U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

National Policy

ORDER 1600.69D

Effective date:
09/26/23

SUBJ: FAA Facility Security Management Program

This order prescribes the Federal Aviation Administration's (FAA) Facility Security Management Program (FSMP). This directive establishes facility security policy, delegates authority, assigns responsibilities, and mandates security requirements at facilities for which the FAA is responsible for security oversight. Unless otherwise explicitly provided, this order establishes requirements for all FAA personnel, which includes FAA employees, FAA contractors, and non-employees as defined in FAA Order 1600.1, Personnel Security Program, regardless of their assigned duty location.

Kathryn B. Thomson
Deputy Administrator

Table of Contents

Chapter 1. General Information 1
1-1. Purpose of This Order 1
1-2. Audience. 1
1-3. Where Can I Find This Order? 1
1-4. Cancellation. 1
1-5. Related Publications and References. 1
1-6. Definitions. 1
1-7. Acronyms 1
1-8. Authority to Change This Order. 1
1-9. Explanation of Policy Changes 1
1-10. Background. 2
1-11. Scope of This Order. 2
Chapter 2. Roles and Responsibilities 3
2-1. FAA Lines of Business (LOBs), Staff Offices (SOs), and Office of the Administrator, (AOA). 3
2-2. Associate Administrator for Security and Hazardous Materials Safety, ASH-1 3
2-3. Director, Office of Infrastructure Protection, AXF-1. 3
2-4. Director, Office of National Security Programs and Incident Response, AXE-1. 4
2-5. Director, Office of Investigations and Professional Responsibility, AXI-1. 4
2-6. Office of the Chief Counsel (AGC). 4
2-7. Office of Government and Industry Affairs (AGI). 5
2-8. Office of International Affairs (API). 5
2-9. Chief Operating Officer, AJO-0. 5
2-10. Director, Air Traffic Control Facilities & Engineering Services, AJW-2. 5
2-11. Facility Manager (FM). 5
2-12. Office of Finance and Management (AFN), Acquisition and Business Services (ACQ), Aviation Property Management (APM). 6
2-13. Service Area/Regional Program and Project Managers of New Facility Construction, Existing Facility Modification, or New Leases. 6
2-14. FAA Personnel. 6
2-15. Owners of FAA Systems Installed at FAA Facilities. 7
Chapter 3. Facility Security Management Program Overview 8
3-1. Purpose 8

3-2. Facility Categories 8
3-3. Assigning a Facility Security Level (FSL) 8
3-4. Establishing Security Countermeasures. 9
3-5. Facility Security Assessments. 10
3-6. Risk Assessment, Management, and Acceptance. 11
3-7. Security Design for New Construction, Renovation, and/or Leased Spaces. 12
3-8. Facility Security Information. 13
Chapter 4. Facility Security Countermeasures 14
4-1. Purpose. 14
4-2. Using the Baseline LOP Templates. 14
4-3. Unique Facilities. 14
4-4. Temporary, Mobile, and Modular Assets or Facilities. 14
4-5. SSE Security System Verification and Approval. 15
Section 1. Site Security Countermeasures 16
4-1-1. Countermeasure Matrix. 16
4-1-2. Identification as a Federal Facility. 17
4-1-3. Landscaping. 17
4-1-4. Pedestrian Access to Site. 17
4-1-5. Vehicle Access Points. 18
4-1-6. Site Lighting. 18
4-1-7. Restricted Areas and Significant Areas and Assets. 18
4-1-8. Signage – Sensitive Areas. 18
4-1-9. Control of Parking. 19
4-1-10. Authorized Parking. 19
4-1-11. Vehicle Access to Controlled Parking. 19
4-1-12. Vehicle Barriers. 19
4-1-13. Vehicle Screening. 20
4-1-14. Pedestrian Access to Controlled Parking Areas. 20
4-1-15. Hazardous Materials (HAZMAT) Storage. 20
4-1-16. Receptacle and Container Placement. 20
Section 2. Structure Security Countermeasures 21
4-2-1. Countermeasure Matrix. 21
4-2-2. Blast Resistance – Windows. 22

4-2-3. Blast Resistance – Façade and Structure. 22
4-2-4. Blast Resistance – Progressive Collapse. 23
4-2-5. Blast Resistance – Under-Building Parking. 23
4-2-6. Burglary Resistance of Windows. 23
4-2-7. Walls and Non-window Openings. 23
4-2-8. Windows in Critical Areas – Ballistic Protection. 23
4-2-9. Protection of Air Intakes. 23
4-2-10. Isolated Ventilation Systems. 23
4-2-11. Heating, Ventilating, and Air Conditioning (HVAC) Control. 23
4-2-12. CBR Detection Technology. 23
4-2-13. Biological Filtration – General Building. 23
4-2-14. Biological Filtration – Lobbies and Mailrooms. 24
4-2-15. Chemical Filtration. 24
4-2-16. Security of Ventilation Equipment and Controls. 24
4-2-17. Location of Utilities and Feeders. 24
4-2-18. Separation of Emergency and Normal Power Distribution. 24
4-2-19. Emergency Generator Protection. 24
4-2-20. Protection of Water Supply. 24
Section 3. Facility Entrance Countermeasures 25
4-3-1. Countermeasure Matrix. 25
4-3-2. Badge Identification System. 26
4-3-3. Regulatory Signage 27
4-3-4. Employee Access Control. 28
4-3-5. Visitor Access Control. 30
4-3-6. Occupant Screening. 33
4-3-7. Visitor Screening. 35
4-3-8. Ballistic Protection at Screening Locations. 35
4-3-9. Lobby Queuing. 36
4-3-10. After-Hours Access Control. 36
4-3-11. Limit Building Entry Points. 36
4-3-12. Entrance Co-Location. 36
4-3-13. Perimeter Doors and Door Locks. 36
4-3-14. Control of Keys and Access Media. 37

4-3-15. Employee Convenience Doors. 37
4-3-16. Emergency Exit Doors. 37
4-3-17. Delayed Egress. 37
Section 4. Interior Security Countermeasures 38
4-4-1. Countermeasure Matrix. 38
4-4-2. Space Planning. 38
4-4-3. Access to Non-public Areas. 38
4-4-4. Security of Critical Areas. 39
4-4-5. Building Systems and Roof Access. 39
4-4-6. Publicly Accessible Restrooms. 39
4-4-7. Publicly Accessible Retail and Mixed-use Space. 39
4-4-8. Blast Resistance – Interior Public Spaces. 39
4-4-9. Blast Resistance – Mail Screening and Receiving Location. 39
4-4-10. Interior Windows. 39
Section 5. Security Systems Countermeasures 40
4-5-1. Countermeasure Matrix. 40
4-5-2. Video Surveillance System (VSS) Coverage. 41
4-5-3. VSS Monitoring and Recording. 42
4-5-4. Security Control Center. 42
4-5-5. VSS Surveillance Advisory. 42
4-5-6. Intrusion Detection System (IDS) Coverage. 42
4-5-7. IDS Monitoring. 43
4-5-8. Duress Alarms or Assistance Stations. 43
4-5-9. Security System Integrity. 43
4-5-10. Security Communications. 43
4-5-11. Building Communication System. 43
4-5-12. Emergency Power for Security Systems. 43
4-5-13. Security System Testing. 43
4-5-14. Security System Maintenance. 43
Section 6. Security Operations and Administration Countermeasures 44
4-6-1. Countermeasure Matrix. 44
4-6-2. Facility Security Committee (FSC). 45
4-6-3. Facility Security Committee (FSC) Chairperson. 45

4-6-4. Security Operations Management. 45
4-6-5. Security Force Fixed Post – Exterior. 45
4-6-6. Security Force Fixed Post – Screening Checkpoint. 45
4-6-7. Security Force Patrols. 45
4-6-8. Security Force Response. 45
4-6-9. Facility Security Plan (FSP). 45
4-6-10. Occupant Emergency Plan (OEP). 48
4-6-11. Availability of Emergency Plans and Documentation. 48
4-6-12. Protection of Construction Information. 48
4-6-13. Security during Construction and Renovation. 48
4-6-14. Mail/Package Handling and Other Deliveries. 48
4-6-15. Security Awareness Training. 48
Section 7. Facility Cybersecurity Countermeasures 50
4-7-1. Countermeasure Matrix. 50
4-7-2. Identify and Define Building Access and Control Systems (BACS) Devices and Networks. 50
4-7-3. Segment BACS from Business Networks; Control Access to Devices and Networks. 50
4-7-4. Establish and Maintain BACS Configuration Management. 50
4-7-5. Maintain BACS Infrastructure. 50
4-7-6. Ensure the Integrity and Availability of BACS Operational Data. 50
4-7-7. Identify and Manage Access Points for Network Communications, Removable Media, Messaging Services, and Internet Access for BACS. 51
4-7-8. Establish Processes for Incident Response for BACS. 51
Chapter 5. Contract Security Officers 52
5-1. Purpose. 52
5-2. CSO Functions and Staffing. 52
5-3. Selecting a CSO Provider. 53
5-4. CSO Standards. 53
5-5. Contract Security Services Oversight. 58
5-6. CSO Operations. 59
Appendix A. Related Publications and References A-1
Appendix B. Construction Standards for Open Storage Secure Areas B-1
B-1. Open Storage Secure Area. B-1
B-2. General Construction Requirements. B-1

B-3. Emergency Notification Systems Criteria. B-4
B-4. Intrusion Detection Systems (IDS) Criteria. B-4
B-5. Physical Access Control System (PACS) Criteria. B-6
B-6. Acoustical Security. B-7
Appendix C. Security Requirements for Flight Standards District Offices (FSDO) C-1
C-1. Purpose. C-1
C-2. Adjusted Security Countermeasures. C-1
C-3. Blast Resistance – Windows. C-1
C-4. Security of Critical Areas. C-1
C-5. VSS Coverage. C-1
C-6. Duress Alarms or Assistance Stations. C-1
Appendix D. Security Requirements for Child Care Centers (CCC) D-1
D-1. Purpose. D-1
D-2. Security Countermeasures. D-1
D-3. Perimeter Doors and Door Locks. D-1
D-4. Security of Critical Areas. D-1
D-5. VSS Monitoring and Recording. D-1
Appendix E. Security Requirements for the MMAC and WJHTC E-1
E-1. Purpose. E-1
E-2. Comprehensive Assessments. E-1
E-3. Adjusted Security Countermeasures E-1
E-4. Pedestrian Access to Site E-1
E-5. Site Lighting. E-1
E-6. Vehicle Access to Controlled Parking E-2
E-7. Blast Resistance – Façade and Structure E-2
E-8. Visitor Access Control. E-2
E-9. Video Surveillance System (VSS) Coverage. E-2
E-10. Security Force Fixed Post – Exterior. E-2
E-11. Security of Critical Areas E-3
Appendix F. Security Requirements for Air Route Surveillance RADAR Joint Surveillance System (ARSR-JSS) Facilities with COMSEC and Common ARSR (CARSR) Facilities F-1
F-1. Purpose F-1
F-2. Adjusted Security Countermeasures F-1

F-3. Restricted Areas and Significant Areas and Assets....F-1
F.4. Vehicle Access Points....F-2
F-5. Burglary Resistance of Windows....F-2
F-6. Employee Access Control....F-2
F-7. Visitor Access Control....F-2
F-8. Perimeter Doors and Door Locks....F-2
F-9. VSS Coverage....F-2
F-10. Intrusion Detection System (IDS) Coverage....F-2
F-11. IDS Monitoring....F-3
F-12. Security Operations Management....F-3
F-13. Facility Security Plan (FSP)....F-3
Appendix G. Security Requirements for Sponsor-Owned or Sponsor-Leased Federal Contract Towers (FCT)....G-1
G-1. Purpose....G-1
G-2. Adjusted Security Countermeasures....G-1
G-3. Identification of a Federal Facility....G-1
G-4. Pedestrian Access to Site....G-1
G-5. Regulatory Signage....G-1
G-6. Employee Access Control....G-1
G-7. Visitor Access Controls....G-1
G-8. Facility Security Plan (FSP)....G-1
G-9. Occupant Emergency Plan (OEP)....G-2
G-10. Availability of Emergency Plans and Documentation....G-2
G-11. Protection of Construction Information....G-2
Appendix H. Security Requirements for Mobile Asset Deployment Centers (MADC)....H-1
H-1. Purpose....H-1
H-2. Adjusted Security Countermeasures....H-1
H-3. Video Surveillance System (VSS) Coverage....H-1
H-4. Facility Security Plan (FSP)....H-1
Appendix I. Definitions....I-1
Appendix J. Frequently Used Acronyms....J-1

List of Tables

Table *Page*
3-1. Typical Facility Security Level Assignments 9
4-1. Non-Standard FAA Facilities 14
4-1-1. Facility Site Security Countermeasures 16
4-1-2. FAA Security Illumination 18
4-2-1. Structure Security Countermeasures 21
4-3-1. Facility Entrance Security Countermeasures 25
4-3-2. FAA Signage Available from FAA Depot 28
4-4-1. Interior Security Countermeasures 38
4-5-1. Security Systems Countermeasures 40
4-6-1. Security Operations and Administration Countermeasures 44
4-6-2. Security Checkpoint Functions and Equipment 45
4-6-3. Sample FSP Contents 45
4-6-4. Initial and Annual Local Security Awareness Briefing Topics 49
4-7-1. Cybersecurity Countermeasures 50
5-1. Initial and Recurring CSO Training Requirements 54
5-2. CSO Uniforms and Equipment 56
5-3. CSO Medical Standards 57
5-4. Cutoff Levels for Drug Tests 57
5-5. CSO On-site Records 59
C-1. Adjusted Security Countermeasures for FSDOs C-1
D-1. Security Countermeasures for CCCs D-1
E-1. Adjusted Security Countermeasures for MMAC and JHTC E-1
F-1. Adjusted Security Countermeasures for ARSR-JSS/CARSR Facilities F-1
G-1. Adjusted Security Countermeasures for Sponsor-Owned/Leased FCTs G-1
H-1. Adjusted Security Countermeasures for MADCs H-1

Chapter 1. General Information

1-1. Purpose of This Order. This order defines the Facility Security Management Program (FSMP) in accordance with FAA Order 1600.6E, Facility Security Policy. The FSMP establishes security requirements at facilities for which the FAA is responsible for security oversight, as described in chapters 3 and 4 of this order.

1-2. Audience. Unless otherwise explicitly provided, this order establishes requirements for all FAA personnel (as defined in Appendix I), regardless of their assigned duty location.

1-3. Where Can I Find This Order? This order can be found on the FAA internal Orders & Notices website: https://employees.faa.gov/tools_resources/orders_notices/.

1-4. Cancellation. This order cancels FAA Order 1600.69C, Facility Security Management Program (FSMP), dated August 22, 2016, and any Office of Infrastructure Protection (AXF) Technical Guidance Memorandums that precede the published date of this order.

1-5. Related Publications and References. Some related publications and references are listed in Appendix A of this order.

1-6. Definitions. Definitions are listed in Appendix I.

1-7. Acronyms. Frequently used acronyms are listed in Appendix J.

1-8. Authority to Change This Order. The Associate Administrator for Security and Hazardous Materials Safety, ASH-1, may issue changes to this order as necessary to ensure that its provisions remain current with applicable Interagency Security Committee (ISC) standards and policies, as well as other applicable national and departmental facility security policies.

1-9. Explanation of Policy Changes. This policy is a complete revision of the prior order. It has been updated as follows to reflect changes to national and department-level policies and organizational changes within the FAA:

a. Implements the FAA's Facility Security Risk Management Process (RMP) pursuant to the 2021 edition of "The Risk Management Process: An Interagency Security Committee Standard" or any successor document.

b. Eliminates security accreditation and replaces it with risk mitigation or risk acceptance by the Line of Business (LOB) and Staff Offices (SO) for facilities they control.

c. Implements facility security scoring methodology to allow FAA leadership to make informed decisions about risk associated with facilities they control.

d. Updates facility security levels (FSLs) and associated security countermeasures that mitigate security risks for FAA-staffed facilities.

1-10. Background. Executive Order 12977, Interagency Security Committee, established the ISC and charged that committee with the authority to develop and evaluate standards for federal facilities. These published ISC standards are used to identify and implement security requirements for FAA-staffed facilities. This order provides the mechanism for assessment, implementation, and oversight of those ISC standards for FAA facilities. Additionally, Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience, states that "All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure (CI) that support primary mission essential functions." This order is consistent with that directive and, using the ISC risk management criteria, establishes the level of protection (LOP) needed to mitigate known and evaluated risks for each CI facility (see paragraph 3-2).

1-11. Scope of This Order. This order applies to all staffed facilities for which the FAA is responsible for security oversight. This order also applies to all personnel permanently or temporarily assigned to work in or on FAA-owned or leased properties or properties utilized by the FAA that are owned, leased, security-controlled, or staffed by the General Services Administration (GSA) or others (e.g., other agencies, public or private entities) in the United States and its territories unless otherwise provided. Unstaffed Common Air Route Surveillance RADAR (CARSR) and Air Route Surveillance RADAR/Joint Surveillance Systems (ARSR-4/JSS) fall under the scope of this order. All other unstaffed facilities do not fall under the scope of this order and are managed by the Unstaffed Infrastructure Sustainment (UIS) Program, AJW-24. However, many of the general security principles outlined in this order can be applied to unstaffed facilities, and ASH can assist AJW-24 in determining security requirements and conducting security assessments as requested. FAA overseas facilities follow U.S. Department of State (DOS) security directives and procedures. Domestic Servicing Security Elements (SSEs) may provide support on physical security issues at FAA organizations overseas, provided the overseas facility submits to ASH-1, in writing, a description of the support being sought and all relevant documentation to support the request. In all cases, requests must have ASH-1 approval and must be coordinated with the DOS, Bureau of Diplomatic Security. Any conflicting guidance contained in this order and any other applicable DOT/FAA order or directive must be referred to the Director, Office of Infrastructure Protection, AXF-1, through the ASH SSE. AXF-1, in coordination with the Office of the Chief Counsel (AGC), will resolve any conflicting guidance. Questions regarding what agency and office is responsible for the security of a particular facility or FAA office should be referred to AXF.

