheet
- SF-702: Security Container Check Sheet
- SF-703: Top Secret Cover Sheet
- SF-704: Secret Cover Sheet
- SF-705: Confidential Cover Sheet
- SF-706: Top Secret Label

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

- SF-707: Secret Label
- SF-708: Confidential Label
- SF-710: Unclassified Label
- SF-711: Data Descriptor Label
- CBP Form 241: Separation Clearance
- CBP Form 242: Contractor Employee Separations Clearance
- CBP Form 2002: Computer Incident Report
- CBP Form 6100: Security Clearance Request
- CBP Form 6101: Classified Visit Request Security Clearance Certification
- No Number: Inadvertent Disclosure Statement (IAW DHS MD 11049-Attachment 2)
- No Number: DHS For Official Use Only (FOUO) Cover Sheet
- No Number: DHS CBP Reporting Foreign Contacts

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.





BACK



BADGES, CREDENTIALS AND OFFICIAL IDENTIFICATION

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

[BACK](#)

CONTENTS

1. CHAPTER 1: DEFINITIONS 851

1.1. DEFINITIONS 851

2. CHAPTER 2: PURPOSE, SCOPE, AND SUPERSEDED/CANCELLED POLICY/SUMMARY OF CHANGES 853

2.1. PURPOSE 853

2.2. SCOPE 853

2.3. SUPERSEDED/CANCELLED POLICY/SUMMARY OF CHANGES 853

3. CHAPTER 3: POLICY 855

3.1. POLICY 855

3.2. NEW BADGES, CREDENTIALS, AND/OR METHODS OF USE OR DISPLAY 855

3.3. USE OF BADGES AND CREDENTIALS 855

3.4. MISCONDUCT AND PENALTIES 856

3.5. QUALIFIED RETIRED LAW ENFORCEMENT OFFICERS 856

4. CHAPTER 4: AUTHORITIES AND REFERENCES 859

5. CHAPTER 5: ROLES AND RESPONSIBILITIES 861

5.1. COMMISSIONER 861

5.2. DIRECTOR OF SECURITY MANAGEMENT DIVISION (SMD) 861

5.3. BADGE AND CREDENTIALING OFFICE MANAGER (BCOM) 861

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

FOR OFFICIAL USE ONLY

BACK

5.4. ASSISTANT COMMISSIONERS, CHIEF OF THE BORDER PATROL, AND CHIEF COUNSEL. 861

5.5. ASSISTANT COMMISSIONER OF HUMAN RESOURCES MANAGEMENT 862

5.6. DEPUTY ASSISTANT COMMISSIONERS, DIRECTORS, EXECUTIVE DIRECTORS, ASSOCIATE CHIEF COUNSELS, OFFICE DIRECTORS, DIVISION DIRECTORS, AND SECTOR CHIEFS 862

5.7. LOCAL FIELD BADGE COORDINATOR 862

5.8. CBP EMPLOYEES 862

6. CHAPTER 6: TITLES, AUTHORITIES, AND POSITIONS 865

6.1. TITLES, AUTHORITIES, AND POSITIONS..... 865

7. CHAPTER 7: ACCOUNTABILITY, RETENTION, INVENTORY, AND STORAGE/PHYSICAL SECURITY 867

7.1. ACCOUNTABILITY AND RETENTION..... 867

7.2. INVENTORY..... 869

7.3. STORAGE AND PHYSICAL SECURITY OF BADGES AND CREDENTIALS..... 869

8. CHAPTER 8: REQUESTING, ISSUING, SHIPPING, AND PURCHASING 871

8.1. BADGE AND CREDENTIALS REQUESTS 871

8.2. ISSUANCE OF BADGES AND CREDENTIALS 871

8.3. CREDENTIAL PHOTOGRAPH, SIGNATURE, AND AUTHENTICATION CRITERIA..... 873

8.4. SHIPMENT OF BADGES AND CREDENTIALS..... 874

8.5. PURCHASE OF BADGES, CREDENTIAL LAMINATES, AND CREDENTIAL STOCK PAPER 874

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

BACK

8.6. ADDITIONAL ISSUES AND OPTIONAL EQUIPMENT..... 874

9. CHAPTER 9: LOST/STOLEN, DAMAGED, OR DESTROYED..... 875

9.1. LOST/STOLEN BADGES AND CREDENTIALS..... 875

9.2. DESTRUCTION OF BADGES AND CREDENTIALS 876

10. CHAPTER 10: INCENTIVE AWARDS, RETIREMENT, BADGE PRESERVATION, AND COMMEMORATIVE BADGES..... 879

10.1. INCENTIVE AWARDS 879

10.2. RETIREMENT AND PRESERVATION OF BADGES AND CREDENTIALS..... 879

10.3. COMMEMORATIVE BADGES..... 880

11. CHAPTER 11: REQUESTING AND ISSUING RETIRED LAW ENFORCEMENT IDENTIFICATION CARDS 883

11.1. POLICY..... 883

12. CHAPTER 12: INSPECTIONS..... 885

12.1. INSPECTIONS 885

13. APPENDIX 8.1: AUTHORIZED BADGE TITLES 887

14. APPENDIX 8.2: CBP CREDENTIAL TYPES AND AUTHORITIES 889

15. APPENDIX 10.1: REQUEST FOR RETIREMENT/PRESERVATION OF CBP BADGE AND CREDENTIAL 891

[RETURN TO TOP](#)

1. CHAPTER 1: DEFINITIONS

1.1. DEFINITIONS

- 1.1.1. Electronic Badge Inventory and Control System (BICS). BICS is the data base system that maintains the CBP badge and credentials life cycle data.
- 1.1.2. **Credentials.** Forms of identification that describe the authority of the bearer and identify that individual's right to exercise specific responsibilities for official and legal purposes. .
- 1.1.3. **Credential Holder.** Two-section plain black leather or vinyl wallet sized item used to display and protect a two-part credential independent of a badge.
- 1.1.4. **Badge.** A metallic emblem that is presented or displayed by the authorized bearer to indicate and serve as a sign and representative symbol of specific authority. CBP Badges are a uniform size and made of heavy gauged metal; and have a primarily gold electroplated finish appearance with dark navy blue enameled background, and the Department of Homeland Security Seal.
- 1.1.5. **Commissioning Book.** Three-section plain black leather or vinyl wallet size item used to display and protect a two-part credential and badge.
- 1.1.6. **Law Enforcement Officer.** As defined in 5 USC §§ 8331(20);8331(17), and includes DHS employees whose primary duties are the investigation, apprehension, and detention of individuals suspected or convicted of offenses against the criminal laws of the United States, or the protection of officials of the United States against threats to personal safety; an employee who transfers from performing the aforementioned duties for at least three years to a supervisory or administrative position; and certain employees who have frequent and direct contact with convicted criminals.
- 1.1.7. **Good Standing.** A CBP employee or an employee from an agency whose functions were merged into CBP, shall be deemed to have retired in good standing, unless at the time of their retirement:
- A determination made or action initiated to remove or proposing to remove the employee from federal employment;
 - Employee's security clearance was suspended or revoked or a proposal to suspend or revoke the clearance had been issued;
 - Employee was the subject of a pending psychological fitness for duty evaluation or had been found to be not fit for duty; or
 - An unadjudicated charge of misconduct against the employee or the employee was subject to an adverse disciplinary action resulting from a substantiated claim of misconduct.
- 1.1.8. **Qualified Retired Law Enforcement Officer.** A qualified retired law enforcement officer is an individual who:
- Retired in good standing from service with a public agency as a law enforcement officer, other than for reasons of mental instability;

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- Before such retirement, was authorized by law to engage in or supervise the prevention, detection, investigation or prosecution of or the incarceration of any person for any violation of law, and had statutory powers of arrest;
- Before such retirement, was regularly employed as a law enforcement officer for an aggregate of 15 years or more; or Retired from service with such agency, after completing any applicable probationary period of such service, due to a service-connected disability, as determined by such agency:
- Has a nonforfeitable right to benefits under the retirement plan of the agency;
- During the most recent 12-month period has met at the expense of the individual, the State's standards for training and qualification for active law enforcement officers to carry firearms;
- Is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and
- Is not prohibited by Federal law from receiving a firearm.

1.1.9. Retiree Identification Card. A photographic identification card issued by CBP that certifies the holder as a qualified retired law enforcement officer as defined under 18 USC §§926B; 926C. The card can be used to satisfy the identification requirements under 18 USC §926B, §926C, but provides the holder with no law enforcement powers or authorities nor any authority to carry a firearm.