Chapter 2. Roles and Responsibilities

2-1. FAA Lines of Business (LOBs), Staff Offices (SOs), and Office of the Administrator (AOA).

a. The Administrator is the final authority for carrying out all functions, powers, and duties of the Agency relating to the acquisition and maintenance of property, services, and equipment of the Agency; and the promulgation of regulations, orders, advisory circulars, bulletins, and other official publications of the Agency, except as otherwise provided by applicable law.

b. The Administrator, Deputy Administrator; Chief Operating Officer of the Air Traffic Organization; Chief Counsel; Associate and Assistant Administrators; Senior Vice Presidents and Vice Presidents; Service Area Directors; Regional Administrators; the Directors of the Mike Monroney Aeronautical Center (MMAC) and William J. Hughes Technical Center (WJHTC); Office Directors; and managers at all levels must ensure that the contents of this order are effectively communicated, adhered to, and implemented within their organization(s).

c. Managers and their staff having responsibility for conceptual development and planning for programs, projects, operations, systems, and facility construction; modification; or leasing must coordinate with their assigned SSE to ensure the implementation of this order.

2-2. Associate Administrator for Security and Hazardous Materials Safety, ASH-1.

a. Exercises overall responsibility and authority for the implementation of the FSMP on behalf of the Administrator;

b. Ensures that policies, procedures, and standards for the FSMP are planned, developed, and implemented throughout the agency;

c. Coordinates with and supports the LOBs/SOs and other organizations as necessary to protect FAA facilities;

d. Through scheduled and unscheduled assessments, monitors the FSMP on behalf of the Administrator to ensure that each LOB/SO develops and implements comprehensive security policies and procedures for its facilities;

e. Ensures that appropriate resources are obtained and budgets planned as needed for the execution and management of the FSMP; and

f. Coordinates with affected LOBs and SOs and issues changes to this order as necessary to meet changing security requirements.

2-3. Director, Office of Infrastructure Protection, AXF-1.

a. Executes centralized governance over the FSMP across the agency on behalf of ASH-1;

b. Ensures that security measures are identified that support facility security risk mitigation;

c. Issues policy updates and clarification affecting the implementation of this order in coordination with ASH-1, AGC, and interested LOBs/SOs as appropriate;

d. Ensures that facility security assessments are planned and conducted as required and that identified security risks are reported to facility managers and the LOBs/SOs owning or operating the facility;

e. Evaluates and grants or denies requests to either add or remove countermeasures that adjust the baseline level of protection (LOP) criteria at specific facilities;

f. Partners with the Facility Security Team (FST) (formerly known as the Facility Security Risk Management (FSRM) program, managed by the Air Traffic Organization (ATO)) consistent with FAA Order 1600.6E, to support program requirements for investment decisions;

g. Oversees and develops program-related training in conjunction with the Director, ASH Office of Business and Mission Services, AXM-1;

h. Resolves conflicts, in coordination with AGC, between this order and other published national, departmental, or agency policy;

i. Evaluates changes to a facility's security level and corresponding security measures;

j. Administers the agency's International Visitor Program in coordination with the Office of International Affairs (API); and

k. Provides onsite security awareness briefings/training as resources allow.

2-4. Director, Office of National Security Programs and Incident Response, AXE-1. AXI-1 coordinates with federal law enforcement and intelligence agencies on national security matters and advises AXF-1 of any nexus to facility security operations.

2-5. Director, Office of Investigations and Professional Responsibility, AXI-1. AXI-1 notifies AXF-1 of any insider threat activities, or information developed during agency checks conducted in support of foreign visit requests, that raises threat concerns for facility security operations.

2-6. Office of the Chief Counsel (AGC).

a. Reviews all real property transactions that meet the requirements of the Acquisition Management System (AMS) Real Estate Policy 3.14.5 to ensure compliance with applicable law, policy, and the terms of this order;

b. Interprets applicable law and policy and advises agency decision-makers regarding compliance with applicable law and policy including the terms of this order; and

c. Coordinates with AXF-1 to resolve conflicts between this order and other published national, departmental, or agency policy.

2-7. Office of Government and Industry Affairs (AGI). AGI provides guidance on visits by congressional and high-profile government officials.

2-8. Office of International Affairs (API). API coordinates all visits by foreign nationals to FAA facilities and ensures completion of the visit requests through the International Visitors Program (IVP).

2-9. Chief Operating Officer, Air Traffic Organization, AJO-0.

a. Determines the criticality of ATO facilities in accordance with National Airspace System (NAS) operational requirements and provides that information to ASH;

b. Oversees the FST and provides resources necessary to acquire and implement required physical security countermeasures for facilities that fall under the responsibility of the FST Program; and

c. Identifies and assigns resources as needed for the implementation of and compliance with the requirements of this order.

2-10. Director, Air Traffic Control Facilities & Engineering Services, AJW-2.

a. Manages and implements the FST Program on behalf of ATO; and

b. Identifies and investigates technology changes that may improve or enhance facility security or result in cost savings without diminishing facility security.

2-11. Facility Manager (FM). The FM is the highest-ranking resident manager (or as otherwise identified by the owning LOB or SO) in an FAA-owned or leased facility. When there is no resident manager, it will be the manager(s) having responsibility for facility operations and/or maintenance. The FM implements the FSMP at their assigned facility as described throughout this order. Most importantly, FMs will:

a. To the extent possible, mitigates security vulnerabilities identified during facility security assessments or other evaluations;

b. Requests resources outside the scope of the FST Program as necessary to fully implement the provisions of this order;

c. Where applicable, reports inoperable, malfunctioning or deteriorating security fixtures, equipment, or systems to the Corrective Maintenance Contractor (CMC);

d. Reports on the status of open security findings after a security assessment is conducted at the facility or when requested by the SSE;

e. Includes the appropriate SSE, throughout the entire process, in facility security planning and implementing facility security policies or procedures; and

f. Conducts periodic security meetings with essential staff, as needed.

2-12. Office of Finance and Management (AFN), Acquisition and Business Services (ACQ), Aviation Property Management (APM).

a. Notifies the SSE of all new lease agreements, modifications to lease agreements, and required site surveys as early as possible so that security requirements are included in construction planning and lease transactions; and

b. Includes the SSE as a member, throughout the entire process, of any planning or design group for new facilities, major renovations or modifications to existing facilities, and FAA leases.

2-13. Service Area/Regional Program and Project Managers of New Facility Construction, Existing Facility Modification, or New Leases. Program and Project Managers must coordinate with the SSE during all phases of facility planning and design and lease negotiations to ensure that facilities meet the standards and requirements of this order prior to FAA acceptance, lease, or occupancy.

2-14. FAA Personnel.

a. Comply with the requirements of this order;

b. Report security incidents upon discovery to their manager (contractors will report to the Alternate Technical Representative (ATR), Contracting Officer's Representative (COR), or Contracting Officer (CO)) or the next available manager in their chain of command. Managers must notify the responsible FM or SSE as stipulated in paragraph 4-6-9;

c. Report non-functional security equipment to their manager (contractors will report to the ATR, COR, or CO) or the next available manager in their chain of command. Supervisors must notify the responsible FM or SSE; and

d. Wear U.S. Government-issued ID Media in accordance with this order and FAA Order 1600.78, Personal Identity Verification (PIV) and Other Identification (ID) Cards;

2-15. Owners of FAA Systems Installed at FAA Facilities. The FAA system owners of systems installed, in full or in part, at FAA facilities must coordinate with ASH to ensure their systems receive the FSMP countermeasures to satisfy FAA Order 1370.121, FAA Information Security and Privacy Policy, requirements for which ASH is the common control provider.

Chapter 3. Facility Security Management Program Overview

3-1. Purpose. This chapter provides requirements for planning and implementing the FSMP and the RMP. It details how security countermeasures are developed and assessed and how the FAA mitigates, accepts, or otherwise manages the risks of undesirable events.

3-2. Facility Categories. FAA facilities are grouped into three categories for the purpose of the FSMP: Critical Infrastructure (CI), Administrative, and unstaffed facilities.

a. Critical Infrastructure (CI). Consistent with PPD 21, which makes all federal department and agency heads responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions, FAA CI includes those air traffic facilities that provide air navigation services, which enable the operation of the National Airspace System (NAS) or house air navigation service capabilities that contribute to national defense, homeland security, law enforcement, and national response efforts to protect the nation from threats involving the air domain. Those facilities are Air Traffic Control Centers (ARTCCs), Terminal Radar Approach Control Facilities (TRACONs), Airport Traffic Control Towers (ATCTs), Combined ATCT/TRACONs, Center Radar Approach Controls (CERAPs), Air Traffic Control System Command Center (ATCSCC), Common Air Route Surveillance Radars (CARSRs), and Air Route Surveillance Radar (ARSR)/Joint Surveillance Systems (JSSs). Refer to Table 3-1.

b. Administrative Facilities. These facilities, although not designated CI, serve an important support function for the FAA's CI. FAA administrative facilities include airport certification and compliance, aviation regulatory and safety oversight and certification, as well as those facilities that house workspace for FAA personnel who provide organizational and administrative support to the FAA.

c. Unstaffed Facilities. An unstaffed facility is defined as a facility where no FAA employees or contractors are permanently assigned but may make onsite visits. With some exceptions (see para 1-11), the Unstaffed Infrastructure Sustainment (UIS) Program, AJW-24, is the office of primary responsibility for these facilities. ASH can provide security assessments and assistance with security requirements as requested by AJW-24 and FMs or in response to a history of security incidents or an unusual security situation.

3-3. Assigning a Facility Security Level (FSL). An FSL is the starting point for determining the specific security requirements and countermeasures that will apply to a particular FAA facility. Because the FAA employs a significant number of single-tenant facilities (FAA-owned and operated), similar facilities that accomplish identical missions in various locations, they have been pre-assigned FSLs by AXF through consultation with the owning organization and are based on the ISC criteria for assigning FSLs, which includes mission criticality, symbolism, population, size, and threats to tenant agencies. For FAA CI, mission criticality factors also include air traffic count level, Core 30 airport support, and resiliency/impact to the NAS. FSLs for multi-tenant facilities are based on ISC criteria and will be made in consultation with the facility tenants, the owning or leasing department or agency, and AXF. These FSLs are

summarized in this paragraph for planning purposes; however, the FSL determination matrix, associated worksheets, and supporting documentation for each FAA-staffed facility is maintained in the Facility Security Reporting System (FSRS). Where conflicts exist, the FSLs are contained in FSRS control.

a. Agency Designated FSLs. FAA facilities are typically assigned FSLs as indicated below:

Table 3-1. Typical Facility Security Level Assignments

FSL	Facility Types
FSL 4	• Mike Monroney Aeronautical Center (MMAC)* • William J. Hughes Technical Center (WJHTC)* • National Enterprise Management Center (NEMC)
FSL 3	• Air Traffic Control System Command Center (ATCSCC) • Air Route Traffic Control Centers (ARTCCs) • Center Radar Approach Control (CERAP) • Airport Traffic Control Tower (ATCT), Terminal Radar Approach Control Facility (TRACON), and combined ATCT/TRACON operating at air traffic count levels 10 – 12 • Administrative facilities as documented within FSRS (normally large facilities such as Regional Offices)
FSL 2	• TRACONs and combined ATCTs/TRACONs operating at air traffic count levels less than 10 • ATCTs operating at air traffic count levels 7 – 9 • CARSR and ARSR/JSS staffed and unstaffed facilities with or without COMSEC • RADAR Approach Control • Mobile Asset Deployment Centers (MADC) • Administrative facilities as documented within FSRS (normally facilities with medium populations such as FSDOs and AFSS)
FSL 1	• ATCTs operating at air traffic count levels 1 – 6 (includes FAA-owned FCTs) • Administrative facilities as documented with FSRS (normally facilities with small populations, such as Airport District Offices [ADOs], Manufacturing Inspection District Office [MIDOs]/Certificate Management Sections [CMSs], International Field Offices [IFOs], System Support Centers [SSCs], Field Maintenance Programs [FMPs], and System Support Units [SSUs])
FSL 1A	• Airport Sponsor-Owned Federal Contract Towers (FCTs)

* MMAC and WJHTC are considered FSL 4 campuses; however, facilities located within each campus carry their own FSLs and are assessed accordingly.

b. Changing an FSL. A change to the evaluated FSL criteria (see paragraph 3-3) may affect the FSL of a particular facility. For FAA single-tenant facilities, changes in FSL are initiated by the SSE, endorsed by the FM, and approved by AXF-1. For multi-tenant facilities, changes in FSL are initiated by the Facility Security Committee (FSC) and endorsed by AXF. An FSL change also affects the determination of the baseline Level of Protection (LOP) (see paragraph 3-4a). Therefore, the consequences of security investment will be considered and changes to an FSL should be limited to those situations where adjustments to the existing baseline LOP countermeasures would not mitigate the updated facility risk or result in an unnecessary security investment.

3-4. Establishing Security Countermeasures. Once a facility's FSL is determined, AXF then evaluates the specific likelihood (threat) of an ISC-identified undesirable event (UE) occurring at that facility type and the consequences to the mission and/or the NAS that could result from that event. A UE is an incident (e.g., arson, active shooter, theft, workplace violence) directed toward

a federal facility that adversely impacts the operation of the facility, the mission of the agency, or personnel. The ISC's Design Basis Threat (DBT) document is used in a threat evaluation as there is no agency-specific threat assessment published that exceeds the DBT. If agency-specific assessments become available, or local threat information differs from the DBT and evaluated threat, the LOP can be adjusted to reflect the changed threat. Respective countermeasures that are identified in the ISC RMP, along with any additional FAA-identified countermeasures, are then evaluated to determine the degree they reduce facility vulnerabilities and UE risk levels that were identified by the threat and consequence evaluations.

a. Baseline LOP. Those countermeasures that best mitigate the standard UE risk become the baseline LOP criteria. Baseline LOP templates become the security planning starting point for the facility's type and security level.

b. Necessary LOP. As an SSE conducts a facility security assessment (see paragraph 3-5), evaluation of local threats may result in adjustments to the baseline LOP to either mitigate an increased risk or, when threats are lower than initially evaluated, reduce or eliminate a countermeasure. When this occurs, the baseline LOP is adjusted to become the "necessary" LOP for that specific facility. These changes are documented by the SSE in FSRS as Based on Evaluation (BOE) measures. BOEs are initiated by the SSE, endorsed by the FM, and approved by AXF-1. If no adjustments are necessary, the baseline LOP is incorporated as the necessary LOP. The continued need for a BOE will be validated by the SSE during each subsequent assessment.

3-5. Facility Security Assessments. There are three types of facility security assessments: comprehensive, supplemental, and remote security evaluations (RSE). FMs are required to comply with assessment activities.

a. Comprehensive Facility Security Assessments. A comprehensive assessment consists of an on-site examination of the facility and its operations and an evaluation of local threats. The assessment will identify the facility's current LOP by evaluating any deviations between those security countermeasures in effect at a facility and the necessary LOP. It results in a final determination of facility risk levels, documents the facility's existing security countermeasures, and makes recommendations to reduce risks where applicable.

(1) Normally, comprehensive assessments are scheduled every 12 months for FSL 4 and 3 facilities, every 24 months for FSL 2 facilities to include all (staffed and unstaffed) CARSR and ARSR/JSS, and every 36-48 months (as scheduled in FSRS) for FSL 1 and FSL 1A facilities. Where separate facilities are considered co-located, they will be assessed simultaneously at the frequency of the highest FSL. Actual schedules are maintained in FSRS. Comprehensive assessments are not normally conducted for unstaffed facilities, excluding CARSR and ARSR/JSS, unless requested by an LOB/SO because of an unusual security situation.

(2) Prior to the beginning and at the conclusion of a comprehensive assessment, the SSE will brief the FM and facility personnel selected by the FM. During the in-brief the SSE will explain assessment activities, review any unresolved issues from previous assessments, and

request any facility documentation required by this order. During the exit-brief the SSE will review the resulting facility risks, discuss any additional mitigation efforts necessary to reduce specific vulnerabilities, and offer assistance with implementing that mitigation.

b. Supplemental Facility Security Assessments. Supplemental assessments are narrower in scope than the comprehensive assessment. They may be scheduled because of frequent or ongoing security issues at a facility, major construction activities, to verify closure of open findings, or as deemed necessary by the SSE. There is no established frequency for supplemental assessments.

c. Remote Security Evaluations (RSEs). RSEs comprise a virtual assessment of the more critical components of a facility's necessary LOP. SSEs will contact FMs via email, provide a list of targeted security countermeasures, and schedule a time to discuss the countermeasures via telephone or video conversation. RSEs are used to augment comprehensive and supplemental assessments.

d. Assessment Reports. An assessment report will be generated for each type of assessment and will normally be provided to the FM within 45 days of the assessment. The report will summarize assessment activities and provide a table of "findings" and "recommendations" that identify deviations from the necessary LOP. FMs are responsible for taking corrective action to address any "findings" and eliminating deviations from the necessary LOP to the maximum extent possible within the scope of the FM's authority. "Recommendations" are beyond the scope of the FM to correct and are either planned for future implementation through the FST program or will be considered during major renovations, new or renewed leases, or new construction. The fewer deviations that exist, the lower the facility's security risk level.

3-6. Risk Assessment, Management, and Acceptance.

a. Risk Assessment Methodology. The FAA uses a risk assessment tool (RAT) within FSRS to evaluate facility risks. The RAT allows the assessor to compare those countermeasures implemented by the facility against the necessary LOP. Each countermeasure is weighted, within FSRS, and generates a vulnerability score for the associated UE. This vulnerability assessment combined with established threat and consequence determinations (see paragraph 3-3) yields a risk determination of the UE and facility.

b. Risk Management. FMs are required to monitor and correct any deviations from the necessary LOP that are within the scope of the FM's authority. Once corrective action is complete on a recommendation or finding, FMs will notify their SSE to validate and "close" the item within the FSRS database. Recommendations/findings will be noted as closed when the SSE verifies that the required actions have been satisfactorily implemented. Normally, this is done through a supplemental assessment, but it may be accomplished by reviewing documentation (including photographs) provided by the FM. Closing these findings and recommendations further mitigates identified risks. SSEs will review and update the status of open findings at assigned facilities at least semi-annually.

c. Risk Acceptance. Baseline LOPs and their corresponding necessary LOPs, when fully implemented, mitigate facility security risks to an FAA-acceptable level. Deviations, in the form of open "findings" or "recommendations," may increase a facility's risk above the established baseline LOP threshold. As such, semi-annual reports are provided through ASH-1 to the heads of the facility-owning LOBs/SOs (ATO-1, AVS-1, APL-1, ANG-1, and ARP-1) that provide current facility security risk assessments of their facilities. These risk assessment reports document the existing deviations from the necessary LOP that affect the facility risk, indicate why the necessary LOP could not be achieved, and provide an explanation of the strategies in place to eliminate or mitigate the deviations and thereby achieve the risk level associated with the necessary LOP. This reporting facilitates either specific action on the part of the owning LOB/SO, consistent with or in addition to the stated strategy, or, in the absence of that, risk acceptance. As deviations across the spectrum of FAA facilities are constantly in flux, AXF maintains current risk and deviation data that can be made available between reporting timelines as requested.

3-7. Security Design for New Construction, Renovation, and/or Leased Spaces. For each new effort, the sponsoring LOB(s) and the logistics organizations, including Real Estate Contracting Officers (RECOs) and Aviation Property Manager (APM), will provide a point of contact (POC) to interface with the SSE throughout the entire process. As necessary, ASH will provide updates to relevant acquisition management system clauses and lease agreement templates. For ATCTs, see also FAA Order 6480.4, ATCT Siting Process, and Order JO 7110.315, Mobile ATCT Siting Criteria (see also paragraph 4-3). The SSE will partner with the project manager and other POCs to determine the required FSL and establish the baseline LOP. The FSL and LOP will be included in the site design review and become the planning document for the facility security design of these facilities. Where baseline LOP criteria cannot be met, the project documentation must include the associated rationale. The SSE will attend site surveys and conduct site design reviews, contractor acceptance inspections/joint acceptance inspections, and other meetings as necessary. An assessment, based on the site design review, will be conducted once the construction is complete.

a. Lease Renewals. In the case of lease renewals, the SSE will provide the RECO and APM with a risk assessment and any necessary mitigation strategies. Any associated facility security risks that cannot be mitigated or accepted by the occupying LOB will be addressed with the lessor during lease renewal negotiations and may inform a decision to terminate the lease and seek a different facility.

b. Guidelines for Selecting Leased Space. In buildings housing multiple external organizations, avoid separating FAA offices throughout the building. Access to FAA-controlled space will be restricted as identified in chapter 4 of this order. Attempt to obtain leased space with entities having similar security needs. Where possible, do not locate FAA personnel in buildings housing high-risk departments or agencies, i.e., other tenants whose mission and interaction with certain segments of the public are adversarial in nature. Examples of high-risk tenants include criminal and bankruptcy courts and law enforcement agencies (e.g., FBI, ATF, DEA) that routinely attract the attention of dangerous groups.

c. Renovations. When renovations to an existing facility are planned, the previous security assessment must be reviewed to determine if any existing deviations from the necessary LOP can be eliminated with the renovation planned. Mitigating any existing security risks must be included in the facility design to the extent possible.

3-8. Facility Security Information. ASH maintains the Facility Security Reporting System (FSRS) database that stores data related to the FSMP.

Chapter 4. Facility Security Countermeasures

4-1. Purpose. This chapter establishes baseline Level of Protection (LOP) countermeasure templates for staffed facilities based on their facility security level (FSL) and the evaluation of the threats and consequences of undesirable events (UE) as related to the facility's critical infrastructure (CI) or administrative functions. This chapter also describes the implementation considerations for each countermeasure or FAA-prescribed security measure that is associated with that countermeasure. Funding for identified countermeasures has a variety of sources. Security system requirements are typically funded through the Facility Risk Management Program administered by ATO/AJW. Security requirements associated with new construction should be included in project funding. Other requirements are provided for through FAA/LOB Operations Accounts. ASH can assist LOBs in developing or advocating for any necessary discretionary increase requests.

4-2. Using the Baseline LOP Templates. Sections 1 through 7 of this chapter identify baseline LOP criteria for the majority of FAA CI and administrative facilities. See paragraph 3-4 for more information on developing LOPs. The baseline countermeasures for each specific FSL are identified with an "X" within the tables, and the term "reserved" is used where the countermeasure doesn't apply. The paragraphs located below each table are used to provide additional information about the countermeasure. If no additional information is necessary, "no additional measures beyond those specified in the table" will appear in the paragraph.

4-3. Unique Facilities. The FAA inventory has several facility types that are unique. Risk reduction for these facilities is not adequately or efficiently achieved by the broad baseline LOP templates described in the respective tables to this chapter. For example, Appendix C to the ISC's Risk Management Process identifies five different federal facility and childcare center relationship scenarios that alter baseline LOPs for these facilities. The FAA employs at least three of those identified relationships. Adjustments to the baseline LOP criteria for these facilities are provided in the following appendices to this order:

Table 4-1. Non-Standard FAA Facilities

Facility Type	Location
Flight Standards District Offices (FSDO)	Appendix C
FAA-sponsored Child Care Centers (CCC)	Appendix D
MMAC and WJHTC Centers	Appendix E
ARSR-JSS and CARSR	Appendix F
Sponsor Owned / Leased Federal Contract Towers (FCT)	Appendix G
Mobile Asset Deployment Centers (MADC)	Appendix H

4-4. Temporary, Mobile, and Modular Assets or Facilities. Other than mechanical and cipher locks on access doors (see paragraph 4-3-13b(3)), security requirements for FAA mobile and modular assets as well as temporary structures will be unique, based on the type of asset and the deployment environment. The SSE and the project engineers, working with the Mobile Asset Sustainment Program of ATO, must identify the protective measures required. In some cases, the use of Contract Security Officers (CSOs) may be required to ensure personnel and material

safety. Additional temporary services of CSOs must be coordinated with the FST Program Manager.

4-5. SSE Security System Verification and Approval. The SSE will review and concur on all security system designs (including, but not limited to, lighting, intrusion detection, video surveillance system [VSS], access controls) prior to their initial installation or upgrade. Prior to occupancy or after installation, SSEs will ensure that installed security systems are operational and consistent with all applicable requirements.

Chapter 4. Facility Security Countermeasures

Section 1. Site Security Countermeasures

4-1-1. Countermeasure Matrix. The following matrix identifies the site security baseline LOP criteria for each FAA facility based on the facility's FSL and classification (Critical Infrastructure [CI] or Administrative).

Table 4-1-1. Facility Site Security Countermeasures

Site Security Criteria	Para	CI - FSL					Admin - FSL		
		1	2	3	4		1	2	3
Identification of a Federal Facility	4-1-2								
Post U.S. property signs (FAA-owned, direct-leased, or GSA-leased facilities)		X	X	X	X				X
Landscaping	4-1-3								
Minimize areas of concealment in and around facilities		X	X	X	X		X	X	X
Establish a 20-foot clear zone outside the fence		X	X	X	X				
Establish a 20-foot buffer zone inside the fence		X	X	X	X				
Trim vegetation so it does not interfere with visibility or systems (e.g., VSS, security lighting)		X	X	X	X				X
Pedestrian Access to Site	4-1-4								
Install landscaping and other barriers to channel pedestrians to authorized entrances									X
Install fence to channel pedestrians to authorized entrances		X	X	X	X				
Vehicle Access Points	4-1-5								
Limit the number of vehicle access points		X	X	X	X				X
Monitor access points with VSS (Refer to Table 4-5-1)			X	X	X				X
Site Lighting	4-1-6								
Perimeter lighting				X	X				
Entrances and exits		X	X	X	X		X	X	X
Parking lots and garages			X	X	X			X	X
Walkways from parking lots to entrances				X	X				X
Restricted Areas and Significant Areas and Assets	4-1-7	Where Present							
Prevent unauthorized entry		X	X	X	X		X	X	X
Secure exterior critical cables hung less than 12 feet from ground		X	X	X	X		X	X	X
Secure exterior ladders that access critical equipment, roofs, or facility access points		X	X	X	X		X	X	X
Signage – Sensitive Areas	4-1-8								
Post "Restricted area" signs		X	X	X	X		X	X	X
Control of Parking	4-1-9								
Control vehicle access to on-site parking		X	X	X	X				X
Authorized Parking	4-1-10								
Limit parking to employee and government vehicles				X	X				
Post signage to keep visitor parking furthest from the facility		X	X						X
Vehicle Access to Controlled Parking	4-1-11								
Use vehicle gates to limit access to authorized vehicles		X	X	X	X				X

Site Security Criteria	Para	CI - FSL					Admin - FSL		
		1	2	3	4		1	2	3
Vehicle Barriers	4-1-12								
Provide vehicle barriers to protect pedestrian entrances				X	X				X
Provide vehicle barriers to protect vehicle access points				X	X				
Provide vehicle barriers to protect critical areas/utilities				X	X				
Vehicle Screening	4-1-13								
Screen visitor vehicles before allowing access to controlled perimeter				X	X				X
Pedestrian Access to Controlled Parking Areas	4-1-14								
Provide barriers to restrict pedestrian access to authorized entry points		X	X	X	X				
Monitor pedestrian access to parking areas using CSOs				X	X				X
Monitor pedestrian access to parking areas using VSS				X	X				X
Hazardous Materials (HAZMAT) Storage	4-1-15								
Store HAZMAT in a restricted area away from loading docks, entrances, and uncontrolled parking			X	X	X			X	X
Receptacle and Container Placement	4-1-16								
Place receptacles and containers away from building entrances or other vulnerable locations			X	X	X			X	X

4-1-2. Identification as a Federal Facility. "U.S. Property – No Trespassing" signs must be posted so that they are visible from the exterior side of fences and the main gate at 50-foot intervals. On buildings without fences, post the signs where they are plainly visible to anyone approaching the facility. See paragraph 4-3-3 for additional sign requirements and procurement information.

4-1-3. Landscaping. For fenced areas, objects within clear or buffer zones that do not present a climbing aid and do not interfere with VSS functions or CSO operations are permitted. In situations where the FAA does not own or control the property outside the perimeter fence to maintain the clear zone, the FM must work with the SSE to mitigate the deviation.

4-1-4. Pedestrian Access to Site. The number of pedestrian gates used to access the controlled perimeter or facility will be the minimum required for operations. See also paragraph 4-3-13b.

a. Perimeter Fencing. Facilities located within airport perimeter fences or border perimeters that are already protected by fences, such as an active military base or any secure, government-controlled property, or are attached to the terminal building of an airport, may make use of those barriers without further fencing installation. Perimeter fencing consists of a 7-foot-high, 9-gauge woven aluminum-coated steel or galvanized steel wire fabric with mesh openings not larger than 2 inches per side and a 1-foot-high outward-facing top guard consisting of 3 strands of galvanized barbed wire set at an outward angle of 45 degrees for a total of 8 feet above grade. Construction of FAA security fences and gates will comply with Federal Supply Service, Federal Specification RR-F-191K, Fencing, Wire, and Post Metal (and Gates, Chain-Link Fence Fabric, and Accessories) (General Specification), Federal Specification Sheets RR-F-191-1E through 4E, and American Society for Testing and Materials (ASTM) F567-07, Standard Practice for Installation of Chain-Link Fence.

b. Temporary Security Fence Requirements. Temporary fencing does not have to meet FAA standard fence requirements, but the temporary fence quality must be adequate and reasonable for the intended purpose and function. The temporary security fence must be equal in height to the permanent fence to which it connects (e.g., a 4-foot fabric anchored to a 4-foot Jersey barrier equals 8 feet and meets this requirement), must minimize gaps, and be affixed to objects or anchored to ensure it cannot be easily moved or bypassed. Park or store construction equipment outside the clear zone or far enough away to preclude its use as a climbing aid when not in use. See also paragraph 3-4 regarding waivers.

4-1-5. Vehicle Access Points. Restrict the number of vehicle access points to the minimum required for operations.

4-1-6. Site Lighting. For existing facilities, lighting is intended to illuminate potential areas of concealment, enhance the observation of CSO patrols and VSSs, and provide for the safety of personnel. Lighting is provided to ensure VSS video images can be used to identify a clear description of the person and any activity they may be engaged in. Perimeter lighting should light FAA property only and light poles located so they don't provide a climbing aid or are easily reached and disabled. For new construction and new leases, follow the security lighting levels as indicated in the below table. The illumination lighting level measurements are taken at the point where the light is needed and not from the light source.

Table 4-1-2. FAA Security Illumination

Facility Area	Lighting Level
Perimeter Fence (to include clear/buffer zone)	Not less than 0.5-foot candles (FC) (Not to exceed 1 (FC)
Parking Areas	Not less than 0.8 FC
Parking Garages	Not less than 1 FC
Entrance Gate at Guardhouse	Not less than 10 FC
Building Entrances	Not less than 5 FC
Exterior Facility Lighting not addressed above	Not less than 0.5 FC

Security lighting will be connected to emergency power systems where available and as required by local fire and safety codes. Alternate power sources, such as solar power, may be used to provide backup power if traditional power capacity is not available. Care must be taken that sensor-activated lighting designs do not affect any adjacent sensors.

4-1-7. Restricted Areas and Significant Areas and Assets. Access will be controlled by either FAA standard locks or their equivalents (see paragraph 4-3-13b). Additional controls may be required as indicated elsewhere in this order. Exterior critical cables will be protected by either fencing or metal cladding or surveillance where security officers are employed. Cables configured in cable runs behind walls or ceilings do not need additional measures. Critical items such as antennas located in non-public areas (e.g., on catwalks, on rooftops, or mounted above 18 feet from the ground) are considered protected by their location.

4-1-8. Signage – Sensitive Areas. Signage will be displayed consistent with the operations conducted at each facility. See paragraph 4-3-3 regarding regulatory signage.

4-1-9. Control of Parking. Designate employee and visitor parking areas and use vehicle gates to limit access to authorized vehicles only (see paragraph 4-1-11). Post vehicle towing signs (see 4-1-11) that reflect towing at the owner's expense at vehicle entrances. Towing signs must comply with local ordinances and state law. Visitor parking and towing signs must be locally procured. "Reserved" parking signs that indicate the presence or positions of government employees should be avoided when local threat conditions warrant. Other parking signs may be used at the FM's discretion.

4-1-10. Authorized Parking. Drive-up and drop-off areas for deliveries and other purposes are allowed. FAA personnel must not use FAA parking areas/grounds to store or reside in personal vehicles. Subject to specific threats or operational needs, FAA personnel may temporarily park personal vehicles on FAA property while they are not working (e.g., personal, official travel, temporary duty). Only vehicles that are legal to operate in the jurisdiction where the facility is located are authorized to park on FAA property. Facilities will establish procedures for the towing of unauthorized vehicles and detail those procedures in the FSP. Local towing companies may be used for this service.

4-1-11. Vehicle Access to Controlled Parking. All vehicle occupants will be identified and either allowed access based on presenting an acceptable ID (PIV) card or processed as a visitor. FMs may implement vehicle ID systems to assist in parking controls; however, vehicle ID media may not be used for access control. Access can only be granted based on an acceptable form of ID (PIV card). See paragraphs 4-3-4b and 4-5-2 for physical access control system (PACS) and video surveillance system (VSS) requirements. Vehicle gates:

a. Will be located so that they do not impede traffic on adjacent public thoroughfares during ID checks.

b. May use lighter framing consistent with gate operation but will maintain the structural integrity of the fence (where installed). When part of a perimeter fence, gate hardware will be secured and gaps from firm ground to gate are limited to four (4) inches (see paragraph 4-1-4 for fencing requirements).

c. Will either be locked when not in use or controlled by CSOs or electronic gate mechanisms supported using gate control video (GCV) where required. The use of a shrouded shackle padlock is preferred where available and the gate mechanism will permit. A high-security padlock will be used with the shortest length of chain needed. The use of multiple mechanical padlocks or electronic lock cylinders/programmable smart keys to accommodate service personnel will only be permitted at unstaffed facilities.

d. That are equipped with electronic gate controls will include a manual disconnect for use during power outages. Automatic exit devices must be adjusted to be only as sensitive as needed for dependable operation. A manual exiting device (i.e., push button) may be used; however, they will not be located closer than 15 feet from the perimeter fencing/gate. Gate-controlling mechanisms will be located on the inside of the perimeter fencing/gate.

4-1-12. Vehicle Barriers. Site traffic patterns should be designed to prevent high-speed approaches by vehicles and use barriers to mitigate the risk of vehicular impact.

4-1-13. Vehicle Screening. Vehicle screening is a visual inspection of areas large enough to conceal a device or weapon, such as the trunk, under the hood, inside the passenger compartment, glove compartment, or the vehicle's undercarriage. While only visitor vehicles are routinely screened, all personnel, vehicles, and property entering a facility, including persons possessing FAA-approved ID media, may be subject to additional screening at the vehicle checkpoint to ensure the safety and security of all persons entering the facility. Additional procedures for delivery vehicles will be published in the FSP and CSO post orders and will include verification of the bill of lading, origin, and destination; POC notification; and inspection and escort requirements. Refusal to submit to a vehicle inspection will result in denial of entry.

4-1-14. Pedestrian Access to Controlled Parking Areas. Limit the number of entrances to the extent practical.

4-1-15. Hazardous Materials (HAZMAT) Storage. No additional measures beyond those specified in Table 4-1-1.

4-1-16. Receptacle and Container Placement. No additional measures beyond those specified in Table 4-1-1.

Chapter 4. Facility Security Countermeasures

Section 2. Structure Security Countermeasures

4-2-1. Countermeasure Matrix. The following matrix identifies the structure security baseline LOP criteria for each FAA facility based on the facility's FSL and classification (Critical Infrastructure [CI] or Administrative).