2. CHAPTER 2: PURPOSE, SCOPE, AND SUPERSEDED/CANCELLED POLICY/SUMMARY OF CHANGES

2.1. PURPOSE

2.1.1. This volume of the U.S. Customs and Border Protection (CBP) Security Policy Handbook establishes the Department of Homeland Security (DHS) CBP policies, roles, and responsibilities regarding CBP official identification. Its purpose is to establish uniform protocols and provide guidance to all CBP employees regarding the issuance, use, display, control, accountability, return, and destruction of all CBP identification. Exceptions to policies and procedures must be requested in writing through the Assistant Commissioner of Internal Affairs and approved in writing by the Commissioner of CBP.

2.2. SCOPE

2.2.1. This publication establishes CBP badge and credentialing procedures and authorizes the implementation of the CBP Badge and Credentialing Program to conduct and manage all activities related to employee identification. These policies apply to all CBP Federal employees and contractors who have been issued or have access to any CBP identification.

2.2.2. This publication also establishes CBP policy with respect to retired qualified law enforcement officers and the application of the provisions of the Law Enforcement Officers Safety Act of 2004.

2.3. SUPERSEDED/CANCELLED POLICY/SUMMARY OF CHANGES

2.3.1. This volume supersedes previous issuances and previously recognized processes relating to the Badge and Credentialing Program. Effective with the issuance of this publication, all current or previous policies and/or directives relating to the CBP Badge and Credentialing Program are hereby rescinded.

3. CHAPTER 3: POLICY

3.1. POLICY

- 3.1.1. The Office of Internal Affairs (IA) is responsible for the oversight, functional, and operational control of CBP identification(s).
- 3.1.2. This publication mandates that badges and credentials will be issued only to authorized employees as evidence of their authority when having contact with the public and in dealings with Federal, State, local or foreign officials under purposes authorized by law, statute or CBP policy. Changes to this policy shall be authorized by the Commissioner and will be added as an addendum as required.
- 3.1.3. Badges and credentials are controlled and accountable CBP property. Every employee issued badges and/or credentials is required to sign a receipt for issuance, and is responsible for the proper use, safeguarding, accountability, and return of their issued badges and/or credentials in accordance with this publication.
- 3.1.4. Employees must not display any badge or credential associating them with CBP that has not been officially issued to them. All CBP offices, officials, and employees will comply with the policy and procedures.
- 3.1.5. Badges and credentials signify that the bearer is authorized to perform specific official functions under the law, statute or position of assignment.
- 3.1.6. No employee, office, organization or unit may privately purchase, obtain or produce CBP badges or credentials. Employees may not alter, deface, change or mark a badge or credential in any manner.

3.2. NEW BADGES, CREDENTIALS, AND/OR METHODS OF USE OR DISPLAY

- 3.2.1. Development, use or display of new badges or credentials will be coordinated in advance with the Assistant Commissioner of Internal Affairs, concurred by the Assistant Commissioner of the functional area concerned, and approved in writing by the Commissioner of CBP.

3.3. USE OF BADGES AND CREDENTIALS

- 3.3.1. Badges and/or credentials will be issued on a selective and/or restricted basis. Badges and/or credentials authorize the bearer to perform specific official functions as mandated by law, statute or position of assignment.
- 3.3.2. Credentials shall identify whether an employee is authorized to:
 - Carry a firearm;
 - Conduct investigations; and
 - Make arrests.
- 3.3.3. Issued badges and credentials are used only for official purposes related to CBP duties and must be displayed with discretion. The use of a badge and/or credential to coerce, intimidate, deceive, or obtain directly or indirectly, any privilege, favor,

preferential treatment, reward or personal gain for themselves or others, is considered misconduct.

- 3.3.4. Possession of credentials does not relieve the bearer from complying with established access control requirements. Any circumstance that presents a reasonable doubt on the authenticity or validity of the credential or the verification of identity or authority of the bearer shall be reported to appropriate security officials.

3.4. MISCONDUCT AND PENALTIES

- 3.4.1. Misconduct. Employees and contractors are responsible for the proper use and safeguarding of all CBP identification. The careless handling, abuse, misuse or intentional misrepresentation of badges and credentials shall be cause for possible administrative or disciplinary action, which may include, but not limited to temporary suspension, reassignment, revocation of official duties and responsibilities, removal from employment with CBP or other penalties.

- 3.4.2. Penalties. Badges and credentials should never be issued or used for transacting non-official business. Penalties may be imposed pursuant to law for the improper use of official identification to include:

- 18 USC §499. Military, naval, or official passes--"Whoever falsely makes, forges, counterfeits, alters, or tampers with any naval, military, or official pass or permit, issued by or under the authority of the United States, or with intent to defraud uses or possesses any such pass or permit, or personates or falsely represents himself to be or not to be a person to whom such pass or permit has been duly issued, or willfully allows any other person to have or use any such pass or permit, issued for his use alone, shall be fined under this title or imprisoned not more than five years, or both."
- 18 USC §1028 details what are fraudulent activities, as well applicable penalties, in connection with identification documents and information.
- USC 18 §701. Official badges, identification cards, other insignia--"Whoever manufactures, sells, or possesses any badge, identification card, or other insignia, of the design prescribed by the head of any department or agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print, or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation thereof, except as authorized under regulations made pursuant to law, shall be fined under this title or imprisoned not more than six months, or both."

3.5. QUALIFIED RETIRED LAW ENFORCEMENT OFFICERS

- 3.5.1. Pursuant to 18 USC §926C, a qualified retired law enforcement officer may carry a concealed firearm, subject to certain limitations, including:
- CBP Credentials (containing their photograph, name, signature, and position title) marked in a visible manner as to designate the retired status on the top and bottom portion of the credentials.; or

- A photographic identification issued by CBP; and
- During the most recent 12-month period, has met, at the expense of the individual, the standards for the state in which the individual resides for training and qualification for active law enforcement officers to carry a firearm.

- 3.5.2. CBP shall prepare and issue a retiree identification card for qualified retired law enforcement officers who have retired from CBP or a predecessor agency that was merged into CBP to replace any lost or stolen “Retired” CBP Credentials. If the retired law enforcement officer did not receive “Retired” CBP credentials or retired credentials for a predecessor agency, a sworn affidavit to that effect must accompany the request for the retired identification card. This identification card shall be separate and distinct from an employee’s retired credentials.
- 3.5.3. CBP shall prepare and issue a retiree identification card only for qualified retired law enforcement officers who have retired from CBP or a predecessor agency that was merged into CBP since 1995. Retirees who retired before 1995 cannot request retired identification cards.
- 3.5.4. If the retiree identification card is being requested as a replacement for lost or stolen CBP “Retired” credentials, the retiree will be required to file a lost or stolen report with their local law enforcement office and ensure that a National Crime Information Center (NCIC) report was filed before the retired identification card can be issued.
- 3.5.5. Each retiree identification card shall, at a minimum, include the name of the applicant, the individual’s photograph, an identification number traceable to the bearer, the date the employee retired in good standing from service with CBP or an agency whose functions were merged into CBP, and the phrase “Retired Law Enforcement Officer.”
- 3.5.6. Retiree identification cards issued to qualified retired law enforcement officers in accordance with this section carry no law enforcement powers or authorities, and do not provide the holder with any authority to carry a firearm. This disclaimer shall be clearly marked on each retiree identification card issued by CBP, and prior to issuance. All qualified retired law enforcement officers will be required to sign a written disclaimer acknowledging that the retiree identification card carries no such powers or authorities.
- 3.5.7. CBP shall not issue a retiree identification card under this section to a qualified retired law enforcement officer until the individual signs a waiver indemnifying CBP for, and holding CBP harmless from, any resulting liability for use of or possession of a firearm carried under 18 USC §§926B; 926C.
- 3.5.8. CBP will not reimburse retired law enforcement officers for any cost associated with the certification requirement referenced in 3.5.1 of this section or provide firearm qualification testing.
- 3.5.9. CBP shall not train or qualify retired employees to carry a firearm. A retired, qualified law enforcement officer must qualify pursuant to 18 USC §926C(d)(2)(B), and in accordance with State standards for active law enforcement officers.

- 3.5.10. It shall be within the discretion of CBP to issue a qualified retired law enforcement officer a retiree identification card as described in this chapter. Should CBP determine that the subject is not qualified, or enter into an agreement in which the subject agrees that he or she is not qualified, the subject shall not be issued the retiree identification card described above.
- 3.5.11. With respect to the requirement that a qualified retired law enforcement officer “is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance,” in addition to any applicable Federal regulations or requirements, each former CBP employee seeking such State certification annually must meet State standards, if any, regarding alcohol or drug use by law enforcement officers authorized to carry a firearm.
- 3.5.12. Individuals who meet the definition of a qualified law enforcement officer under 18 USC §926B, §926C may or may not meet the definition of a law enforcement officer under the Civil Service Retirement System or the Federal Employee Retirement System. No provision of credentials or identification should be constituted as having bearing on qualifications for any other Federal program.

4. CHAPTER 4: AUTHORITIES AND REFERENCES

United States Code

- [5 USC §301](#), Departmental Regulations
- [18 USC §499](#), Military, Naval or Official Passes
- [18 USC §701](#), Official Shields, Identification Cards, and Other Insignia
- [18 USC §926B, §926C](#), Law Enforcement Officers Safety Act (LEOSA) of 2004
- [18 USC §1028](#), Fraud and Related Activity in Connection with Identification Documents and Information
- [6 USC §112](#), Secretary; Functions
- [31 USC §321](#), General Authority of the Secretary; [Treasury Directive 71-10, Chapter III, Section 6, Department of the Treasury Credentials and Badges/Shields, June 30, 1998] to the extent this is included for retirees with IDs.

Public Law

- Law Enforcement Officers Safety Act of 2004, Pub. L.108-277, 118 Stat. 865 (certified at [18 USC §926B, §926C](#).)
- Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (codified as amended in scattered sections of [6 USC §101](#) et. seq.)

Department of Homeland Security Management Directives

- DHS MD [11010.1](#), Issuance and Control of Credentials
- DHS MD [121-01-002](#), Issuance and Control of DHS Badges

U.S. Customs and Border Protection Handbooks

- [HB 5200-13B](#), U.S. Customs and Border Protection, Personal Property Management Handbook, dated November 2005

U.S. Customs and Border Protection Training Directive

- Mandatory Successful Completion of Basic Training Directive [51250-001A](#), September 3, 1999

Legacy

- Customs Directive Number [4510-017A](#), U.S. Customs Firearms and Use of Force, dated December 17, 2001
- CIS [HB 4500-01A](#), 03/03, Firearms and Use of Force Handbook

5. CHAPTER 5: ROLES AND RESPONSIBILITIES

5.1. COMMISSIONER

- 5.1.1. Oversight responsibility for the development, coordination, and administration of the CBP Badge and Credentialing Program.

5.2. DIRECTOR OF SECURITY MANAGEMENT DIVISION (SMD)

- 5.2.1. Responsible for the management of the CBP Badge and Credentialing Program and ensures policies and procedures are established and implemented by CBP.

5.3. BADGE AND CREDENTIALING OFFICE MANAGER (BCOM)

- 5.3.1. Appointed by the Director of SMD and is responsible for the overall management of the operational and administrative functions of the CBP Badge and Credentialing Program. The BCOM will ensure program compliance and controls are in place to account for all badges and credentials.
- Operates and manages the Badge and Credentialing Office;
 - Issues all badges and credentials for CBP;
 - Provides CBP field locations with administrative, functional guidance, and procedures regarding the Badge and Credentialing Program;
 - Maintains records and accounting of all CBP badges and credentials;
 - Conducts annual inventories of all badges and credentials;
 - Maintains an inventory of badges, laminate, and credential stock paper;
 - Assists in the development of a CBP identification checklist for use during periodic management inspections;
 - Ensures compliance, standardization, and continuity for all aspects of the Badge and Credentialing Program; and
 - Serves as the Contracting Officer Technical Representative (COTR) for all badges, commissioning books, credential laminate, credential cardstock, and peripheral equipment/software to manage and supply materials for the Badge and Credentialing Program.
- 5.3.2. Responsible for reviewing all applications for retiree identification cards, coordinating with the appropriate program officers to ensure that all necessary checks are conducted and determinations made as to an applicant's eligibility, verifying the applicant's identity, and issuing the card.
- ### **5.4. ASSISTANT COMMISSIONERS, CHIEF OF THE BORDER PATROL, AND CHIEF COUNSEL.**
- 5.4.1. Will ensure the CBP Badge and Credentialing Program is implemented according to established Federal laws, Executive Orders, and statutes.
- Ensures all CBP employees comply with CBP Badge and Credentialing policies and procedures; and
 - Ensures all CBP employees are issued a badge and/or credential only after

[RETURN TO TOP](#)

successfully meeting mandatory training requirements and/or meeting other established CBP criteria governing the issuance of badges and/or credentials to CBP employees.

5.5. ASSISTANT COMMISSIONER OF HUMAN RESOURCES MANAGEMENT

5.5.1. Responsible for ensuring that information about the application of LEOSA and the process for obtaining the required retiree identification card is provided to all CBP law enforcement officers who are about to retire as part of their retirement processing, and, upon request, to all retired law enforcement officers who retired from CBP or an agency whose functions were merged into CBP.

5.6. DEPUTY ASSISTANT COMMISSIONERS, DIRECTORS, EXECUTIVE DIRECTORS, ASSOCIATE CHIEF COUNSELS, OFFICE DIRECTORS, DIVISION DIRECTORS, AND SECTOR CHIEFS

5.6.1. Responsible for directing the operational and administrative functions of the Badge and Credentialing Program within their components. Responsible for appointing in writing to the CBP Badge and Credentialing Office, a local Field Badge Coordinator and an alternate to operate a Badge and Credentialing Program within their offices, areas or sectors.

5.7. LOCAL FIELD BADGE COORDINATOR

5.7.1. An individual appointed by the Field Office Principal to locally manage the needs of the field office employees regarding badges and credentials.

- Serves as the primary point of contact for correspondence, requests, and actions with the Badge and Credentialing Office;
- Maintains accurate records of all badges and credentials within that components area of responsibility;
- Ensures CBP badges and credentials are issued only to CBP employees;
- Immediately reports the loss or theft of CBP badges and/or credentials; and
- Maintains accountability and coordinates all inventories and reports any discrepancies.

5.8. CBP EMPLOYEES

5.8.1. CBP employee are responsible for:

- Ensuring issued badges and/or credentials are properly used and safeguarded at all times;
- Becoming familiar and complying with the provisions of this publication;
- Carrying issued badges and/or credentials physically on their person at all times while on duty or while carrying a CBP issued or authorized firearm or weapon;
- Immediately reporting the loss or theft of the badges and/or credentials detailed in [Chapter 9](#);
- Ensuring badges and/or credentials are properly maintained in serviceable and presentable condition;

[RETURN TO TOP](#)

FOR OFFICIAL USE ONLY

[BACK](#)

[RETURN TO TABLE OF CONTENTS](#)

- Requesting authorization to retain their badges and/or credentials upon retirement as detailed in [Chapter 10](#);
- Surrendering all badges and/or credentials upon:
 - Request of a supervisor or other duly authorized CBP official;
 - Retirement;
 - Termination, suspension or otherwise deemed unfit for duty
 - Resigning from CBP; or
 - Assignment to a position that no longer requires the issuance of a badge and/or credential as detailed in [Chapter 8](#).
- Requesting updates to badges and/or credentials due to:
 - A change in occupational series;
 - A change of name; or
 - A defect found on the badge and/or credential as detailed in [Chapter 9](#).

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

6. CHAPTER 6: TITLES, AUTHORITIES, AND POSITIONS

6.1. TITLES, AUTHORITIES, AND POSITIONS

- 6.1.1. CBP badges and credentials are issued based on the employee's responsibilities and duties. CBP employees meeting one of the following criteria may be issued CBP badges upon satisfactory completion of required training for:
- Designated law enforcement officers;
 - Employees required to carry a firearm pursuant to his or her official duties;
 - Employees who perform investigations and inspections relating to enforcement of laws or regulations; and
 - Employees that the Commissioner may designate in writing.
- 6.1.2. CBP employees with the duties and responsibilities in 6.1.1 will receive the badge(s) as required by their position of assignment, a standard commissioning book, and an appropriate two-part credential listing the applicable and approved authority of the individual's CBP job series and the current title of the employee.
- 6.1.3. All other employees within CBP will receive an appropriate two-part credential that lists the applicable and approved authority of the individual's CBP job series and a credential holder.
- 6.1.4. Employees who are assigned on detail to a position that requires different badges and/or credentials will:
- Turn in their assigned badges and/or credentials to be held in the Badge and Credentialing Office until the detail is completed.
 - Be issued another badge and/or credentials to reflect the position of assignment of their detail.
 - Turn in their temporary badges and/or credentials when their detail is completed.
 - Receive their original badge(s) and credential(s) upon completion of their detail.
- 6.1.5. CBP credentials will be permanently laminated before issuance.
- 6.1.6. Only the Commissioner of CBP has the authority to remove, change or add badge titles and/or credential authorities.