Table 4-2-1. Structure Security Countermeasures

Structure Security Criteria	**Para**	**CI – FSL**					**Admin - FSL**		
		1	2	3	4		1	2	3
Blast Resistance - Windows	4-2-2								
Exterior setback – 125 feet				X	X				
Glass fragmentation film or glazing systems to reduce glass fragmentation hazard									X
Blast Resistance – Façade and Structure	4-2-3								
Exterior setback – 125 feet				X	X				
Controlled Perimeter		X	X						
Blast Resistance – Progressive Collapse	4-2-4								
No special measures required for existing facilities									
Blast Resistance – Under Building Parking	4-2-5								
No special measures required for existing facilities									
Burglary Resistance of Windows	4-2-6								
Locked ground floor and/or readily accessible windows (within 16-feet of ground)		X	X	X	X		X	X	X
Intrusion Detection System (IDS) requirements	4-5-6	See Table 4-5-1							
Walls and Non-window Openings	4-2-7								
Floor-to-ceiling walls on perimeter of leased space							X	X	X
Secure openings 96 square inches or greater		X	X	X	X		X	X	X
Windows in Critical Areas – Ballistic Protection	4-2-8								
Reserved									
Protection of Air Intakes	4-2-9								
Secure accessible air intake grilles from tampering or removal		X	X					X	
Protect accessible air intakes with fencing				X	X				X
Monitor with VSS or CSO patrols				X	X				X
Isolated Ventilation Systems	4-2-10								
Provide separate isolated HVAC systems in lobbies, loading docks, and mail rooms				X	X				X
Loading docks and mailrooms are full-height construction and sealed to floor and ceiling					X				
HVAC Control	4-2-11								
Written procedures for emergency shutdown of exhaust & air handling systems		X	X	X	X		X	X	X
Install emergency shutoff and exhaust system for air handlers				X					X
One step shut off and exhaust system					X				
Control movement of elevators				X	X				X
Chemical, Biological, Radiological (CBR) Detection Technology	4-2-12								

Structure Security Criteria	Para	CI – FSL					Admin - FSL		
		1	2	3	4		1	2	3
Reserved									
Biological Filtration – General Building	4-2-13								
MERV 10 filters on exterior air handling units				X					X
MERV 13 filters on all air handling units					X				
Biological Filtration – Lobbies and Mailrooms	4-2-14								
MERV 13 filters on all air handling units in lobbies and mailrooms				X	X				X
Chemical Filtration	4-2-15								
Reserved									
Security of Ventilation Equipment and Controls	4-2-16								
Protect systems from unauthorized access		X	X	X	X				X
Equip control room doors with electronic PACS				X	X				
Location of Utilities and Feeders	4-2-17								
Reserved									
Separation of Emergency and Normal Power Distribution	4-2-18								
Reserved									
Emergency Generator Protection	4-2-19								
Access controlled and limited to duty essential		X	X	X	X				X
Located within a controlled perimeter		X	X	X	X				
EG and fuel tank secured from unauthorized access		X	X	X	X				
Protection of Water Supply	4-2-20								
Reserved									

4-2-2. Blast Resistance – Windows. Blast resistance is achieved either through setback for critical infrastructure or through performance validation by a certified blast consultant for administrative facilities. Acceptable window glazing systems include thermally tempered glass and thermally tempered, heat strengthened, or annealed glass with fragment retention film installed on the interior surface (edge-to-edge, wet glazed, or daylight installations are acceptable).

a. Setback. For the purposes of determining blast mitigation of the design basis threat (DBT) for critical infrastructure, exterior setback is used. Exterior setback is the distance from the face of the facility's or building's exterior (the building's skin) to the uncontrolled perimeter accessible by any motorized vehicle. Facilities that maintain a minimum 125-foot exterior setback will satisfy blast mitigation standards for the defined DBT.

b. Blast Resistance Analysis. A blast resistance design analysis is not required for existing FSL 3 administrative facilities but would be required for new construction or for existing buildings undergoing a major structural renovation. The blast analysis must either be on file from or conducted by a blast consultant with demonstrated experience in industry-accepted blast design practices that validate the facility meets the LOP.

4-2-3. Blast Resistance – Façade and Structure. The setback and blast resistance analysis established in paragraph 4-2-2 apply. For critical infrastructure where setback doesn't apply, the existence of a controlled perimeter mitigates the risk. For new construction at FSL 2 CI facilities, the design must include the use of construction materials that have inherent ductility and that are

able to respond to load reversals. For FSL 3 administrative facilities undergoing façade and/or window modifications or for new construction, the facility must provide a LOP in accordance with the American Society of Civil Engineers (ASCE) 59.

4-2-4. Blast Resistance – Progressive Collapse. There are no progressive collapse requirements for existing FAA facilities. However, requirements may apply for new FSL 3 administrative facilities. These requirements will be determined through the design process established in paragraph 3-7.

4-2-5. Blast Resistance – Under-Building Parking. There are no under-building parking blast requirements for existing FAA facilities. Requirements for new construction of FSL 2 and above facilities that will have under-building parking will be determined through the design process established in paragraph 3-7.

4-2-6. Burglary Resistance of Windows. Protect windows from unauthorized entry by a locking mechanism and, where required, monitor with Intrusion Detection System (IDS) (see Table 4-5-1). All windows, their supporting frames and wall attachments, and all hardware will be heavy-duty builder's material and use comparable construction techniques. Windows that are within 16 feet of the ground, or are readily accessible, will:

a. Have any exterior hinges and mounts modified to prevent removal;

b. Have an effective latching or locking mechanism; and

c. Be closed and locked when the room or surrounding area is not attended.

4-2-7. Walls and Non-window Openings. True floor-to-ceiling walls or, where not possible, an equivalent barrier (e.g., wire mesh, steel screen) will be attached to the existing perimeter wall. These true floor-to-ceiling walls will delineate leased from non-leased space in multi-use leased facilities. Openings of 96 square inches or greater that have a lesser dimension of 6 inches or more will be secured through any combination of substantial grates or screens, tamper-resistant screws, utility hole liner locking devices (as used by servicing utility companies), or the FAA standard lock system.

4-2-8. Windows in Critical Areas – Ballistic Protection. Reserved.

4-2-9. Protection of Air Intakes. No additional measures beyond those specified in Table 4-2-1.

4-2-10. Isolated Ventilation Systems. No additional measures beyond those specified in Table 4-2-1.

4-2-11. Heating, Ventilating, and Air Conditioning (HVAC) Control. HVAC equipment rooms will be secured to prevent unauthorized entry (see paragraph 4-4-4a).

4-2-12. CBR Detection Technology. Reserved.

4-2-13. Biological Filtration – General Building. To the extent current HVAC systems allow, facilities will meet established Minimum Efficiency Reporting Value (MERV) ratings identified

in Table 4-2-1. Appropriate MERV filters must be planned when considering HVAC upgrades or new facility construction. Existing MERV ratings will be documented in the facility assessment report.

4-2-14. Biological Filtration – Lobbies and Mailrooms. See paragraph 4-2-13.

4-2-15. Chemical Filtration. Reserved.

4-2-16. Security of Ventilation Equipment and Controls. See Table 4-4-1 and paragraph 4-4-4.

4-2-17. Location of Utilities and Feeders. Reserved.

4-2-18. Separation of Emergency and Normal Power Distribution. Reserved.

4-2-19. Emergency Generator Protection. See Table 4-4-1 and paragraph 4-4-4.

4-2-20. Protection of Water Supply. Reserved.

Chapter 4. Facility Security Countermeasures

Section 3. Facility Entrance Countermeasures

4-3-1. Countermeasure Matrix. The following matrix identifies facility entrance baseline LOP criteria for each FAA facility based on the facility's FSL and classification (Critical Infrastructure [CI] or Administrative).

Table 4-3-1. Facility Entrance Security Countermeasures

Facility Entrance Security Criteria	**Para**	**CI – FSL**					**Admin - FSL**		
		1	2	3	4		1	2	3
Badge Identification (ID) System	4-3-2								
Wear DOT/FAA ID Media (excluding FSL 1 and 2 facilities with less than 10 personnel)		X	X	X	X		X	X	X
Regulatory Signage	4-3-3								
"No weapons" signs posted at all gates and building entry points		X	X	X	X		X	X	X
"Notice of inspection" signs posted at all public gates and entry points		X	X	X	X		X	X	X
"VSS warning" signs where VSS is in use		X	X	X	X		X	X	X
"X-Ray warning" signs where X-ray machines are in use		X	X	X	X		X	X	X
"Restricted area" signs posted at interior entrances into critical areas		X	X	X	X		X	X	X
"Closed area" signs posted at interior entrances to closed areas		X	X	X	X		X	X	X
Employee Access Control	4-3-4								
Utilize PACS to control access to employee entrance doors			X	X	X			X	X
PIV card readers on exterior doors			X	X	X			X	X
PIV card readers on vehicle gates			X	X	X				X
PIV card readers on doors protecting critical administrative areas				X	X				X
PIV card readers on doors protecting critical operations areas	4-4-4		*	X	X				X
Mechanical push-button or electronic keypads at control room doors (in addition to standard locks)	4-4-4	X							
Verify the identity of persons prior to allowing access			X	X	X			X	X
Grant unescorted access only to personnel possessing DOT/FAA ID media		X	X	X	X		X	X	X
Visitor Access Control	4-3-5								
Ensure visitors are sponsored and escorted		X	X	X	X		X	X	X
Issue temporary visitor ID badges and require them to be worn by visitors		X	X	X	X		X	X	X
Log visitors on the DOT/FAA Visitor Register (FAA Form 1600-8) or equivalent		X	X	X	X		X	X	X
Occupant Screening	4-3-6								
Prohibited items		X	X	X	X		X	X	X
Controlled items		X	X	X	X		X	X	X
Visitor Screening	4-3-7								
Screen visitors and their property with X-ray machines and metal detectors				X	X				X
Ballistic Protection at Screening Locations	4-3-8								
Reserved									
Lobby Queuing	4-3-9								

Facility Entrance Security Criteria	Para	CI – FSL					Admin - FSL		
		1	2	3	4		1	2	3
Reserved									
After Hours Access Control	4-3-10								
Require FAA employees to sign in and out after hours using a locally designed register									X
Limit Building Entry Points	4-3-11								
Keep the number of access doors to a minimum to support operations		X	X	X	X		X	X	X
Entrance Co-location	4-3-12								
Reserved									
Perimeter Doors and Door Locks	4-3-13								
Limit number of perimeter doors used to access a facility		X	X	X	X		X	X	X
Door construction standard		X	X	X	X		X	X	X
BHMA Grade 1 Hardware		X	X	X	X		X	X	X
Install interior mounted hinges or modify to prevent removal on exterior doors		X	X	X	X		X	X	X
Equip perimeter doors and critical operational area doors with latch guards or astragals		X	X	X	X		X	X	X
Equip all doors with FAA standard locking system		X	X	X	X		X	X	X
Install request-to-exit device for egress			X	X	X			X	X
Control of Keys and Access Media	4-3-14								
Implement a formal key control program									
Designate a key control officer in writing		X	X	X	X		X	X	X
Maintain a record of the total number of keys and cores, number issued, and on hand; number of lost/missing or destroyed keys		X	X	X	X		X	X	X
Conduct an annual inventory of keys and cores		X	X	X	X		X	X	X
Keep unissued keys in a locked container		X	X	X	X		X	X	X
Report lost access media and keys		X	X	X	X		X	X	X
Immediately terminate access rights associated with lost electronic access media		X	X	X	X		X	X	X
Change cipher lock and other combination codes after personnel changes or compromise		X	X	X	X		X	X	X
Employee Convenience Doors	4-3-15								
Refer to paragraphs 4-3-11 and 4-3-12									
Emergency Exit Doors	4-3-16								
Use compliant life-safety emergency exit hardware		X	X	X	X		X	X	X
Monitor emergency exits with visual, electronic, or audible alarms		X	X	X	X		X	X	X
Delayed Egress	4-3-17								
Reserved									

*Applies to Tier 1 facilities as specified in FSRS.

4-3-2. Badge Identification System.

a. Wear and Use of Identification (ID) Media. Issued DOT/FAA ID media will be contained in the FAA-approved Federal Information Processing Standard (FIPS)-compliant shielded carrier and worn on the front of a person, above the waist and below the neck, uncovered by clothing with the picture facing out (to allow others to visually validate it) while on FAA property, unless the bearer is currently using it to access a computer system they are actively working with. Those individuals working in hazardous areas, including flight lines or other areas where safety factors must be addressed, must be provided with ID media holding devices that permit the display of the identification and meet the requirements of FAA Order

1600.78, Personal Identity Verification (PIV) Cards and Other Identification Cards. FAA personnel at FSL 1 and 2 facilities with fewer than 10 personnel assigned are not required to wear ID media unless required by local security procedures; however, they must have it in their possession.

b. Temporary Employee ID Media. Temporary employee ID media is required to be worn by all FAA personnel who do not have their issued DOT/FAA ID media with them but require unescorted access to the facility. Temporary employee IDs consist of either the "Temporary PIV" card found in FAA Order 1600.78 and issued where facilities have PIV-trusted agents or paper stock IDs provided by AXF. The temporary employee ID must be worn in the same manner as a standard DOT/FAA ID. If paper stock temporary employee IDs are used, they will be tracked on the facility's DOT/FAA Visitor Register (FAA Form 1600-8). Paper stock temporary employee IDs will be dated with the day they are issued and, unless otherwise allowed (see Appendix E), will expire at the end of the issued date.

c. Requesting and Controlling Temporary Employee ID Media.

(1) FMs, or a designee, must request temporary employee ID media stock from their SSE.

(2) SSEs must issue the temporary employee media stock in serialized blocks and record the range of serial numbers and the date issued for all badges distributed to the responsible individual.

(3) Temporary employee ID media stock must be sent via certified mail, return receipt requested, or other commercial carrier with a package tracking capability.

(4) Temporary employee ID media stock must be stored in a locked filing cabinet or other locked container approved by the SSE.

(5) The FM must report lost or stolen temporary employee ID media stock to the SSE immediately and via the Web-Based Incident Reporting System (WebIRS) (see paragraph 4-6-9b).

d. Loss of ID Media. FAA personnel must report lost FAA-issued ID media to their manager as soon as possible. An incident report must be completed in accordance with paragraph 4-6-9b. Provisions for ID replacement are contained in FAA Order 1600.78. Upon notification, FMs must also ensure that access rights associated with the lost ID media are removed from any existing physical access control system used in the facility within 24 hours.

4-3-3. Regulatory Signage. "No Weapons" and "Notice of Inspection" signs will be displayed at gates and building entry points of staffed facilities. Other listed signs will be installed where systems are in use or on or adjacent to access points of protected areas. The use of bilingual signs will be determined by the FM in consultation with the SSE based on the needs of the local population. Certain signs may be ordered from the Logistics Center Support System (LCSS). Call Customer Care at 405-954-3793 or email at Customer-Care@faa.gov.

Table 4-3-2. FAA Signage Available from the Logistics Center Support System

Description	LCSS Part Number	National Stock Number
U.S. Property – No Trespassing (Plastic)	005592971	9905-00-5592971
U.S. Property – No Trespassing (Aluminum)	015197338	9905-01-5197338
No Weapons (18x24 Metal)	015064142	9905-01-5064142
No Weapons (8.5x11 Plastic)	015064148	9905-01-5064148
Notice of Inspection (NOI) (18x24)	014989598	9905-01-4989598
Notice of Inspection (NOI) (8x11)	015383541	9905-01-5383541
CCTV Warning (Warning – This Facility Is Under 24 Hour Surveillance)	014777224	9905-01-4777224
CCTV Warning (Warning – This Facility Is Under 24 Hour Surveillance) (Spanish/English)	014802154	9905-01-4802154
X-Ray Warning (Warning – X-Ray Machine in Operation)	014777225	9905-01-4777225
X-Ray Warning (Warning X-Ray Machine in Operation) (Spanish/English)	014802421	9905-01-4802421
Restricted Area (Restricted Area – Authorized Personnel Only)	014763025	9905-01-4763025
Restricted Area (Restricted Area – Authorized Personnel Only) (Spanish/English)	014802489	9905-01-4802489
Closed Area - (Closed Area Authorized Personnel Only)	014802156	9905-01-4802156
Closed Area - (Closed Area Authorized Personnel Only) (Spanish/English)	014802487	9905-01-4802487

4-3-4. Employee Access Control.

a. Facility Access. FMs have final authority over who is authorized to enter their facility. Generally, persons possessing valid DOT/FAA ID media as defined in FAA Order 1600.78 or other federal agency-issued PIV (or equivalent) cards (e.g., military liaisons and National Oceanic and Atmospheric Administration (NOAA) weather observers) are granted unescorted access to facilities and spaces where they are assigned to work. All persons issued DOT/FAA ID media that allows unescorted access to FAA facilities must have a favorably adjudicated Tier 1 or higher background investigation on record, or the initiation and favorable review of all forms of the Tier 1 or higher background investigation, and a favorably adjudicated FBI Fingerprint National Criminal History Check. Non-employees are persons who are neither an FAA employee nor a contractor employee (e.g., childcare parents, carpoolers, fitness center employees). These persons, by agreement with the FAA, have limited access to FAA facilities and are subject to the specified requirements in FAA Order 1600.1, Personnel Security Program. FMs may extend this privilege to other DOT or non-assigned FAA employees with valid DOT/FAA ID media on a case-by-case basis as mission needs require. During periods of heightened security, all personnel and their vehicles may be subject to inspection. AXF will notify facility personnel of the reason for any heightened security as soon as practical unless restricted by the need to protect sensitive or classified information or to protect ongoing investigations or law enforcement operations.