7. CHAPTER 7: ACCOUNTABILITY, RETENTION, INVENTORY, AND STORAGE/PHYSICAL SECURITY

7.1. ACCOUNTABILITY AND RETENTION

- 7.1.1. Employees, their supervisors, Deputy Assistant Commissioners, Directors of Field Operations, Executive Directors, Associate Chief Counsels, Office Directors, Division Directors, and Sector Deputy Chiefs, and the Badge and Credentialing Officer are responsible for CBP identification accountability within their geographic areas of responsibility.
- 7.1.2. Badges and credentials will be accounted for on the CBP Form 259, Personal Equipment and Clothing Record. This document will be generated at the Badge and Credentialing Office when badge and/or credentials are initially issued to an employee.
- 7.1.3. The CBP Form 259, Personal Equipment and Clothing Record, will be shipped with the badge and credential; the Field Badge Coordinator will have the employee sign the CBP Form 259 indicating receipt/turn-in of the badge and/or credential. One copy will be given to the employee, a copy will be maintained in the employee's local personnel file, and a copy will be transmitted to the Badge and Credentialing Office within 10 days of receipt.
- 7.1.4. When a badge and/or credential is returned to the Badge and Credentialing Office the same procedure will apply indicating the return of badge and/or credential. In addition to returning the badge and/or credential with CBP Form 259, the head of the office will provide supporting documentation detailing the employee's status and reason(s) as to why the badge and/or credential is being returned.
- 7.1.5. When an employee is reassigned, transferred or moved to a different location within CBP the employee will:
- Retain the assigned badge and/or credential if the new position the employee will occupy warrants the same type of badge and/or credential;
 - Relinquish the badge and/or credential at the gaining duty station if the employee must travel while carrying an authorized CBP firearm and the new position does not require the same type of badge and credential issued to the employee;
 - Turn in the badge at the losing duty station if the new position does not require the same type of badge and the employee is not carrying an authorized CBP firearm during travel. Employee will travel with the credentials;
 - Turn in the credentials at the gaining duty station if the new position does not require the same type of credentials;
 - Upon arriving at the new duty station the employee will contact their Field Badge Coordinator and indicate that they have arrived with their assigned badge and/or credentials or that they require a new badge and/or credential be issued because of the employee's position and/or assigned duties;

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- 7.1.6. An employee must turn in the assigned badge and/or credential when:
- Employment with CBP has been terminated;
 - Resigned from CBP;
 - Retired from CBP;
 - Transferred to a position that no longer requires badge and/or credentials;
 - Badge or credential is damaged and no longer presentable or serviceable;
 - No longer meeting CBP requirements to retain the badge and/or credential;
 - Law Enforcement Officers on authorized sick leave or leave without pay status for an entire qualification period;
 - Suspended from their positions (badge and/or credentials must be turned in prior to suspension);
 - Placed on administrative leave during the course of an internal investigation/inquiry;
 - Recalled/mobilized for active military duty for 30 days or more; or
 - Determined by the Commissioner that it is in the best interest of CBP.
- 7.1.7. All employees who no longer meet CBP requirements in 7.1.6 will:
- Return their badge and/or credentials to the Badge and Credentialing Office until final disposition on the employee is determined.
 - When final disposition is made on these employees, the Badge and Credentialing Officer will be notified and the badge and/or credentials will be processed as required.
- 7.1.8. Employees who have terminated, retired, resigned or transferred from CBP will return their badge and/or credentials to their immediate supervisor prior to being granted final clearance. A completed CBP Form 241, Separation Clearance Form, will be sent with the badge and credentials so final disposition of the badges and/or credentials can be implemented according to this publication. The Field Badge Coordinator will take the appropriate action to ensure that badge and/or credentials are returned to the Badge and Credentialing Office pursuant to this publication within 10 days after completion of the personnel action.
- 7.1.9. Employees who have resigned or are terminated from CBP may not retain their badge and/or credential as a memento. Exceptions to this policy will be granted on a case-by-case basis with a waiver approved through the respective Assistant Commissioner of the functional area and approved in writing by the Commissioner.
- 7.1.10. CBP badges and/or credentials that have been confiscated and are being held by the U.S. Attorneys Office, Federal, State or local law enforcement agencies will be reported to the Badge and Credentialing Office. The Field Badge Coordinator will prepare memorandum with the contact information of the individual who will be the primary point of contact for the confiscated badge and/or credentials. A copy of this memorandum will be maintained with the local records and a copy sent to the

Badge and Credentialing Office. The badge and/or credentials will be placed into a pending status at the Badge and Credentialing Office. Confiscated badge and/or credentials are required to be inventoried on an annual basis. Once the badge and/or credentials are no longer required for legal proceedings they will be returned to the Badge and Credentialing Office for final disposition.

7.2. INVENTORY

7.2.1. Badge and Credential Inventory. The Badge and Credentialing Office will conduct an annual, CBP-wide, inventory of issued and un-issued badges and issued credentials.

7.2.2. All Field Badge Coordinators will ensure that every badge and credential within their geographic area of responsibility is physically inventoried. A signed and dated copy of the inventory will be returned to the Badge and Credentialing Office. Documentation for any discrepancies will be forwarded to the CBP Badge and Credentialing Office.

7.2.3. The Badge and Credentialing Office is responsible for reviewing all inventoried records received from all CBP offices and initiating any necessary actions to address discrepancies annotated or not identified during the annual inventory.

7.2.4. The Badge and Credentialing Office will conduct an annual inventory of all badges and credentials stored in the Badge and Credentialing Office(s). Representatives of the Badge and Credentialing Office will conduct the annual inventory.

7.3. STORAGE AND PHYSICAL SECURITY OF BADGES AND CREDENTIALS

7.3.1. Badges and credentials that are not assigned to an employee will be retained at the CBP Badge and Credentialing Office or other physically secure areas authorized as satellite CBP Badge and Credentialing Offices. Unassigned badges and credentials are not authorized to be stored at field offices for any purpose.

7.3.2. Badges, credentials, laminate, and credential stock paper will be stored in a physically secured area with controlled access to the CBP Badge and Credentialing Office employees.

8. CHAPTER 8: REQUESTING, ISSUING, SHIPPING, AND PURCHASING

8.1. BADGE AND CREDENTIALS REQUESTS

- 8.1.1. Requests for new, updated (change in name or position) or replacement of lost/stolen/damaged badges and/or credentials must be requested using CBP Form 56. All items on the form must be completed. For employees in the field, the Field Badge Coordinator will forward the request to the Badge and Credentialing Office.
- 8.1.2. Requests for badges and/or credentials will include:
- Documentation indicating the employee has been hired or promoted to a new position by CBP;
 - Using [Appendix 8.1](#), Authorized Badge Titles, determine the appropriate Job Title to be placed on credentials; employees not issued a CBP badge will not have a title on their credential;
 - Remarks section will include the CBP Credential Type, three letter designation, to be issued; and a copy of course diploma or other official documentation with the name, class number, and date of graduation of the employee will be included with the request if specific training is required prior to issuance of a badge and/or credential.
- 8.1.3. Requests to replace lost or stolen badges and/or credentials are addressed in [Chapter 9.1](#), Lost/Stolen Badges and Credentials.

8.2. ISSUANCE OF BADGES AND CREDENTIALS

- 8.2.1. Only the Office of Internal Affairs Badge and Credentialing Office is authorized to issue badges and credentials.
- 8.2.2. CBP employees may not retain more than one badge set and/or one credential at a time. Issuance of updated badges or credentials will only occur when the badge and/or credential to be replaced are turned in on a one for one basis, except in the case of lost or stolen badges and credentials.
- 8.2.3. The Commissioner of CBP has the authority to permit additional badges. This additional badge will be an authorized CBP badge, required by the employee's position or assignment. Badges issued as a set will always be the same type of badge. CBP employees are not authorized to purchase a replica badge from a private vendor for any official or non-official purpose.
- 8.2.4. Employees will be issued their badges and/or credentials upon successful completion of mandatory basic training programs or when they meet the CBP criteria for the authorized issuance of a badge and/or credential. The Badge and Credentialing Office will verify that the employee has met the mandatory training requirements and/or criteria for the issuance of the requested badge and/or credential type.
- 8.2.5. The CBP Commissioner is authorized to waive CBP training requirements. A copy of the signed waiver must be provided at the time of the request for badge and/or

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

credentials.