(1) FMs must establish procedures that ensure a secure employee entrance and enable identification verification prior to allowing access. CSOs are authorized to require individuals who are attempting to access FAA facilities to hand the CSO their ID card for closer visual or electronic verification of the card. FAA personnel must comply if so requested. Where CSOs are

not present, a PIV-compliant physical access control system (PACS) is used where indicated in the LOP criteria. If a PIV-compliant or other electronic PACS is not feasible at certain FAA administrative facilities, alternate access control procedures must be developed and documented in the FSP. At CSO-controlled perimeters, each employee's ID must be verified prior to entry, regardless of how many occupants are in the vehicle (e.g., no "piggybacking" or "tailgating" is allowed).

(2) FMs may require FAA personnel who are not assigned to the facility but have been granted access to sign in and out on a building register (if the electronic access control system will not accommodate) to ensure they can be located and evacuated in the event of an emergency. The Visitor Register, FAA Form 1600-8, may be used.

b. Physical Access Control System (PACS). PIV cards using electronic card readers, access cards using PIV-compatible technology where PIV cards are not issued to an individual but physical access is still required, or other electronic card entry systems where PIV-compliant readers are not available provide a PACS for FAA facilities. Single-factor card readers (SFCRs) that reach the end of their life cycle will be replaced with multi-factor card readers (MFCRs). A MFCR offers the capability for an FM to increase the access control security of the facility by requiring a PIV card and either a PIN or a biometric (fingerprint), or both, as additional identification verification. These additional capabilities may be leveraged in the future during periods of heightened security. *Note: Under long-standing agreements with Bargaining Units, PACS and VSS will not be used for monitoring employees or for time-keeping purposes. Any use or release of PACS and VSS data in relation to the imposition of discipline must be subsequent to an official investigation. See FAA Order 1600.38, Office of Investigations (AXI) Duties and Investigative Responsibilities, for additional information.*

(1) New Installation or Replacement of PACS. Any new or replacement systems must be PIV compliant and comply with Homeland Security Presidential Directive 12 (HSPD-12) and current Federal Information Processing Standard 201 (FIPS-201) requirements. For facilities with a PACS at both controlled perimeters and on facility doors, PIV certificate validation need only occur at the facility door. When integrated with an IDS, a PACS provides an equivalent alarm notification. Perimeter doors or gates equipped with electronic or electro-mechanical entry systems must be designed to remain locked from the outside (to prevent entry) during power loss but still allow emergency exit for personnel. Designers must adhere to local and national fire and safety codes and standards, as applicable, which supersede this requirement, in the event a conflict exists. PACS will be equipped with an uninterruptible power supply capable of providing a minimum of four (4) hours of backup power and, where possible, be connected to the critical power supply (emergency generator). Doors that have a PACS installed must also be equipped with a manual locking system (see paragraph 4-3-13b).

(2) Temporary Electronic Physical Access Cards. To facilitate access through doors controlled by a PACS, temporary physical access cards may be issued to an employee who does not have their permanently issued access card (e.g., PIV card or temporary PIV card) with them once the identity of the employee has been verified. Temporary physical access cards must be returned once the employee has completed their required duties/shift. The access cards must not

be removed from the facility. Temporary electronic physical access cards will be controlled as required in paragraph 4-3-14.

(3) PACS Review. Employees will be allowed only those access privileges needed to accomplish assigned duties. Where feasible, FMs should consider implementing time-defined access control restrictions. Changes to access authorities (e.g., transfer, retirement, position change) must be updated in the system within 24 hours. Where not automated (through physical security enterprise management system (PSEMS) or PAD/PACS integration), the FM must review the personnel access privileges quarterly.

4-3-5. Visitor Access Control. A visitor is any individual not possessing valid DOT/FAA ID media. FMs approve visitor access. Visitors must be sponsored by an FAA employee or FAA contractor, have a sanctioned reason for the visit, produce current government-issued photo identification that has an expiration date, sign in on a visitor's log, be under continuous escort by personnel possessing valid DOT/FAA ID media, and properly display an FAA visitor badge while at the facility. Facility visitor controls must be included in the FSP.

a. Escort Requirements. Visitors must always be escorted while in the facility or on controlled facility property. An FAA employee or contractor will maintain visual and voice control over visitors under escort. For larger visitor groups, a sufficient number of escorts must be assigned in order to properly monitor and control visitor conduct and movement. Information access must be commensurate with the purpose of the visit; must comply with all applicable law and policy related to the type(s) of information involved, including those related to export controls and the protection of classified and controlled unclassified information (CUI); and must be considered before the visit is approved. See FAA Order 1240.13, Export Control Compliance; FAA Order 1600.2, Classified National Security Information (CNSI); FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI); and FAA Order 1370.121, FAA Information Security and Privacy: Policy, and its supplemental implementing directives, for additional information. Procedures must be instituted that eliminate any casual access to sensitive information or operations during a visit. While under escort, a visitor is not deemed to have been "granted access" to the facility.

b. Visitor Logs. All visits will be logged in on the DOT/FAA Visitor Register, FAA Form 1600.8, or electronic equivalent. The log must record the name of the visitor and the organization or company they represent, the visitor's sponsor's name, the date and time of the visit, the type and identifying number of the presented government-issued ID, and the serial number of the visitor ID. If the visit entails a large group, the visitor log may be filled in prior to the visit, but each visitor must sign next to their information. Guardians of minors without identification will sign on their behalf. Visitor logs will be maintained for three years (reference oldest date listed on log) and then destroyed (per National Archives & Records Administration (NARA) General Record Schedule (GRS) 5.6).

c. Visitor ID Media. Visitor ID media is required to be worn by all visitors, consistent with paragraph 4-3-4. The visitor ID must be annotated on its face with an expiration date upon issuance. Self-expiring commercial visitor IDs are authorized, but they must indicate expiration within 24 hours of issuance.

d. Terminated Visits. If any visit becomes suspicious or when visit circumstances change in a way that could possibly compromise information, systems, or operations, the visitor sponsor or escort official must terminate the visit, retrieve the ID media, and notify the FM. The FM must complete an incident report (see paragraph 4-6-9b) and notify local law enforcement as/if appropriate.

e. Visits Requiring Access to Classified National Security Information (CNSI), CNSI Areas, or CNSI Equipment. In addition to all the requirements contained in this order, refer to FAA Order 1600.2.

f. Students Attending Courses at an FAA Facility. All students must present a letter of acceptance signed by an FAA official or other pre-notification from the training authority and be issued visitor ID media upon presenting a valid government-issued photo identification that has an expiration date. Visitor ID expiration dates may coincide with expected class end dates. Students do not require continuous escort, but information, facility, and equipment access must be restricted commensurate with course activities and applicable law and policy.

g. Visits by Federal Executives, U.S. Government Officials, Foreign Dignitaries, and Heads of State. For visits involving U.S. Government officials, the FM (or the sponsoring LOB/SO/AOA) will notify the SSE, Office of Government and Industry Affairs (AGI), and Office of Communications (AOC). For visits involving foreign dignitaries, the Office of International Affairs (API) will also be notified. FMs may alter procedures to include waiving screening and pre-populating/signing the visitor log. Procedural changes will be coordinated with the SSE.

(1) Visits by elected officials or candidates must be handled in accordance with FAA Order 1200.14, Visits to Field Offices and Facilities by Elected Officials.

(2) Once properly identified, DOT or other federal executives and their protective detail members (if any) will not be screened or formally escorted while in the facility. However, the FM or designee should personally escort the visiting executives during the visit. Armed members of a protective detail who are accompanying DOT or other federal executives are authorized to retain their firearms throughout the visit.

h. Visits Involving Media. Any requests for visits involving the media will be referred to and approved by AOC. Once approved, all normal visitor procedures and any photography or video restrictions in paragraph 4-6-9d will be followed.

i. Foreign National Visitors, Including Dignitaries. Foreign visitors must have a sponsor. Sponsors may be FAA employees or contractors. The sponsor must submit a visit request through the FAA's automated International Visitors Program (IVP), which is located on the FAA's intranet at: https://destination.faa.gov/LandingPage.aspx. Except as otherwise stated in this order, the rules for foreign national visitors, including dignitaries, are the same as for other visitors; a foreign passport is an acceptable form of ID.

(1) A minimum of 10 working days is needed to process a foreign visit request through the IVP. If this timeframe cannot be accommodated, the FM may allow the visit to proceed after

weighing the sensitivity of the facility and information, technology, or operations being shown or discussed and the visit's impact on the agency or other U.S Government initiatives. The visit will still be recorded through the IVP.

(2) The IVP is a role-based notification and approval system that involves the FM, SSE, and API. Additional information on roles and responsibilities is available in the system's user's guide available on the IVP website. While the FM retains the authority to disapprove any visit based on operational considerations, the FM cannot overrule a foreign visit disapproval made by ASH or API representatives.

(3) The SSE will coordinate with the FM to ensure all required visitor procedures are in place and determine if any additional restrictions are necessary.

(4) Foreign national visitors conducting official/routine business at facilities within public-facing areas (FSDOs, Certificate Management Offices (CMOs), etc.) or North American Aerospace Defense Command (NORAD) personnel on official business are not processed through the IVP. Additionally, lawful permanent residents (LPRs) are not processed through the IVP but will be verified by the SSE through the Department of Homeland Security (DHS) Systematic Alien Verification for Entitlements (SAVE) database. LPRs requesting facility access will provide a front and back copy of their U.S. Permanent Resident Card (aka "Green Card") to facilitate these checks.

j. Guidance for Cooperating with Law Enforcement Agencies (LEAs) and Process Servers. The FAA's general policy is to cooperate with LEAs and law enforcement officers (LEOs) acting within the scope of their official duties. However, civilians serving legal process may not have the same authority as LEOs and, accordingly, may not be entitled to the same access to FAA facilities. Issues that arise that are not addressed in this paragraph will be referred to the SSE for further coordination with AGC and affected LOBs/SOs.

(1) LEOs.

(a) LEOs may enter any building to conduct authorized duties, provided they do not interfere with necessary operations as determined by the FM. LEOs on official duty may carry weapons as otherwise provided in paragraph 4-3-6 of this order while at an FAA facility; screening is not required.

(b) For process serving activity, the FM will contact the employee being sought and request that the employee meet the LEO in a private location within the facility as determined by the FM. If the employee refuses or there are exigent circumstances, the LEO may be escorted into the workspace to locate and serve the employee if the activity doesn't interfere with critical functions. If the activity would interfere with critical functions, arrangements should be made to conduct the activity as soon as the employee can be made available.

(2) Civilian process servers.

(a) If a civilian (non-LEO) process server appears at an FAA facility to serve legal process, he or she will be allowed access to the facility in accordance with the applicable visitor and security orders, policies, and laws of the jurisdiction in which the facility is located.

Application of the relevant orders, policies, and laws may not entitle a civilian process server to enter beyond the facility's perimeter security station. The FM will contact AGC for guidance through the responsible HQ, Region, or Center office. If entry into the FAA facility is not authorized, the civilian process server must be so advised.

(b) If it is determined that the civilian process server must be granted access to the workspace in the FAA facility to serve the employee, the FM will first contact the employee being sought, advise the employee of the civilian process server's visit, and request that the employee meet the civilian process server in a private location within the facility as determined by the FM. If the employee refuses and critical functions are not affected, the process server may be escorted into the workplace. Otherwise, the employee's on-site manager will work with the FM and the process server to make the employee available as soon as possible.

(3) Other provisions.

(a) FAA employees are not authorized to accept service of process on behalf of other employees, the FAA, or the Administrator unless authorized by regulation, order, or prior approval of AGC through the responsible HQ, Region, or Center office.

(b) If the LEO or civilian process server is attempting to serve a summons on the FAA itself or the Administrator (in their official capacity) or other process on the FAA for agency records, documents, or testimony, direct the server to AGC through the responsible Region, Center office, or HQ, as applicable. Subpoenas should be sent directly to AWA-AGC-300-Subpoenas@faa.gov. In any event, if an employee is served with a subpoena for records, documents, or testimony on an FAA-related matter, the employee will immediately notify their manager, who will advise AGC through the responsible Region, Center, or Headquarters office.

k. Other Exceptions to Visitor Entry and Escort Procedures.

(1) Emergency response agencies, such as fire, ambulance, and police, who are responding to an emergency, will be allowed unescorted access to FAA facilities and property to resolve the emergency. However, these personnel must be escorted if the nature of the emergency permits, and their identity must be verified and logged when they are preparing to depart.

(2) Facilities that deal extensively with the public (e.g., FSDOs) do not have to follow visitor procedures in the public areas of the facility. Visitor entry and escort procedures still apply for visits to non-public areas of these facilities.

4-3-6. Occupant Screening. The FAA has the authority to conduct inspections of every individual's personal effects upon entering or exiting federal property. Entry inspections of both personnel and visitors to government buildings have been upheld, citing the security and safety concerns associated with building entry as the constitutional justification for their use. All individuals, their vehicles, and property in the immediate possession of individuals entering FAA federal property are subject to inspection as provided under 41 CFR § 102-74.370. Visitor screening will follow the provisions of paragraph 4-3-7. FMs will regulate the introduction of prohibited and controlled items into the facility as specified in the facility security plan (see paragraph 4-6-9).

a. Prohibited Items. FMs will adhere to the ISC standard, "Items Prohibited from Federal Facilities," February 2013, or any succeeding edition, to deny the introduction of dangerous or unlawful items into an FAA facility. The FSP will contain a listing of prohibited items and any facility-specific exceptions or exemptions that apply. No person, while in or on FAA-owned/leased facilities/properties (including vehicles) or those facilities/properties where FAA has security responsibility, will carry or have in their possession, to include their personal vehicles, firearms, ammunition, or other deadly weapons, unless authorized in writing by the FAA Administrator or falling within one of the following excepted categories or conditions:

(1) FAA CSOs. FAA CSOs may carry authorized weapons necessary for the performance of their assigned duties while on duty or to/from a duty location, as provided in paragraph 5-4.

(2) Law Enforcement Officers (LEOs). Firearms may be carried by LEOs while the officer is performing official duties as provided in paragraph 4-3-5j of this order or if they are required by their jurisdiction to carry weapons 24 hours a day, 7 days a week. In those instances where a LEO is also performing security services at an FAA facility and is working (e.g., moonlighting) in the capacity of a security officer at an FAA facility, he or she may not carry any other firearm or weapon other than those prescribed by the security services contract/agreement.

(3) FAA employees within the Alaskan region may possess personal firearms and other weapons for survival or emergency purposes, or as otherwise authorized for the performance of job-related duties, in FAA-owned or leased remote facilities, at operational areas, and in or on government-furnished vehicles, where specifically authorized under an Alaskan Region supplemental directive.

(a) The Alaskan Region supplemental directive is issued by the Regional Administrator, Alaskan Region, after coordinating it with AGC and ASH. The supplemental directive will include a list of the types of personal weapons other than firearms that may be possessed in FAA-owned or leased remote facilities and employee housing and provide for training and storage requirements, geographical and operational limitations, and time-limited written authorizations for individual employees submitted by the appropriate management chain for such employee and approved by the Regional Administrator, Alaskan Region. Time-limited written authorizations will not be required for firearms and other weapons stored in employee housing for purely personal use while off duty. A copy of the supplemental directive will be made part of the facility record in the ASH facility security database.

(b) For purposes of this sub-paragraph, "remote facilities" refer to an FAA-owned or leased property located in rural areas, which do not have assigned security officers on site.

(4) FMs whose facility hosts an ATM or a credit union may allow armed currency couriers to access the facility subject to the following stipulations:

(a) Verification of the state licensing of the courier service,

(b) Receipt of a current by-name list of assigned couriers provided by the company, and

(c) FSP-published identification and verification procedures used by CSOs or other facility personnel to grant facility access. Couriers must be in uniform and driving a company armored vehicle. Couriers will be signed in as visitors but are exempt from normal escort requirements while performing their duties. Armored vehicles may be admitted inside otherwise restricted parking areas after identification and verification is completed.

b. Controlled Items. Controlled items are those items that may be otherwise prohibited but are "tools of the trade" and "sporting equipment" that are considered potentially dangerous. FAA personnel may possess controlled items on federal property. Government-furnished items are authorized within facilities. Personal items are allowed within a facility if the item is necessary to perform a mission or maintenance operation (e.g., saws, screwdrivers) and its need is sanctioned by the FM or designee. The FM will determine whether display items (e.g., engraved baseball bat) are allowed within the facility. Otherwise, personal items will remain in personal vehicles. Within these parameters, FMs will refer to the ISC standard, "Items Prohibited from Federal Facilities," February 2013, or any succeeding edition when developing local procedures for controlled items. The FSP will contain a listing of controlled items and any facility-specific policy or procedures for their introduction and possession.

4-3-7. Visitor Screening. All visitors will be screened to preclude the introduction of any prohibited or controlled items into the facility (see paragraph 4-3-6) unless exempted or authorized by the FM. Refusal to submit to visitor screening will result in denial of entry. At facilities without CSOs, this screening will consist of observation by the FM (or designee) and escorts. Visitors may be asked to leave all unnecessary hand-carried items in their vehicle. At facilities with CSOs, X-ray and Walk-Through Metal Detection Devices (WTMDDs) will be used, as available, to screen items hand-carried by individuals entering the facility. Hand-Held Metal Detection Devices (HHMDD) will be used to assist in the resolution of WTMDDs. Where screening equipment is not available, the FM will develop alternate procedures in coordination with the SSE. These procedures will be included in the FSP.

a. If a suspicious item is discovered during an inspection (screening) or if a visitor refuses an inspection, the visit will be terminated. If the visitor is part of a larger group visiting the facility, the FM will need to determine if the rest of the group may proceed with the visit or if the entire group will be denied access. See paragraph 4-3-5d.

b. Minor children will be granted temporary access to a facility's controlled perimeter when accompanied by, and in a vehicle operated by, an FAA employee or contractor for the purpose of drive-up, pick-up/drop-off of another FAA employee or contractor. Minor children accessing the controlled perimeter under these conditions will not be subjected to screening but will also not be allowed entry into the facility.

c. Where public access to restrooms is required by law, FMs must establish procedures for screening individuals seeking access to public restrooms in controlled space on FAA facilities.

4-3-8. Ballistic Protection at Screening Locations. Reserved.