- 8.2.6. Contractors and other temporary CBP employees will not be issued CBP badges or credentials.
- 8.2.7. The Badge and Credentialing Office will review the CBP Form 56 for accuracy, the required photo, and signature prior to issuing a badge and/or credential.
- 8.2.8. Only the employee's legal name is authorized to appear on a credential. Any discrepancies will be resolved by verifying the employee's identification with a driver's license, social security card, birth certificate or passport.
- 8.2.9. All CBP employees authorized to carry a badge and/or credential will be issued:
- One commissioning book or credential case;
 - Badge(s) (if required);
 - One two-part credential that reflects the employee's authority and title (if applicable); or
 - Replacement commissioning books or credential cases will not be issued by the Badge and Credentialing Office.
- 8.2.10. Credentials Authorizing Firearms
- A request for a credential authorizing the carrying of firearms for an employee who has not carried a firearm previously must:
 - Be signed by an Assistant Commissioner of the functional area or Chief of the Border Patrol prior to forwarding the request to the Badge and Credentialing Office;
 - If the employee is in a job series that does not authorize or usually does not have a firearm associated with it, a written memorandum authorizing the employee to carry a firearm from the Assistant Commissioner of the function area must accompany the request.
 - Subsequent requests for replacement credentials can be requested by the Field Badge Coordinator;
 - Prior to the issuance of a credential authorizing an employee to carry a firearm:
 - Certification(s) will be made by the appropriate Assistant Commissioner that the employee has qualified with a primary duty weapon;
 - Has a need to carry a firearm; and
 - Date of the most current qualification of the employee will be placed on the CBP Form 56.
 - The Field Badge Coordinator will ensure:
 - Prior to issuing a firearms credential to an employee whose job title/series is not authorized to carry a firearm that a copy of the Assistant Commissioner's waiver for approval for the individual/position to carry a firearm is attached to [CBP Form 56](#);

- o Mandatory training requirements must be met in accordance with the CBP Basic Training Directive for a new issue or a waiver approved in writing through the Assistant Commissioner of the functional area and the Commissioner of CBP; and
- o Employees who fail to qualify with the weapon they are authorized to carry must immediately surrender their credential authorizing them to carry firearms to their Field Badge Coordinator who will forward them to the Badge Office to be held in a pending status.
- A credential, as identified above, can be requested for employees who fail to qualify to identify them as a CBP employee, but with no authorities.

8.2.11. Credentials remain valid for the duration of employment. Credentials may be updated and reissued to the bearer when a change takes place under the following conditions:

- Upon legal name change (Documentation must be provided with request);
- Official change in the bearer's authority (Documentation required);
- Significant change in the bearer's appearance over a period of time; or
- Mutilation or excessive wear of the credential.

8.3. CREDENTIAL PHOTOGRAPH, SIGNATURE, AND AUTHENTICATION CRITERIA

8.3.1. Credential photographs should be sent in a digital JPEG format via e-mail and the signature can be transmitted via fax or in a digital form via e-mail to the [Badge and Credentialing Office](#). All digital media will be identified with the employee's last name and the last four of the social security number.

8.3.2. The following criteria must be met for a credential photo to be accepted:

- A full-face, frontal view, color digital image, in JPEG Format, showing a true likeness of the bearer. If prescription glasses are worn full-time, then glasses will be worn when the credential photograph is taken, except when the glasses are tinted;
- Tinted glasses or sunglasses must be removed prior to taking photograph;
- No headgear to include uniform hats will be worn for the photo, except for religious wear. Small hairclips, bows, etc., are acceptable. However, the hair should be pushed to the side or back if it interferes with a clear picture of a large portion of the face or the eye area. Hair will not cover any facial features;
- Employees will be photographed in authorized uniforms, if not in uniform, business attire is authorized;
- Facial hair is acceptable unless it conflicts with approved uniform standards;
- Both eyes must be open;
- The photo must be clearly focused; and
- A gray backdrop is the only acceptable backdrop.

8.3.3. The following criteria must be met for a credential signature to be acceptable:

[RETURN TO TOP](#)

- A neat and legible signature of the employee will be provided; and
- The employee will sign his or her name exactly as printed on the credential. Initials or abbreviations are not authorized.

8.3.4. The CBP Commissioner authenticates every CBP credential by electronically signing all CBP credentials.

8.4. SHIPMENT OF BADGES AND CREDENTIALS

8.4.1. Badges and credentials will be:

- Packaged and shipped in double envelopes;
- Sent via:
 - The current carrier authorized by DHS for U. S. Government express mailings;
 - Certified mail with return receipt required; or
 - Overnight mail.

8.4.2. All badges and/or credentials shipped will be transferred with the [CBP Form 259](#), documenting the status of the badge and/or credentials. (NOTE: Badges and credentials returned without any or all documentation will be destroyed or returned to inventory).

8.5. PURCHASE OF BADGES, CREDENTIAL LAMINATES, AND CREDENTIAL STOCK PAPER

8.5.1. The Badge and Credentialing Office is responsible for ordering badges, credential laminate, and credential stock paper from authorized vendors.

8.5.2. The Badge and Credentialing Office is required to maintain sufficient stock of badges, credential laminate, and credential stock paper, commissioning books, and credential holders to meet the annual needs of CBP.

8.6. ADDITIONAL ISSUES AND OPTIONAL EQUIPMENT

8.6.1. CBP organizations are authorized to purchase belt clips, lanyard badge holders, and personalized commissioning books for their employees from outside vendors.

8.6.2. Employees are authorized to purchase and use privately purchased belt clip badge holders, or lanyard badge holders, and commissioning books from outside vendors.

9. CHAPTER 9: LOST/STOLEN, DAMAGED, OR DESTROYED

9.1. LOST/STOLEN BADGES AND CREDENTIALS

- 9.1.1. CBP Employees must report the loss or theft of their issued badge and/or credential within 24 hours by filing the following reports:
- Verbal and written notification to the employee's immediate supervisor;
 - Notification to their servicing Internal Affairs Field Office or the Joint Intake Center via 1-877-2-INTAKE;
 - An incident report filed with the National Communication Center and request to be entered into the National Crime Information Center (NCIC); and
 - A formal report will be filed with the local law enforcement agency for stolen badges and/or credentials.
- 9.1.2. Each report filed regarding a lost or stolen badge and/or credential must include:
- Employee's name;
 - Proof that they are employed by CBP;
 - Social security number;
 - Credential serial number;
 - Title on the credential;
 - Badge number (including the three alphabetical letters);
 - Type of badge;
 - Date and place where the incident occurred;
 - Explanation of the incident; and
 - Any other relevant facts.
- 9.1.3. Reports and documentation of the lost/stolen badge and/or credentials will be forwarded through the Field Badge Coordinator to the Badge and Credentialing Office and all required documentation will be updated.
- 9.1.4. A request for replacement of lost or stolen badges and/or credentials will be forwarded through the employee's Field Badge Coordinator to the Badge and Credentialing Office. The request for replacement will be made using the CBP Form 56. No replacement badge and/or credential will be issued until copies of below reports are filed with the Badge and Credentialing Office:
- Law enforcement report;
 - Employee report; and
 - NCIC case number included with the supporting documentation
- 9.1.5. Recovered badge and/or credentials will be reported in the same manner.
- 9.1.6. Reports, documentation, and the recovered badge and/or credentials will be forwarded through the Field Badge Coordinator to the Badge and Credentialing

[RETURN TO TOP](#)

Office and records shall be adjusted to reflect the recovery as appropriate.

- 9.1.7. Recovered badge(s) will be returned to the Badge and Credentialing Office for processing and removed from inventory.
- 9.1.8. Recovered credentials will be returned to the Badge and Credentialing Office for processing and destruction.
- 9.1.9. Lost or Stolen badges and/or credentials will be processed through existing Board of Survey procedures outlined in the Personal Property Handbook by the employees duty station. If it is determined that negligence or poor judgment was used in safeguarding the badge and/or credentials, the employee may be subject to discipline and/or required to pay for the badges and/or credentials.
- 9.1.10. Damaged Badges and Credentials
- 9.1.11. Damaged badges are authorized to be replaced. If a badge is damaged to the extent that it projects an unprofessional appearance or is not serviceable, replacement will be requested using the CBP Form 56.
- 9.1.12. If a credential becomes unserviceable (i.e. separating laminate or damaged through excessive wear or use) it will be replaced using CBP Form 56.
- 9.1.13. Damaged badges will be approved for repair or destruction based on their condition as determined by the Badge and Credentialing Office.
- 9.1.14. Damaged credentials will be returned to the Badge and Credentialing Office, removed from the inventory and destroyed.