4-3-9. Lobby Queuing. Reserved.

4-3-10. After-Hours Access Control. No additional measures beyond those specified in Table 4-3-1. Facilities that are not in continuous operation may use a secure key safe (e.g., Knox Box) to allow emergency response access. Facility managers must coordinate with local fire response agencies before installing these device types.

4-3-11. Limit Building Entry Points. No additional measures beyond those specified in Table 4-3-1.

4-3-12. Entrance Co-Location. Reserved.

4-3-13. Perimeter Doors and Door Locks.

a. Door Requirements. Perimeter doors will be made of solid, closed, or tight-grained wood, steel or employ sheet metal/metal clad 14-gauge (.0747 inches) or thicker or have tempered or American National Standards Institute (ANSI) rated burglary-resistant glass used or an equivalent film or laminate applied (glass embedded with wire mesh may also be used) (see also paragraph 4-2-6). Doors must be equipped with Building Hardware Manufacturer's Association (BHMA) Grade 1 hardware. Door frames must be substantial and consistent with door construction. Hinge pins on the unsecured side of exterior doors will be designed or modified to prevent removal.

(1) Perimeter doors and critical operational area doors must be equipped with latch guards or be designed to protect the latching hardware from tampering. Perimeter double doors must be equipped with full-length astragals or other mechanism (e.g., rim latch hardware, interior mullion) to prevent defeat of the locking hardware. Unusual door designs (e.g., rolling (garage-type) or sliding) will be secured in a manner that achieves similar protection to the standards listed above.

(2) Exterior perimeter doors and controlled area doors will be kept closed and always locked unless there are personnel providing access control. Doors of facility outbuildings that the SSE determines do not house critical equipment, do not lead to critical areas, do not protect valuable or easily pilfered government equipment and supplies, and are within a properly fenced perimeter are excluded from this requirement.

b. Locking Systems. All exterior perimeter doors and those interior doors through which the FM restricts access will be fitted with any BHMA Grade 1 system that accepts a universal 7-pin removable and interchangeable core that can be changed without disassembling the entire core or BHMA Grade 1 equivalent electronic lock cylinders and programmable smart key systems. Electronic/programmable systems are recommended in circumstances where they are more cost-effective than traditional cores and keys. Keys and access cards must be numbered to facilitate inventory control (see paragraph 4-3-14b).

(1) For FAA-leased facilities, the lessor will furnish FAA standard BHMA Grade 1 locking hardware except for lock cores and keys, which will be provided by the FAA. The FAA will maintain its own key system.

(2) Mechanical push-button keypads or hard-coded electronic keypads may be used in addition to FAA standard locks on any FSL 1 or FSL 1A facility perimeter door; perimeter doors of facility outbuildings that do not house critical equipment or lead to critical areas and are within a fenced perimeter; any internal door not otherwise protected with PACS; and pedestrian gates at FSL 2 and 1 facilities.

(3) The exterior doors on Mobile Air Traffic Control Towers and Deployable Air Traffic Control Facilities will be mechanical cipher and keyed locks.

4-3-14. Control of Keys and Access Media.

a. Key Control Program. The FM must establish and maintain a key control program and will either serve as or appoint a key control officer (KCO) in the FSP. The KCO is responsible for the management, inventory, and disposition of keys, locks, cores, and electronic access cards. If a lessor manages facility keys and provides access cards and keys to FAA leased spaces, an FAA KCO will be appointed to ensure only authorized individuals receive keys to FAA spaces. Key and electronic access card quantities will be kept to a minimum and issued only when needed for official duties. Unissued keys/cores/access cards must be stored in a locked container and access to that container restricted to the FM and any appointed KCOs. The issuance of spare keys must be kept to a minimum to support operations. Keys and any access cards must be returned by or retrieved from personnel who no longer require access to the protected space. Cypher lock codes and other combinations in use will be changed when there are personnel changes where an employee no longer requires access to the protected space or whenever compromise is suspected. For classified storage, FAA Order 1600.2 takes precedence.

b. Annual Inventories. The FM or KCO will complete an inventory of all keys, cores, and electronic access cards annually and/or upon change of the KCO. The inventory will reflect all cores, keys, and access cards installed and in use at the facility. Items will be accounted for by number as being on hand, issued (via a signed, dated hand receipt), listing an installation location, and a loss (incident) report or a destruction record. Issued keys/hand receipts will be verified annually as part of the inventory.

c. Lost Keys, Cores, and Electronic Access Cards. Losses will be reported through the FM via WebIRS (see paragraph 4-6-9b, Incident Reporting). In the report, list whether a lost key was a master, sub-master, or control key, the area(s) the key protected, the key's number, the date of loss, who it was assigned to, and whether a compromise has occurred. Generally, the loss of any grand master key or any two sub-master keys, the control key, or five percent of the keys of a series is considered to have compromised the whole series. If compromise is suspected, the FM and SSE will evaluate the extent of the compromise and determine mitigation strategy. Lost electronic access cards must immediately be removed/deactivated from the facility access control system. Lost cyber keys will be treated in the same way as PACS (see para 4-3-4b) and deleted from associated cores within 24 hours.

4-3-15. Employee Convenience Doors. Reserved.

4-3-16. Emergency Exit Doors. No additional measures beyond those specified in Table 4-3-1.

4-3-17. Delayed Egress. Reserved.

Chapter 4. Facility Security Countermeasures

Section 4. Interior Security Countermeasures

4-4-1. Countermeasure Matrix. The following matrix identifies the interior security baseline LOP criteria for each FAA facility based on the facility's FSL and classification (Critical Infrastructure [CI] or Administrative).

Table 4-4-1. Interior Security Countermeasures

Interior Security Criteria	**Para**	**CI - FSL**					**Admin - FSL**		
		1	2	3	4		1	2	3
Space Planning	4-4-2								
Reserved									
Access to Nonpublic Areas	4-4-3								
Reserved									
Security of Critical Areas	4-4-4								
Limit access into critical areas		X	X	X	X		X	X	X
Install FAA standard locks on critical area doors		X	X	X	X		X	X	X
Use PACS to control access to critical administrative areas				X	X				X
Use PACS to control access to critical operations areas	4-3-4		*	X	X				
Use PACS to control access to control room doors	4-3-4		*	X	X				
Use VSS to monitor entry into critical operations areas	4-5-2		*	X	X				
Mechanical push-button or electronic keypads at control room/tower cab doors (in addition to standard locks)	4-3-4	X	X						
Building Systems and Roof Access	4-4-5								
Limit access into utility, mechanical, electrical, and telecom rooms		X	X	X	X		X	X	X
Install FAA standard locks on utility, mechanical, electrical, and telecom room doors		X	X	X	X		X	X	X
Protect access to interior spaces from the roof using IDS				X					X
Protect access to interior spaces from the roof using PACS and IDS					X				
Access ladders secured from unintended use			X	X	X				X
Publicly Accessible Restrooms	4-4-6								
Reserved									
Publicly Accessible Retail and Mixed-use Space	4-4-7								
Accommodate through such means as separating entryways		X	X				X	X	
Accommodate through controlling access, screening, and security forces				X	X				X
Blast Resistance – Interior Public Spaces	4-4-8								
Reserved									
Blast Resistance – Mail Screening and Receiving Location	4-4-9								
Reserved									
Interior Windows	4-4-10								
Reserved									

* Applies to Tier 1 Facilities as specified in FSRS.

4-4-2. Space Planning. Reserved.

4-4-3. Access to Non-public Areas. Reserved.

4-4-4. Security of Critical Areas. A critical area is an interior or exterior area to which unescorted access is limited to personnel who need access to perform official functions as determined by the FM. Critical Areas can be either critical operations areas or critical administrative areas.

a. Critical Operations Area. An area of an FAA CI facility that houses equipment or services that would adversely impact the NAS or the operation of the facility if it were damaged or lost. Examples of critical operations areas include CSO guardhouse, air traffic control rooms/cabs, equipment rooms housing NAS navigational systems/communications equipment, secure rooms used for Communications Security (COMSEC) and/or CNSI processing, areas/rooms containing power or HVAC systems supporting the facility (including cooling towers, condenser units, emergency generators, and battery back-up locations).

b. Critical Administrative Area. An area of any FAA facility in which controlled, unclassified information or protected materials are used, stored, or regularly processed. Examples of critical administrative areas include areas with financial or acquisition information, FAA identification and access control media, mail rooms, medical, or where other controlled, unclassified information is used, stored, or regularly processed.

4-4-5. Building Systems and Roof Access. No additional measures beyond those specified in Table 4-4-1.

4-4-6. Publicly Accessible Restrooms. Reserved.

4-4-7. Publicly Accessible Retail and Mixed-use Space. The requirements of Table 4-4-1 apply only where such space exists.

4-4-8. Blast Resistance – Interior Public Spaces. Reserved.

4-4-9. Blast Resistance – Mail Screening and Receiving Location. Reserved.

4-4-10. Interior Windows. Reserved.

Chapter 4. Facility Security Countermeasures

Section 5. Security Systems Countermeasures

4-5-1. Countermeasure Matrix. The following matrix identifies the security systems baseline LOP criteria for each FAA facility based on the facility's FSL and classification (Critical Infrastructure [CI] or Administrative).

Table 4-5-1. Security Systems Countermeasures

Security Systems Criteria	**Para**	**CI - FSL**					**Admin - FSL**		
		1	2	3	4		1	2	3
VSS Coverage	4-5-2								
Surveillance									
Perimeter				X	X				
Screening checkpoints				X	X				X
Vehicle entrances/exits				X	X				X
Loading docks				X	X				X
Lobbies				X	X				X
Parking areas					X				
Alarm Assessment									
Exterior alarmed perimeter doors			X	X	X			X	X
Exterior alarmed critical areas				X	X				X
Alarmed windows			X	X	X			X	X
Interior critical operations areas			*	X	X				
Access Screening									
Entry Control Video – Main visitor doors			X					X	
Entry Control Video – Tower Cab/Control Room doors				X	X				
Gate Control Video			X						
Peephole		X	X				X	X	
VSS Monitoring and Recording	4-5-3								
Active monitoring				X	X				X
Record on digital medium			X	X	X			X	X
Security Control Center	4-5-4								
Facility security checkpoint or guardhouse				X	X				X
VSS Surveillance Advisory	4-5-5								
Regulatory signage – where VSS is in use	4-3-3		X	X	X		X	X	X
Intrusion Detection System (IDS) Coverage	4-5-6								
Perimeter doors			X	X	X			X	X
Operable ground floor windows			X					X	
Ground floor windows				X					X
All windows within 16 feet of the ground					X				X
Roof openings that access internal space				X	X				X
Exterior critical areas				X	X				X
HVAC control rooms					X				
Open storage secure areas		Where Installed							
Intrusion Detection System (IDS) Monitoring	4-5-7								
Local annunciation			X					X	
Annunciate at CSO guardhouse/checkpoint				X	X				X

Security Systems Criteria	Para	CI - FSL					Admin - FSL		
		1	2	3	4		1	2	3
Duress Alarms or Assistance Stations	4-5-8								
Guard posts				X	X				X
Sensitive public contact areas								X	
Garages and high-risk locations (if applicable)					X				
Security System Integrity	4-5-9								
Reserved									
Security Communications	4-5-10								
Provide multi-channel radio transceiver communications equipment				X	X				X
Building Communications System	4-5-11								
Provide a communications system for security and emergency announcements				X	X				X
Emergency Power for Security Systems	4-5-12								
Provide 4-hour uninterruptible emergency power to essential security systems				X	X				X
Security Systems Testing	4-5-13								
Conduct annual security system testing			X	X	X			X	X
Conduct daily testing of screening equipment			*	X	X				X
Security System Maintenance	4-5-14								
As specified in the Corrective Maintenance Contract			X	X	X			X	X

* Applies to Tier 1 Facilities as specified in FSRS.

4-5-2. Video Surveillance System (VSS) Coverage. Components of VSS must be secured against unauthorized access. Where CSOs are used, camera site mapping and/or site plan is required. If designs allow, single cameras may provide more than one function or monitor more than one alarm point.

a. Surveillance. The design objective for perimeter surveillance is to view as much of the perimeter as possible using building or pole-mounted fixed or moving cameras looking from the facility outward. It is acceptable that the design does not provide camera coverage of the entire perimeter simultaneously. Some camera obstructions may be accepted as long as unauthorized activity is recorded prior to individuals reaching any protected building's exterior. Perimeter camera resolution will be sufficient to record suspect activity and alert CSOs.

b. Alarm Assessment. Cameras supporting exterior alarmed points will provide an external view to assist in recording suspect activity and persons in the immediate area of the alarmed point. Cameras supporting interior alarmed points will provide a capability to view a front-facial image of individuals accessing the areas. If design allows, cameras supporting interior alarmed points may be satisfied by mounting the camera inside or outside of the door.

c. Access Screening. Entry control video (ECV) and gate control video (GCV) allow an operator to identify persons, objects, and vehicles and speak with persons requesting access to a facility or area, and then remotely open doors or gates to allow access. The capability to remotely open the door or gate may be placed in multiple locations to meet operational need. Capability can be met by stand-alone prepackaged systems or by using a separate camera and intercom/telephone. There is no requirement to monitor or record visitor screening systems.

(1) ECV is utilized at the facility's visitor/main entrance door at FSL 2 facilities. ECV is utilized at tower cab/control room doors at FSL 3 CI and above.

(2) GCV is utilized at automated vehicle gates that are routinely used for access at facilities where guards are not assigned or always present. The view from a GCV camera must provide general coverage of the vehicle and a view of the gate itself. The view of the gate must allow the user to observe that the gate has closed completely and that only the visitor's vehicle passed through the gate. Where an acceptable camera view of a vehicle is concurrently provided by an existing surveillance system camera, that camera may be used for the GCV function.

4-5-3. VSS Monitoring and Recording. Cameras will continuously record. Where active monitoring is available (FSL 3 and FSL 4 CI facilities), cameras will automatically display upon alarm. Recorded video will be stored for 30 days, in accordance with NARA GRS 5.6, and easily exportable to commercial off-the-shelf video players or web browsers and saved to separate media. Installation of additional exterior or interior area VSS may be required to mitigate a finding of inadequate security (e.g., parking garages, critical cable runs, rooftop egress ladders) or to aid in the investigation of theft, vandalism, or other events consistent with an official Office of Investigations and Professional Responsibility (AXI) investigation. Like PACS, video will not be used for time and attendance tracking purposes. The FM may review stored video for internal system or incident validation purposes. Stored video will be released by the FM:

a. To security system technical staff for system maintenance purposes,

b. To the SSE in support of security assessment activities or subsequent to an official investigation once initiated by ASH/AXI; and

c. To law enforcement to assist in an investigation as authorized by the SSE.

d. When otherwise required by law, such as in response to an order of a court of competent jurisdiction or in response to a Freedom of Information (FOIA) request if no FOIA exemption applies.

4-5-4. Security Control Center. The SCC may be, and is typically, co-located with the facility security checkpoint. An SCC provides a central place for security equipment that is utilized by the CSOs during operational hours.

4-5-5. VSS Surveillance Advisory. VSS (CCTV) warning signs must be posted at facilities where VSS is in use. Signs will be posted on the exterior side of fences, gates, and other areas where they are plainly visible to anyone approaching. See paragraph 4-3-3.

4-5-6. Intrusion Detection System (IDS) Coverage. Where PACS provides for intrusion detection on required doors, a separate IDS system for doors is not required. At FSL 3 and FSL 4 facilities, IDS will be equipped with an uninterruptible power supply capable of providing a minimum of four (4) hours of backup power and, where possible, be connected to the critical power supply (emergency generator). Installation of additional IDS components may be required to mitigate specific facility risks. Where Perimeter IDS (PIDS) has been previously installed at a facility, it will be removed upon technical refresh or when it reaches end of lifecycle (equipment no longer functions and there are no replacement parts for the equipment). Where CSOs are used

and can monitor ground floor (lobby) windows and/or where windows are constructed to prohibit penetration (e.g., burglary resistant or hurricane or seismic standards) and CSOs can respond, IDS is not required.

4-5-7. IDS Monitoring. Where IDS is integrated with PACS and installed under the PSEMS, local monitoring of alarms can be forwarded (via email) to facility managers in response to increased incidents to mitigate risk. Alarm logs are generated internally by PSEMS. Historical alarm data must be preserved and be retrievable within PSEMS for three years.

4-5-8. Duress Alarms or Assistance Stations. CSO duress alarms will annunciate at a designated location documented in the FSP. Facilities without CSOs will include duress procedures in their FSPs.

4-5-9. Security System Integrity. Reserved.

4-5-10. Security Communications. No additional measures beyond those specified in Table 4-5-1.

4-5-11. Building Communication System. Systems may include public address systems, specially designed phone systems, and computer-based mass delivery.

4-5-12. Emergency Power for Security Systems. No additional measures beyond those specified in Table 4-5-1.

4-5-13. Security System Testing. The FM, or designee, will conduct testing in accordance with procedures published by AXF. During comprehensive assessments, the SSEs will conduct random door/area tests of the appropriate systems in accordance with procedures published by AXF. Testing results will be documented in the facility assessment report.

4-5-14. Security System Maintenance. No additional measures beyond those specified in Table 4-5-1.

Chapter 4. Facility Security Countermeasures

Section 6. Security Operations and Administration Countermeasures

4-6-1. Countermeasure Matrix. The following matrix identifies the security operations and administration baseline LOP criteria for each FAA facility based on the facility's FSL and classification (Critical Infrastructure [CI] or Administrative).