9.2. DESTRUCTION OF BADGES AND CREDENTIALS

- 9.2.1. Unserviceable badges will be destroyed at least once every fiscal year and credentials will be destroyed at least once a month.
- 9.2.2. Destruction of Badges
 - The Badge and Credentialing Office will identify unserviceable CBP badges that are damaged, obsolete or for any reason removed from the badge inventory to be destroyed. The Badge and Credentialing Office representative will complete CBP Form 4613, Order to Destroy and Record of Destruction of Forfeited, Abandoned, or Unclaimed Merchandise, with the required information;
 - A memorandum requesting destruction of the CBP badges will be prepared, a [Report of Excess Personal Property, SF 120](#), completed with type and serial number of each badge to be destroyed, and the [CBP Form 4613](#) Order to Destroy and Record of Destruction of Forfeited, Abandoned, or Unclaimed Merchandise, prepared and sent to the Director, Security Management Division for approval;
 - Once approval for destruction is received each badge will be listed by type of badge and serial number on the SF 120. The badges will be inventoried and verified by two other CBP employees and annotated with the date of the inventory and employee's name and signature on the SF 120. Badges will be

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

sealed with tape and marked in such a manner that will prevent unauthorized access and secured in the Badge and Credentialing Office until shipped or transported to an authorized destruction facility; and

- All records of the badge destruction will be maintained in the Badge and Credentialing Office. Records will be updated with the proper destruction code and date of destruction.

9.2.3. Destruction of Credentials

- Credentials that have been returned by employees, damaged, obsolete or for any reason removed from the credential inventory will be destroyed and certified on the Order to Destroy and Record of Destruction of Forfeited, Abandoned, or Unclaimed Merchandise, CBP Form 4613;
- Each credential will be listed by credential form number and serial number on the Report of Excess Personal Property, SF 120. The credentials will be inventoried and verified by another CBP employee and annotated with the date of the inventory and employees name and signature on the SF 120. Once the credentials are inventoried they will be locally shredded in the presence of the BCOM or their designee and one witness. CBP employees witnessing the credential destruction will sign the CBP Form 4613; and
- All records of the credential destruction will be maintained in the Badge and Credentialing Office. Records will be updated with the proper destruction code and date of destruction.

10. CHAPTER 10: INCENTIVE AWARDS, RETIREMENT, BADGE PRESERVATION, AND COMMEMORATIVE BADGES

10.1. INCENTIVE AWARDS

- 10.1.1. In accordance with the CBP Incentive Awards Program, presentations of badges as honorary awards are authorized in recognition of the recipient's specific significant accomplishments in furtherance of the CBP mission.
- 10.1.2. When the intention is to honor an employee by awarding a badge in Lucite, the recommendation must be in compliance with CBP Incentive Awards Program guidelines and submitted to the CBP Badge and Credentialing Office.
- 10.1.3. The Badge and Credentialing Office will forward the request to the Headquarters Honorary Awards Administrator for processing.

10.2. RETIREMENT AND PRESERVATION OF BADGES AND CREDENTIALS

- 10.2.1. CBP employees who retire in good standing and are authorized to have their badges and/or credentials preserved as a memento of their service.
- 10.2.2. CBP employees who have been promoted or changed positions within CBP and their new position does not require the same type of badges are authorized to have one of their assigned badges embedded in Lucite.
- 10.2.3. CBP employees who have been promoted or changed positions within CBP and their new position does not require the same type of credentials are not authorized to retain their credentials as a memento.
- 10.2.4. Employees who have resigned or transferred from CBP are not authorized to have their badges embedded in Lucite or their credentials canceled and returned to them as a memento.
- 10.2.5. Badge Preservation
 - Retiring employees occupying law enforcement officer positions for an aggregate of 15 years or more prior to retirement, or retired due to a service-connected disability (after completing any applicable probationary period) are authorized to have badges preserved with an embossed "RETIRED" emblem or encased in Lucite. One of these methods is mandatory to limit such use to exhibition purposes and to ensure distinction from active badge. New or replacement badges are not authorized to be issued to retirees or persons separated from CBP;
 - Retiring employees who occupied law enforcement officer positions for less than an aggregate of 15 years prior to retirement are authorized to have badges preserved by being encased in Lucite and returned to the employee. This is mandatory to limit such use to exhibition purposes and to ensure distinction from active badges. New or replacement badges are not authorized to be issued to retirees or persons separated from CBP;

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- Employees who were promoted or changed positions within CBP and are authorized may have one of their assigned badges preserved by being encased in Lucite and returned to the employee. This is mandatory to limit such use to exhibition purposes and to ensure distinction from active badges; and
- The CBP Badge and Credentialing Office will provide approved vendor information, costs, and options for badge preservation.

10.2.6. Credential Preservation

- Retirees are authorized to have their credentials retired. Credentials will be marked in a visible manner as to designate the Retired Status. New or replacement credentials are not authorized to be issued to retirees or persons previously separated from CBP; and
- Retired credentials issued by CBP meet the requirements of LEOSA.
- Additional information on the LEOSA retiree identification card can be found in [Chapter 3.5.1](#).

10.2.7. Deceased CBP Employees

- Families and/or co-workers are authorized to request to have the badges and/or credentials of a CBP employee who has died while employed by CBP preserved as a memento. The CBP Badge and Credentialing Office will provide approved vendor information, costs, and options. The badge and credentials will be embossed with an “FOR HONORABLE SERVICE” emblem. This is mandatory to limit such use to exhibition purposes and to ensure distinction from active badges and/or credentials. Funds through the CBP National Awards Program are authorized for payment of badges and/or credentials of a CBP employee who is deceased.

10.2.8. Requesting Retirement and/or Preservation of CBP Badges and Credentials

- All authorized requests for the retirement and/or preservation of CBP badges and credentials must use the Request for Retirement/Preservation of CBP Badges and Credentials ([Appendix 10.1](#)). Requests for the retirement and/or preservation of badges and/or credentials will include documentation indicating the employee has retired from CBP or been promoted or transferred within CBP. All items must be filled out and the request, supporting documentation and badge and/or credentials forwarded to the Badge and Credentialing Office through their respective Field Badge Coordinator; and
- CBP employees who are requesting retirement and/or preservation of their badges and credentials and who were employed as a law enforcement officer for an aggregate of 15 years or more before retirement or retired due to a service-connected disability (after completing any applicable probationary period) will be required to provide documentation of their law enforcement officer service with the Request for Retirement/Preservation of CBP Badges and Credentials.

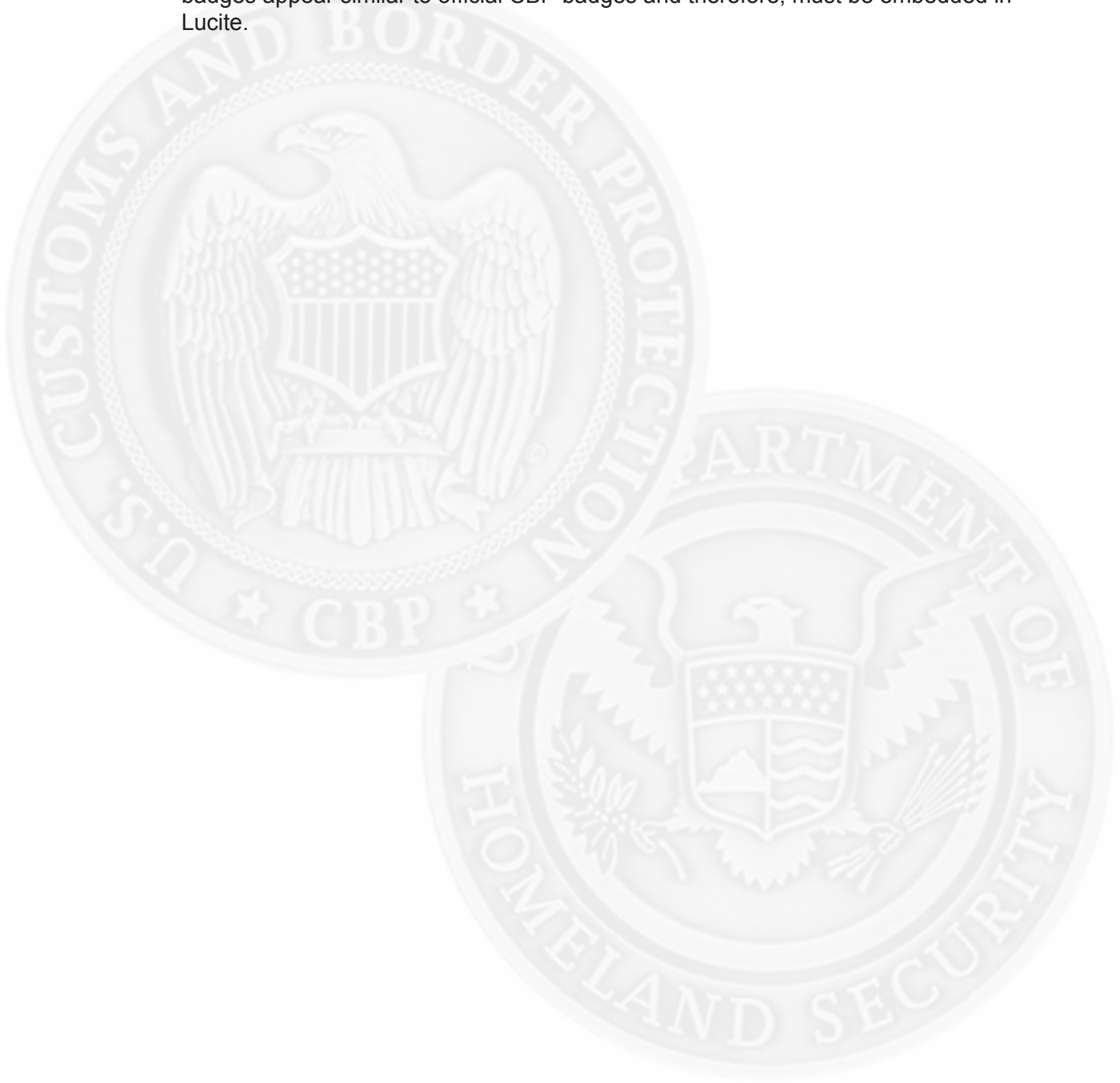
10.3. COMMEMORATIVE BADGES

10.3.1. Commemorative badges are unofficial and are not administered by the Badge and

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Credentialing Office. Because of the potential for misuse when badges imitations are distributed, the manufacture and purchase of commemorative badges is prohibited without the direct written approval of the Commissioner of CBP. These unofficial badges appear similar to official CBP badges and therefore, must be embedded in Lucite.



11. CHAPTER 11: REQUESTING AND ISSUING RETIRED LAW ENFORCEMENT IDENTIFICATION CARDS

11.1. POLICY

- 11.1.1. Retired law enforcement officers must prepare and submit a complete application package to the CBP Badge and Credential Program. The application must contain original signatures. Electronic signatures will not be accepted. The complete application package can be accessed on the Internet at <http://www.cbp.gov>.
- 11.1.2. Once an application is received, the CBP Badge and Credential Office will review the package, paperwork, and determine the applicant's eligibility to receive a retiree identification card.
- 11.1.3. A determination as to an applicant's eligibility to receive the retiree identification card shall be made within 60 business days of the receipt of the initial application.
- 11.1.4. If after all the necessary and/or required checks are conducted, the retiree is determined to be eligible to receive a retiree identification card, the CBP Badge and Credential Office will mail the card to the requested address.
- 11.1.5. If the retiree is determined to be ineligible to receive the retiree identification card, the CBP Badge and Credential Office will mail a letter to the retiree indicating such determination and the basis for this decision. The individual will then be given an opportunity to respond as provided for in the letter.

12. CHAPTER 12: INSPECTIONS

12.1. INSPECTIONS

- 12.1.1. The CBP Badge and Credentialing Office is authorized to conduct inspections. Inspections will be conducted to verify conformance with this policy and provide advice and assistance to employees. A formal report will be provided to the office listing any deficiencies within 10 working days after the inspection. The office inspected will have 60 days to correct any deficiencies from the date of the report and provide written documentation to the Badge and Credentialing Office that deficiencies have been corrected.



13. APPENDIX 8.1: AUTHORIZED BADGE TITLES

Badge Designation	Organization of Primary Assignment	Approved Badge Title
AIA	Air and Marine	Air Interdiction Agent
AIR	Air and Marine	Aviation Enforcement Officer
AMA	Air and Marine	Chief of Staff
AMB	Air and Marine	Executive Director
AMC	Air and Marine	Assistant Commissioner
AMD	Air and Marine	Deputy Assistant Commissioner
AME	Air and Marine	Director
AMF	Air and Marine	Deputy Director
AMG	Air and Marine	Detection Enforcement Officer
AMH	Air and Marine	Supervisory Detection Enforcement Officer
AMJ	Air and Marine	Specialist
ASA	Air and Marine	Supervisory Air Interdiction Agent
AUD	Customs and Border Protection	Regulatory Auditor
BPA	Border Patrol	Border Patrol Chief
BPB	Border Patrol	Deputy Chief
BPC	Border Patrol	Associate Chief
BPD	Border Patrol	Chief Patrol Agent
BPE	Border Patrol	Deputy Chief Patrol Agent
BPF	Border Patrol	Assistant Chief Patrol Agent
BPG	Border Patrol	Patrol Agent In Charge
BPH	Border Patrol	Assistant Patrol Agent In Charge
BPJ	Border Patrol	Supervisory Patrol Agent
BPL	Border Patrol	Senior Patrol Agent
BPM	Border Patrol	Patrol Agent
CAA	Customs and Border Protection	Deputy Commissioner
CAB	Customs and Border Protection	Assistant Commissioner
CAC	Customs and Border Protection	Deputy Assistant Commissioner
CAD	Customs and Border Protection	Chief of Staff
CAE	Customs and Border Protection	Senior Policy Advisor
CAF	Customs and Border Protection	Chief Counsel
CAG	Customs and Border Protection	Deputy Chief Counsel
CAH	Customs and Border Protection	Deputy Chief Of Staff
CAJ	Customs and Border Protection	Director Field Operations
CAK	Customs and Border Protection	Director
CAL	Customs and Border Protection	Deputy Director
CAM	Customs and Border Protection	Assistant Director
CAN	Customs and Border Protection	Port Director
CAP	Customs and Border Protection	Chief
CAQ	Customs and Border Protection	Supervisor
CAR	Customs and Border Protection	Officer
CAS	Customs and Border Protection	Agriculture Specialist
CAT	Customs and Border Protection	Seized Property Specialist
CAU	Customs and Border Protection	Import Specialist
CAV	Customs and Border Protection	Regulatory Auditor
CAW	Customs and Border Protection	Forensic Scientist

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

CAX	Customs and Border Protection	Congressional Liaison
CAY	Customs and Border Protection	Public Affairs Specialist
CAZ	Customs and Border Protection	Associate Chief Counsel
CBD	Customs and Border Protection	Honorary Officer
CBI	Customs and Border Protection	Internal Affairs
CBP	Customs and Border Protection	Commissioner
CCA	Customs and Border Protection	Supervisory Attorney
CCB	Customs and Border Protection	Attorney
CCD	Customs and Border Protection	Security Specialist
CCE	Customs and Border Protection	Communications Officer
CCF	Customs and Border Protection	Intelligence Research Specialist
CIA	Customs and Border Protection	Technology Officer
DSP	Customs and Border Protection	Specialist
MIA	Air and Marine Operations	Marine Interdiction Agent
SMA	Air and Marine Operations	Supervisory Marine Interdiction Agent