Table 4-6-1. Security Operations and Administration Countermeasures

Security Operations and Administrative Criteria	**Para**	**CI - FSL**					**Admin - FSL**		
		1	2	3	4		1	2	3
Facility Security Committee (FSC)	4-6-2								
Identify an FSC at multi-tenant federal facilities									X
Facility Security Committee (FSC) Chairperson	4-6-3								
Establish an FSC chair at multi-tenant federal facilities									X
Security Operations Management	4-6-4								
Assign a security coordinator (FM's option)		X	X	X	X		X	X	X
Security Force Fixed Post – Exterior	4-6-5								
Provide exterior posts as designated in post orders				X	X				X
Security Force Fixed Posts – Screening Checkpoints	4-6-6								
Provide a CSO guardhouse/checkpoint				X	X				X
Security Force Patrols	4-6-7								
Provide security force patrols as designated in post orders				X	X				X
Security Force Response	4-6-8								
Provide response to alarms and incidents as designated in post orders				X	X				X
Facility Security Plan	4-6-9								
Publish a facility security plan		X	X	X	X		X	X	X
Occupant Emergency Plan (OEP)	4-6-10								
Publish an occupant emergency plan		X	X	X	X		X	X	X
Conduct annual tests of the OEP		X	X	X	X		X	X	X
First Responder Book		X	X	X	X		X	X	X
Availability of Emergency Plans and Documentation	4-6-11								
First Responder Book		X	X	X	X		X	X	X
FAA Threat Checklist		X	X	X	X		X	X	X
Protection of Construction Information	4-6-12								
Protect security-related construction documents as controlled unclassified information		X	X	X	X		X	X	X
Security During Construction and Renovation	4-6-13								
Mitigate vulnerabilities associated with construction or renovation activities		X	X	X	X		X	X	X
Mail/Package Handling and Other Deliveries	4-6-14								
Inspect mail and packages prior to distribution throughout the facility		X	X				X	X	
Screen mail and packages prior to distribution throughout the facility				X	X				X
Security Awareness Training	4-6-15								
Local orientation		X	X	X	X		X	X	X
Security Awareness Virtual Initiative (SAVI)		X	X	X	X		X	X	X

4-6-2. Facility Security Committee (FSC). A facility security committee is required at facilities with multiple federal tenants. An FSC is not required at single-tenant (FAA-only) facilities. If an official FSC is not required, it is recommended that FMs still conduct periodic security meetings with facility management and labor representatives, as needed.

4-6-3. Facility Security Committee (FSC) Chairperson. A facility security committee chairperson is required at facilities with multiple federal tenants. An FSC chairperson is not required at single-tenant (FAA-only) facilities.

4-6-4. Security Operations Management. FMs may appoint a security coordinator (SC) to assist in the management of the facility's security program. The appointment is recommended at larger facilities. At smaller facilities, the SC may be the FM. The FM will notify the SSE of the appointment.

4-6-5. Security Force Fixed Post – Exterior. No additional measures beyond those specified in Table 4-6-1. See Chapter 5 for CSO standards.

4-6-6. Security Force Fixed Post – Screening Checkpoint. The screening checkpoint may take the form of a guardhouse or booth located at the perimeter or take the form of an operations center placed in the entrance lobby depending on the facility layout, functions, and equipment supported by the security forces. If a checkpoint is sited within a lobby and access control into a fenced area is required, then a traffic checkpoint will be placed at the perimeter. Security checkpoint functions and equipment needs include:

Table 4-6-2. Security Checkpoint Functions and Equipment

Security Checkpoint	Equipment
Visitor, mail, and package screening	Magnetometers and X-ray machines
Temporary parcel and mail storage	VSS (CCTV) monitors
CSO duress alarms	Alarm annunciator equipment
CSO firearm clearing barrel	CSO firearm ammunition storage
Temporary identification media	CSO firearm storage

4-6-7. Security Force Patrols. No additional measures beyond those specified in Table 4-6-1. See Chapter 5 for CSO standards.

4-6-8. Security Force Response. No additional measures beyond those specified in Table 4-6-1. See Chapter 5 for CSO standards.

4-6-9. Facility Security Plan (FSP). The FM must publish an FSP for all staffed facilities. The plan must be reviewed and updated as changes are made or at least annually. An electronic copy of the facility's FSP will be provided to the SSE for inclusion in the FSRS facility profile. AXF publishes FSP templates that are tailored to the needs of different facility security levels and sizes and are available through the SSE. FMs are encouraged to use these templates to develop their FSPs. Examples of information included in an FSP are listed in Table 4-6-3 below.

Table 4-6-3. Sample FSP Contents

Plan Contents	Plan Supplements
Roles and Responsibilities	Facility Security Assessment Report

Plan Contents	Plan Supplements
Security Countermeasures Maintaining Countermeasures Prohibited Items Controlled Items Incident Response Management Information Security Government Property Training and Exercises Plan Review	Scheduled Requirements Checklist Workplace Violence Plan Active Shooter Plan Testing of Emergency Plans Procedures for Safeguarding Government Property Shipping and Receiving Procedures Screening Suspicious Mail or Packages HVAC Emergency Procedures National Terrorism Advisory System (NTAS) Guide Visitor Screening Procedures Detecting and Reporting Suspicious Unmanned Aircraft Systems

Because it is not explained elsewhere in this order, the following information is provided to assist in developing relevant portions of the FSP.

a. Safeguarding Government Property. Property custodians must comply with FAA Order 4600.27, Personal Property Asset Lifecycle Management. Loss of government property will be reported consistent with FAA Order 4600.27 and this order, paragraph 4-6-9b, Incident Reporting. Additionally, FMs must provide secure environments for government property under their control. Measures to consider include:

(1) Adequate control of accountable equipment and items easily pilfered.

(2) In large storage areas, accountable equipment is stored separately from the general storage area (e.g., in security cages secured by FAA-approved padlocks).

(3) High-value items are inventoried upon receipt with a record of where the items were delivered or stored.

(4) Interior and remote storage areas protected against unauthorized entry.

(5) Shipping and receiving areas and loading docks secured whenever unattended and access always controlled.

b. Incident Reporting. FAA security incidents are reported through the Web-based Incident Reporting System (WebIRS), a system that automates formal incident reporting to the SSE. WebIRS can be found at: https://incidentreporting.faa.gov. Although all FAA personnel have access to and are encouraged to utilize WebIRS for incident reporting, FAA personnel are required to report security incidents to their immediate manager/CO/COR, another manager, the SC, or FM as soon as possible but always within 24 hours. From that initial reporting, the FAA employee's manager, SC, or FM must ensure a WebIRS entry is made within 48 hours of the event. In today's threat environment, the standing practice is "see something, say something," and employees are encouraged to use WebIRS to report anything they consider out of the ordinary. Additionally:

(1) Threats against the President, Vice President, other government officials, visiting dignitaries, and DOT officials must be reported as prescribed in FAA Order 1600.55, Reporting Threats Against the President, Vice President, Other Government Officials, and Dignitaries.

(2) Nothing in this order is intended to interfere with prompt reporting of emergencies to first responders or to delay the reporting of possible criminal activity to police.

(3) Nothing in this order is intended to circumvent the reporting of significant activities, incidents, or events as directed within FAA Order 1990.1, FAA National Command and Control System.

c. National Terrorism Advisory System (NTAS). DHS issues NTAS alerts and bulletins. Alerts indicate specific and credible terrorist threats of a limited duration. Bulletins communicate current developments or trends. Additionally, there are two types of alerts, an elevated alert and an imminent alert that relate to the specificity and credibility of the threat information. Upon receipt of an alert, FMs, working with their SSEs, may identify specific protective measures for the facility. Additional security measures may also be directed through security notices issued by AXF. Bulletins are informative in nature and additional security measures are typically not implemented when they are received.

d. Information Security. This section details the protective measures implemented to safeguard the facility's information assets. SSEs and other federal investigators are authorized to take photographs or video recordings on or within FAA facilities when conducting assessments, investigations, or other official duties. In other cases, photography or video recording on or within an FAA facility is contingent upon FM approval. In all situations, care must be taken to protect sensitive information or operations, consistent with the requirements of applicable law and policy. See FAA Order 1240.13, Export Control Compliance; FAA Order 1600.2, Classified National Security Information (CNSI); FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI); and FAA Order 1370.121, FAA Information Security and Privacy: Policy, and its supplemental implementing directives, for additional information.

e. Active Shooter Plan. The facility's active shooter plan requirements are contained in the supplement to the FSP template that is provided by AXF and made available to all FMs. The plan will include the development of a First Responder Book (FRB) designed to assist law enforcement and other first responders by providing them with specific facility information for their use during an emergency. The book will be kept at the facility entry or the best site-specific location that will be readily available to first responders.

f. Testing of Emergency Plans. The facility's Occupant Emergency Plan (OEP) (see paragraph 4-6-10) contains both security and emergency items that must be tested annually, and that testing must include an actual facility evacuation. Additionally, an annual table-top or functional exercise will be conducted and documented that rotates between bomb threat, violence in the workplace, and active shooter preparedness scenarios. Where possible, it should include representatives of local emergency response agencies. The SSE may be invited to participate. Scenario examples and exercise checklists are provided by AXF for FM use.

4-6-10. Occupant Emergency Plan (OEP). An OEP is a site-specific requirement for federal facilities to establish procedures for safeguarding lives and property in and around the facility during emergencies. These plans reduce the threat to personnel, property, and other assets within the facility in the event of an incident inside or immediately surrounding a facility by providing facility-specific response procedures for occupants to follow. The OEP is required and defined by 41 CFR 102-71.20. The FM, or alternate, executes the OEP. At leased facilities with multiple tenants, the agency with the highest-ranking government official assigned to the facility is the designated official for executing the OEP. Shelter-in-place and evacuation procedures should be developed as part of the facility's emergency planning.

4-6-11. Availability of Emergency Plans and Documentation. All facility personnel must have access to the facility's OEP. The FM, other emergency management personnel, and first responders should have immediate access to the FRB. An FRB will be prepared to assist law enforcement and other first responders by providing them with specific facility information for their use during an emergency. Procedures must be developed to ensure after-hours access to these plans. To assist employees in responding to a bomb threat, a suspicious letter or package, or an active shooter event, an FAA Threat Checklist (FAA Form 1600-53) is available at the top of the Windows Start Menu on every FAA-issued employee computer.

4-6-12. Protection of Construction Information. Protection will be in accordance with the requirements of applicable law and policy. Refer to FAA Orders 1240.13, 1600.2, 1600.75, and 1370.121 and its supplemental implementing directives, for additional information.

4-6-13. Security during Construction and Renovation. No additional measures beyond those specified in Table 4-6-1.

4-6-14. Mail/Package Handling and Other Deliveries. Mail/package handling procedures are included in the FSP and are addressed in AXF-published FSP templates. In addition, persons who process or distribute mail should review "Best Practices for Managing Mail Screening and Handling Processes: A Guide for the Public and Private Sectors." The document can be found on the Cybersecurity and Infrastructure Security Agency (CISA.gov) public website. At facilities with CSOs, X-ray machines will be used to screen delivered mail/parcels and those packages carried by visitors that will fit through the X-ray machine. All items too large to be X-rayed will be screened by procedures established in the FSP (e.g., verification of sender, off-site delivery). Mail and packages will be screened as soon as possible after delivery to the facility.

4-6-15. Security Awareness Training. Local security orientation will be conducted within 30 calendar days of entering on duty at any FAA facility and annually thereafter. Additionally, FAA personnel must complete the Security Awareness Virtual Initiative (SAVI) training available through the electronic Learning Management System (eLMS), or as otherwise made available by the LOB, within 90 days of entering on duty and annually thereafter. Security awareness is the cornerstone of any effective security program. For security awareness programs to be successful, individuals must understand their program responsibilities. Therefore, employee security awareness briefings are an important part of the FSMP. Topics for local security orientation are listed in Table 4-6-4. Local security orientation training must be documented and provided to the SSE during facility security assessments.

Table 4-6-4. Initial and Annual Local Security Awareness Briefing Topics

Briefing Topics	Briefing Topics	Briefing Topics
Individual Security Responsibilities	Security Points of Contact	Protection of Classified/Controlled Unclassified Information
Visitor Control (including after-hours entry)	Facility Security Plan	Occupant Emergency Plan
Bomb Threat Procedures	Reporting Security Incidents	Active Shooter/Workplace Violence
Vehicle Parking Policies	Protecting Government Property	ID Media Display Requirements
Local Threats and Vulnerabilities	Other Security Issues of Concern	

Chapter 4. Facility Security Countermeasures

Section 7. Facility Cybersecurity Countermeasures

4-7-1. Countermeasure Matrix. The following matrix identifies the cybersecurity baseline LOP criteria for each FAA facility based on the facility's FSL and classification (Critical Infrastructure [CI] or Administrative).

Table 4-7-1. Cybersecurity Countermeasures

Facility Cybersecurity Criteria	**Para**	**CI - FSL**					**Admin - FSL**		
		1	2	3	4		1	2	3
Identify and Define BACS Devices and Networks; Establish Governance and Training Practices	4-7-2								
Reserved									
Segment BACS from Business Networks; Control Access to Devices and Networks	4-7-3								
Control access to security systems server				X	X				X
Establish and Maintain BACS Configuration Management	4-7-4								
As specified in PSEMS Certification and Accreditation documents			X	X	X				X
Maintain BACS Infrastructure	4-7-5								
As specified in PSEMS Certification and Accreditation documents			X	X	X				X
Ensure the Integrity and Availability of BACS Operational Data	4-7-6								
As specified in PSEMS Certification and Accreditation documents			X	X	X				X
Identify and Manage Access Points for Network Communications, Removable Media, Messaging Services, and Internet Access for BACS	4-7-7								
As specified in PSEMS Certification and Accreditation documents			X	X	X				X
Establish Processes for Incident Response for BACS	4-7-8								
As specified in the Corrective Maintenance Contract			X	X	X			X	X

4-7-2. Identify and Define Building Access and Control Systems (BACS) Devices and Networks. Reserved.

4-7-3. Segment BACS from Business Networks; Control Access to Devices and Networks. No additional measures beyond those specified in Table 4-7-1. See also paragraph 4-4-4 a.

4-7-4. Establish and Maintain BACS Configuration Management. No additional measures beyond those specified in Table 4-7-1.

4-7-5. Maintain BACS Infrastructure. No additional measures beyond those specified in Table 4-7-1.

4-7-6. Ensure the Integrity and Availability of BACS Operational Data. No additional measures beyond those specified in Table 4-7-1.

4-7-7. Identify and Manage Access Points for Network Communications, Removable Media, Messaging Services, and Internet Access for BACS. No additional measures beyond those specified in Table 4-7-1.

4-7-8. Establish Processes for Incident Response for BACS. No additional measures beyond those specified in Table 4-7-1.

Chapter 5. Contract Security Officers

5-1. Purpose. This chapter describes requirements and establishes standards for Contract Security Officer (CSO) services at facilities for which FAA is responsible for security oversight. They apply to new contracts solicited and awarded after the effective date of this Order. For current contracts, the requirements contained in the CSO Statement of Work (SOW) will be followed. This chapter does not apply to CSOs provided and managed by the Federal Protective Service (FPS) or to CSOs at a facility where security is managed by another agency (e.g., FAA Headquarters, which is managed by DOT).

5-2. CSO Functions and Staffing. Normally, armed CSOs are required at all FSL 3 and 4 facilities consistent with the staffing standards outlined below. In areas where facilities are located on protected airport property, the use of unarmed CSOs may be required because of local laws and/or ordinances. The respective circumstances that restrict arming of CSOs will be annotated in the FSRS facility profile.

a. Use of Unarmed CSOs. Where facilities are located on protected airport property, the use of unarmed CSOs may be required because of local laws and/or ordinances. In the situations described below, armed CSOs are not required. The respective circumstances that restrict arming of CSOs will be annotated in the FSRS facility profile by the SSE. Armed CSOs are not required:

(1) Where access by the public to the ATCT entrances requires processing through an airport screening checkpoint, or where access to the ATCT by FAA personnel requires entry on the security air operations area of an airport or military installation; and

(2) There is assurance of armed response by the airport authority or other law enforcement agency to appropriate requests for assistance.

b. CSO Functions. CSO functions will include, at a minimum, facility access control, visitor control and screening, alarm and VSS (CCTV) monitoring and response, and random patrolling. Patrols must be documented/logged to facilitate CSO oversight. This can be accomplished using an electronic guard tour monitoring system (PIV card readers/watch clock) or manually. See paragraph 5-6 for additional duty information.

c. CSO Staffing. A facility's CSO staffing level is based on the need and methods required to fulfill those functions as well as whether equivalent capabilities exist through other means at a particular facility. For CI, the standard is 2-2-2 (2 CSOs per 8-hour shift), all shifts, all days. For the facilities that procure CSOs under separate contracts, staffing is determined based on specific facility needs in terms of fulfilling required functions. CSO contracts must include the ability to increase staffing on short notice in response to incidents or threat information.

d. CSO Site Supervisor. The contractor must identify a CSO site supervisor. The site supervisor is the contractor's day-to-day representative on site and must:

(1) Ensure CSO staff compliance with all contract requirements.

(2) Have two years of facility protection experience at a level commensurate with the scope of work of an FAA contract.

(3) Where operations allow, the Site Supervisor may be part of the CSO working staff for their duty shift if they meet the qualifications set forth for individual CSOs.

(4) Ensure that each post is staffed as required, that employees are properly uniformed and present a neat appearance, and that each employee is familiar with their post and duties and is fully certified.

(5) Be available at all times to receive and implement orders or special instructions from the CO, COR, or contract technical representative during emergency situations concerning matters that affect the operation, protection, or security of assigned areas.

5-3. Selecting a CSO Provider. At a minimum, the vendor must:

a. Have five (5) years of experience in the field providing services to facilities similar in size to FSL 3 and 4 facilities.

b. Possess all appropriate and required state, local, territorial, and tribal certifications and licenses.

c. Be able to provide the site-specific staffing requirements.

5-4. CSO Standards.

a. Personnel Security Responsibilities. CSOs must meet the investigative requirements of FAA Order 1600.1 for moderate-risk positions unless otherwise noted in contract language. CSOs will receive the security clearance necessary based on facility operations. The contractor must immediately report to the CO/COR any subsequent derogatory information on any employed CSO. This includes any arrest, unauthorized Controlled Unclassified Information (CUI) disclosure, or other violations of FAA policy or directives as contained in AMS contract clauses.

b. Personal Qualifications. CSOs must: be U.S. citizens; be at least 21 years of age; possess at least a high school diploma or GED; and speak, read, and write English. Any person who has been convicted of any crimes of domestic violence is ineligible for any FAA CSO position.

c. Professional Experience. CSOs must either have: three (3) years of security experience within the past five (5) years; or earned an associate degree in a security or law enforcement-related field plus one (1) year of practical experience; or three (3) years of military experience (active, reserve, or national guard) and either be currently serving or have been honorably discharged; or successfully completed a state-certified Police Officers Standard Training certification course.

d. Training and Licensing. All CSOs must be fully trained, qualified, and certified or licensed as appropriate before being assigned an FAA post.

(1) The contractor must submit documentation of successful completion of all required training by each CSO to the COR. These records must provide the name and location of the

training facility, the date and times of training courses, and who conducted the training. The COR will accept any of the CSO's current unexpired certifications and qualifications if they meet current FAA requirements for certification and qualification. Where no state certification is required, the contractor must provide a training plan for CSOs. AXF should be consulted to assist in reviewing this training plan. This training plan must be reviewed by the COR and approved by the CO in advance of use by the contractor.

(2) The contractor must ensure that all CSOs possess all appropriate and required state, local, territorial, and tribal weapons permits and armed or unarmed CSO certifications, as applicable, needed to perform CSO services in their respective jurisdiction of employment.

(3) Initial and Recurring Training Requirements. Table 5-1 lists the required initial training. Those topics followed by an asterisk (*) are recurring and require annual certification. Records will be maintained by the contractor and be available for review by the COR or AXF.

Table 5-1. Initial and Recurring* CSO Training Requirements

Topic	Focus
Human Interaction	Communication skills and human behaviors that lead to effective security job performance
Jurisdiction and Authority*	Detention, apprehension, inspection, seizure, and use of deadly and secondary force
Use of Deadly Force*	Deadly force may be used only in those circumstances where the CSO reasonably believes that either they or another person are in imminent danger of death or serious bodily harm.
Use of Secondary Force*	A CSO must use only such force as is necessary to overcome any opposing force or threat. Training topics will include: • Four (4) hours of lecture and hands-on training on the use of Oleoresin Capsicum (OC) gel or foam. • Four (4) hours of lecture and hands-on training on the use of the baton. • Techniques and safe use of handcuffs.
First Aid, CPR, and AEDs*	Certified by the American Red Cross
FSP/OEP//FRB	Entry control, visitor screening, alarm response, vehicle inspection, mail inspection (where required), facility layout, and emergency equipment. Appropriately reacting to workplace violence, bomb threats, sabotage or vandalism, active shooter, and other criminal activity. Training will include the use of fire extinguishers. Must be re-reviewed whenever updated.
Security Officer Manual (SOM) and Post Orders	Reviewed and acknowledged.
Firearms*	• Eight (8) hours of classroom and 24 hours of live fire. Includes safe handling, cleaning, loading, and unloading. • Range qualification will be conducted on a State-approved range under the supervision of a certified range instructor and using the FPS course of fire. Passing score is 80%. • Certification will be in writing and will include the date, score, make, model, and serial number of the weapon, manufacturer's name, type and catalog/product number of ammunition, and printed and signed name of the certifying official.
Workplace Safety	Special emphasis on any hazardous materials stored at the facility.
Security Systems and Equipment	Operation and testing of Walk-Through Metal Detection Devices (WTMDD), Hand-Hand Metal Detector Devices (HHMDD) and X-ray

Topic	Focus
	machines. Demonstrate ability to operate all electronic security equipment installed and communications equipment used at the facility.
Reports	Report writing and submission requirements.

e. Uniforms and Equipment. The contractor must provide the equipment either specifically noted in this chapter or necessary to fulfill assigned duties as well as seasonally appropriate uniforms that provide a professional appearance in keeping with a federal contract security force. The National Institute of Justice (NIJ) conducts standards-based testing and comparative evaluations to ensure that equipment used in the field is safe and reliable and meets the needs of the users. CSO equipment, where tested by the NIJ, must meet NIJ standards. Minimum uniform and equipment requirements per SOW include:

(1) Firearms. The contractor will provide CSOs with their own pistol. The use of personal weapons is prohibited. Approved calibers are the .38 special, .40, or 9mm (9X19mm) revolver or pistol. More than one caliber may be carried at a given facility.

(a) The CSO must carry the same weapon by serial number and the same ammunition that they qualified with on the range. The contractor must have a process in place to randomly inspect the CSOs to ensure they are carrying the authorized/assigned firearms issued to them by the contracting company. The inspection must be documented and provided to the COR.

(b) Only the handgrips and sights of a firearm may be modified to meet the needs of the user. However, if modified, qualification must be performed with the changed item(s) in place, not simply removed and reinstalled before and after qualification.

(c) The contractor must provide a list of serial numbers of firearms that are used on the contract to the COR prior to the period of performance start date. The contractor and/or the CSO site supervisor must immediately report any changes to the inventory list to the COR. For accountability, the contractor and CSO site supervisor must maintain the current firearm inventory list on-site and provide a copy to the COR upon request for subsequent AXF review.

(d) While the FAA prefers that the contractor not store weapons on FAA facilities, firearms used by CSOs may be stored on FAA property. The contractor will maintain and provide the COR with a current list of the serial numbers of all firearms stored on FAA property. CSO firearms stored on FAA property will be stored unloaded in a container specifically designed for the storage of firearms. Firearms may not be stored in containers with ammunition, money, drugs, precious materials, evidence, or CNSI. The container need not be located in a locked room but must be out of sight of visitors and facility personnel and where it can be monitored by other CSOs. It must remain locked when not in use. The CSO supervisor will maintain combinations and keys; controls will follow requirements elsewhere in this order (see paragraph 4-3-14).

(e) Firearms maintenance and cleaning must be performed on a quarterly basis by the CSO. Maintenance must not occur while on duty and must be verified and documented by the CSO supervisor. A quarterly record will be maintained on-site by the CSO supervisor and available for SSE review.

(f) A clearing barrel or a bullet trap that is rated by the manufacturer for the caliber being carried will be available and used for the loading and unloading of firearms.

(g) While on duty, a CSO must not remove any firearm from its holster or carrier unless pursuant to use, retrieval to/from storage, or upon being ordered to surrender the firearm by a LEO, another CSO acting on the direction of the FAA, or employer. No unauthorized person will handle a CSO's firearm. Warning shots or firing at a fleeing person or a moving vehicle is prohibited.

(2) Ammunition. Ammunition must be from a U.S. commercial manufacturer and meet the weapon's manufacturer's recommended specifications. No subsonic, +P, +P+, or reloaded ammunition is authorized. The same type of ammunition used for qualification will be used on duty. Each CSO will carry a fully loaded firearm and two fully loaded magazines or speed loaders (as appropriate) for that firearm. Ammunition will be stored in a container specifically designed for the storage of ammunition. Ammunition may not be stored in containers with firearms, money, drugs, precious metals, evidence, or CNSI.

(3) CSO uniform and other equipment requirements are detailed in Table 5-2.

Table 5-2. CSO Uniforms and Equipment

Uniform and Equipment Components	Description
Boots/Pair	Quarter
Cap	Baseball Style
Cap	Faux Fur Trooper Style
Disposable Gloves	Single Use, Disposable
Double Magazine Case or Speed Loader Case	Nylon, Compatible with Specified Weapon
Duty Belt "Keepers"	Nylon
Expandable or Straight Police Baton	With Holder
Glove and Micro-shield Pouch	Nylon, Slide on Belt Type, Holds Set of Single Use Disposable Gloves and One (1) Single Use Disposable Micro-Shield
Gloves Winter	Pair
Handcuff Case	Nylon
Handcuffs and Keys	Meets NIJ 0307.01
Jacket Winter	Patrol Type
Jacket	Nylon Windbreaker
Key Strap with Flap	Nylon
Level II Firearm Retention Holster	Nylon, Slide on Belt Type with Hammer Safety Strap (Left/Right as Required)
Micro-shield	Single Use, Disposable
Nameplate	2-1/2" x 5/8" Metal Plate with Rounded Edges and ¼" Lettering Identifying First Initial and Last Name
Necktie	Clip-on
Oleoresin Capsicum (OC) or Combination OC-CS Orthoclorobenzalmalononitrile Canister	2.0-ounce Non-Flammable Flip Top Safety Canister with Gel or Foam Spray Pattern
OC Case	Nylon, Slide on Belt Type
Pistol Belt	Nylon without Shoulder Strap
Shirt, Long Sleeve	Insignia, Shoulder Patch
Shirt, Short Sleeve	Insignia, Shoulder Patch
Trouser	All Season Weight
Whistle	With Chain Attachment

Uniform and Equipment Components	Description
Flashlight	With Holder 2-D Cell

f. Medical Standards. A physician licensed in the US must determine a candidate CSO to be physically fit to perform the normal duty functions of a CSO. In general terms, this means that the CSO must be physically able to: remain alert with frequent and prolonged walking, standing, and sitting for up to 12 hours, stand without restroom relief for up to four (4) hours, use all issued equipment, occasionally run short distances, and be able to subdue and handcuff hostile persons. CSOs must undergo a pre-employment medical or physical examination and every three (3) years thereafter. The licensed physician must document the results and provide them to the COR for subsequent review by AXF, typically using a provided medical questionnaire. The following standards apply.

Table 5-3. CSO Medical Standards

Category	Standard
Vision	Binocular corrected to 20/30. No peripheral vision deficits, night blindness, or other condition that adversely affects job functions.
Hearing	Average hearing across 500, 1000, 2000, and 3000 Hz of 25 decibels or less and at 4000 and 5000 Hz of 45 decibels or less. If a hearing aid is used for testing, it must be worn on duty. No equilibrium disorders.
Speech	No impediment that interferes with communication to a degree that adversely affects job functions.
Cardiovascular	Aerobic capacity of 9 metabolic equivalent (MET) or 31.5 ml/kg/min VO2 max during standardized capacity test for six (6) minutes.
Musculoskeletal	Full range of motion, able to get down to and up from a kneeling position. Lift 40 pounds from floor to waist, bench press 40% of bodyweight.
Respiratory	Must be cleared to use disposable particulate respirators meeting N95 National Institute for Occupational Safety and Health (NIOSH) standards.
Other Physical Systems	Includes gastrointestinal, genitourinary, endocrine, metabolic, hematological, neurological, psychiatric, and dermatological systems. Must not interfere with safe and efficient completion of job functions.
Medications	The prolonged use (e.g., beyond 10 calendar days) of narcotics, sedative hypnotics, barbiturates, or amphetamines prescribed for a persistent or recurring underlying condition is a disqualifying factor.

g. Drug Testing.

(1) CSOs must submit to urine drug screening as part of initial and recurring (every three years) medical examinations. Additionally, the contractor must conduct a random screening of 10 percent of CSOs over a 12-month period and provide reports of those results to the COR. CSOs are screened for nine (9) substances at the following cutoff levels:

Table 5-4. Cutoff Levels for Drug Tests

Substance	Cutoff Level (ng/mL)
Marijuana metabolites (THCA)[2]	50 ng/mL[3]
Cocaine metabolite (Benzoylecgonine)	150 ng/mL[3]
Codeine/Morphine	2,000 ng/mL
Hydrocodone/Hydromorphone	300 ng/mL

Substance	Cutoff Level (ng/mL)
Oxycodone/Oxymorphone	100 ng/mL
6-Acetylmorphine	10 ng/mL
Phencyclidine	25 ng/mL
Amphetamine/Methamphetamine	500 ng/mL
MDMA[4] /MDA[5]	500 ng/mL

(2) A CSO will be automatically disqualified if the presence of a positive reading for any of the tested drugs is over the designated cutoff level. CSOs may not be permitted to take multiple tests to receive an acceptable reading.

(3) The CO may request that a CSO submit to drug screening when the government has reasonable belief that a CSO is on duty and under the influence of an intoxicating substance. Upon written request, the contractor must arrange for a test as soon as possible but no later than three (3) business days.

(4) Drug screening methodology must conform to the U.S. Department of Health and Human Services Substance Abuse and Mental Health Services Administration's (SAMHSA) "Mandatory Guidelines for Federal Workplace Drug Testing Programs." The contractor is urged to use laboratories endorsed by SAMHSA, but, if others are chosen, the contractor must verify that the laboratory's methodology conforms to SAMHSA's guidelines prior to utilizing the laboratory.

5-5. Contract Security Services Oversight. This paragraph outlines oversight requirements that are typically applicable for the ATO-sponsored national CSO contracts. Facilities (MMAC, WJHTC, and most regional offices) will adopt these measures to the extent possible and tailor them to accommodate their individual acquisition oversight needs. The following sub-paragraphs do not apply where Federal Protective Services (FPS) guard forces are used. FPS conducts their own oversight. With FPS, tenants are typically restricted to negotiating guard staffing and facility-specific duties.

a. Contract Administration. For the national CSO contracts, AXF and ATO personnel at the headquarters and service area level will ensure that the delivery of CSO services is consistent with the requirements of this order and/or any pre-existing SOW. Where facilities manage their own CSO contracts (e.g., MMAC and WJHTC), the SSE, the contracting logistics office, and the FM (or designee) will ensure requirements consistent with this chapter or a pre-existing SOW are met.

(1) The COR provides principal oversight of contract execution and may take such actions as necessary to ensure contract compliance. The COR may request assistance from AXF/SSEs in the evaluation and observance of training activities and will maintain required contract documents. The documents will be made available to AXF as necessary to facilitate guard/contract effectiveness evaluations.

(2) The Alternate Technical Representative (ATR) is the FM designee for facility-level CSO matters who provides oversight of CSO operations at the facility for compliance with contract terms.

(3) AXF provides headquarters-level oversight of the AJW-administered national CSO contract certifications and qualifications. AXF will conduct reviews of CSO records maintained by the COR and may assist in training validation as requested.

(4) SSEs provide facility-level oversight of CSO requirements as part of the comprehensive facility security assessment. SSE oversight parameters are contained in the Risk Assessment Tool (RAT).

b. CSO Records. In addition to the records required by the CO and COR, the contractor will maintain a current copy of individual CSO records that are listed in Table 5-5 on-site for SSE review for the length of the contract.

Table 5-5. CSO On-Site Records

On-Site Records	On-Site Records
Firearms Qualification State/Local/Territorial/Tribal Company Licensing	Initial/Recurring Training Documentation • Red Cross-approved CPR, First Aid, and AED • Baton Certification • OC Certification • Post Orders, FSP, OEP, and SOM Reviews

c. Use of Force Incident Reporting. All incidents involving CSO discharge of a firearm or use of non-lethal force equipment (e.g., OC spray, baton, or handcuffs) on FAA property will be reported immediately by the individual responsible or supervisor to the FM, ATR, and SSE. Reporting is required any time that a firearm is discharged for any reason, whether intentional or accidental, regardless of whether personal injury resulted from the discharge. If injury or criminal activity was involved, the local LE agency will be notified. The FM will preserve any CCTV recording of the incident for review.

(1) A written follow-up report will be completed and include:

(a) Name and duty assignment of the individual discharging the firearm/using force.

(b) Time of the event (date/day/hour).

(c) Reason or activity that resulted in the discharge of the firearm or use of force.

(d) A summary of any injuries, fatalities, or property damage resulting from the discharge. If an injury was sustained, then to the extent known, include identifying information of the victim (name, age, date of birth, etc.).

(f) Names of all witnesses having knowledge of the incident.

(2) The SSE will notify AXF management of the incident and the circumstances. Additional notifications will be as directed by AXF-1. AXF-1 will determine if the incident will be referred to AXI for further investigation.

5-6. CSO Operations. CSO Operations and duties are contained in three facility-specific documents: Post Orders, the FSP, and the SOM.

a. Post Orders. Post orders must be specific to the facility and include general orders, special orders, and temporary orders. Post orders must clearly describe the required duties and actions to be taken by CSOs at each post and include emergency response procedures. They will include daily operational testing of systems and screening equipment. AXF publishes templates that will be used by the FM or the ATR, with the assistance of the SSE, to develop needed post orders. An electronic copy of each post order will be forwarded to the COR for review and approval and to the SSE when developed and updated. Post orders will be available at each guard post.

(1) General orders. General orders apply to all posts and patrols for the CSO force as a whole and prescribe general performance criteria for CSO duties and responsibilities.

(2) Special orders. Special orders are issued to supplement general orders and prescribe duties and responsibilities related to a specific post or patrol, such as the location, duty hours, and staffing requirements. For example, special orders related to response requirements to IDS alarms in designated classified material open storage rooms must be included in the post orders.

(3) Temporary orders. Temporary orders prescribe duties and responsibilities and/or actions to be taken by CSOs during unusual conditions or situations. Temporary orders are situational and are issued for a finite period.

b. Facility Security Plan (FSP) and Occupant Emergency Plan. The FSP is a structured, site-specific security plan. For more information, see paragraph 4-6-9.

c. Security Officer Manual (SOM). The contractor must develop, issue, and maintain a comprehensive contractor SOM for each facility with a CSO assigned. The manual is intended to be a contractor-employee manual and will contain the basic guidance issued by the contractor to its employees concerning supervisory and employee responsibilities, detention of suspects and arrest powers, courtesy, communications, and chain of command. A detailed review of the SOM must be provided as part of each employee's initial training and each time the manual is modified to ensure the CSO has read the document. A copy will be maintained at each guard post.

Appendix A. Related Publications and References

National Directive	Directive Title	Publication Date
EO 12977	Interagency Security Committee	October 19, 1995
HSPD-12	Policies for a Common Identification Standard for Federal Employees and Contractors	August 27, 2004
PPD-7	Critical Infrastructure Identification, Prioritization, and Protection	December 17, 2003
PPD-21	Critical Infrastructure Security and Resilience	February 12, 2013
OMB-M-11-11	Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a common Identification Standard for Federal Employees and Contractors	February 3, 2011

Interagency Security Committee (ISC) Standards, Guides, and Best Practices	Publication Date
Risk Management Process: An