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

14. APPENDIX 8.2: CBP CREDENTIAL TYPES AND AUTHORITIES

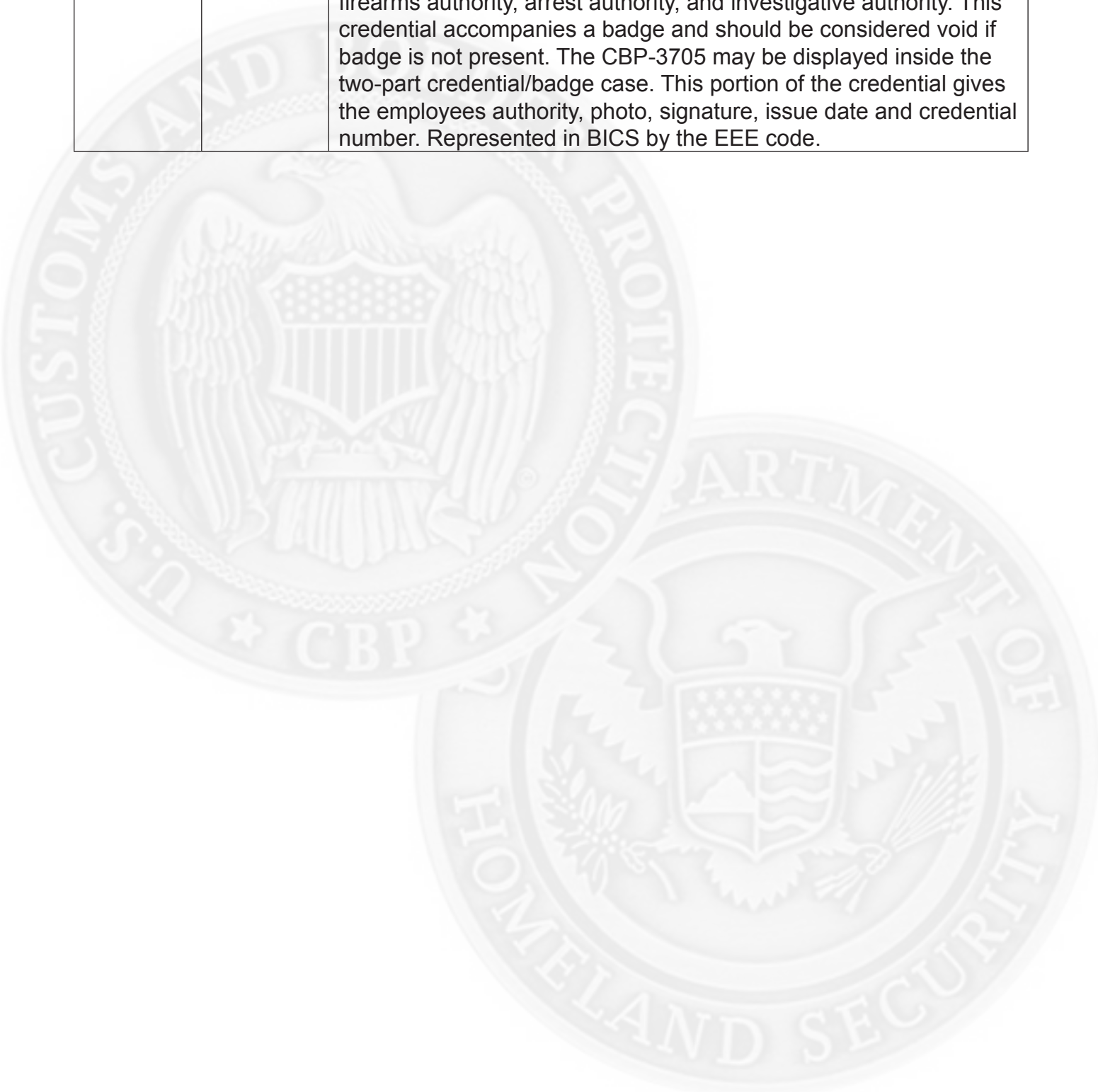
Credential Type	Credential Letter	Credential Authority
3700		CBP issues a two-part credential. The top portion of all credentials is referred to as a 3700. This portion of the credential states the employee name, credential number and title if applicable.
3700/3701	AAA	A two-part credential issued to employees who are authorized to make arrests and carry firearms. The credential is issued to Officers and other employees who do not have investigation duties. This portion of the credential reflects the employees authority, photo, signature, issue date and credential number. This credential accompanies a badge and should be considered void if badge is not present. The CBP-3701 may be displayed inside the two-part credential/badge case. Represented in BICS by the AAA code.
3700/3702	BBB	A two-part credential issued to employees authorized to carry a firearm and who do not have arrest or investigative authority. This portion of the credential gives the employees authority, photo, signature, issue date and credential number. This credential accompanies a badge and should be considered void if badge is not present. The CBP-3702 may be displayed inside the two-part credential/badge case. Represented in BICS by the BBB code.
3700/3703	CCC	A two-part credential issued to employees who are issued a badge, but have no firearms authority, no arrest authority, and no investigative authority. This credential accompanies a badge and should be considered void if badge is not present. The CBP-3703 may be displayed inside the two-part credential/badge case. This portion of the credential gives the employees authority, photo, signature, issue date and credential number. Represented in BICS by the CCC code.
3700/3704	DDD	A two-part credential issued to employees who have no badge, no firearms authority, no arrest authority, and no investigative authority. The CBP-3704 may be displayed inside the two-part credential case. This portion of the credential gives the employees authority, photo, signature, issue date and credential number. Represented in BICS by the DDD code.

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

3700/3705	EEE	A two-part credential issued to Border Patrol Agents and Enforcement Officers who are authorized full authority to include firearms authority, arrest authority, and investigative authority. This credential accompanies a badge and should be considered void if badge is not present. The CBP-3705 may be displayed inside the two-part credential/badge case. This portion of the credential gives the employees authority, photo, signature, issue date and credential number. Represented in BICS by the EEE code.
-----------	-----	--



[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

15. APPENDIX 10.1: REQUEST FOR RETIREMENT/PRESERVATION OF CBP BADGE AND CREDENTIAL

DATE:

TO: CBP BADGE AND CREDENTIALING OFFICE
Federal Law Enforcement Training Center
TH-390 A
Glynco, GA 31524
ATTN: Badge & Credentials
(912) 554-4289/CBP.CREDENTIALS@cbp.dhs.gov

FROM: _____

E-Mail: _____
Phone #: _____

Employee: NAME: _____
SSN: _____
BADGE#'s: _____
BADGE TYPE: _____
CREDENTIAL #: _____
CREDENTIAL TITLE: _____

The above referenced CBP Employee requests retirement/preservation of his/her badge and/or credentials as indicated below and has the approval of a supervisor, or higher official as indicated by signature below. I certify that the individual is (please check below reason):

_____ Retiring from Federal Service employed as a LAW ENFORCEMENT OFFICER WITH 15 YEARS OR MORE years of service.
Attach copy of SF52 or clearing papers and copies of SF50's documenting 15 years of service as a Law Enforcement Officer.

_____ Retiring from Federal Service employed as a Law Enforcement Officer due to a service-connected disability.
Attach copy of SF52 or clearing papers and copies of SF50's documenting Law Enforcement Officer service and service-connected disability.

_____ Retiring from Federal Service with less than 15 year of service as a Law Enforcement Officer.
Attach copies of SF52 or clearing papers and copy of SF50 documenting Law Enforcement Officer service at time of retirement.

_____ Retiring from Federal Service.
_____ Attach copies of SF52 or clearing papers.

_____ Being promoted and/or new position and does not require same type of badge and/or credential.

[RETURN TO TOP](#)

FOR OFFICIAL USE ONLY

BACK

[RETURN TO TABLE OF CONTENTS](#)

Attach copy of SF52 or clearing papers and waiver if required.

_____A survivor of a CBP employee who died while in service.

NOTE: WITHOUT PROPER DOCUMENTATION ATTACHED BAGDE AND/OR CREDENTIAL RETIREMENT/PRESERVATION WILL NOT BE PROCESSED.

OPTIONS: (Refer to CBP Law Enforcement Badge and Credential Policy for further details of options.) PLACE AN X IN FRONT OF CHOICE.

_____ Retiring from Federal Service employed as a LAW ENFORCEMENT OFFICER WITH 15 YEARS OR MORE years of service.

_____ Retiring from Federal Service employed as a Law Enforcement Officer due to a service-connected disability.

BADGE: _____ RETIRED ROCKER: _____ EMBED IN LUCITE: _____
DO NOT WISH TO RETAIN BADGE _____

CREDENTIALS: _____ MARKED RETIRED AND RETURNED
_____ DO NOT WISH TO RETAIN CREDENTIALS

_____ Retiring from Federal Service with less than 15 year of service as a Law Enforcement Officer.

BADGE : _____ EMBED IN LUCITE ____ DO NOT WISH TO RETAIN BADGE

CREDENTIALS: _____ MARKED RETIRED AND RETURNED
_____ DO NOT WISH TO RETAIN CREDENTIALS

_____ Retiring from Federal Service or promoted/new position or resigned from CBP with waiver.

BADGE: _____ EMBED IN LUCITE
_____ DO NOT WISH TO RETAIN BADGE

CREDENTIALS: _____ MARKED RETIRED AND RETURNED
_____ DO NOT WISH TO RETAIN CREDENTIALS

APPROVING OFFICIAL: _____

SIGNATURE: _____

EMPLOYEE SIGNATURE: _____

[RETURN TO TOP](#)

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.



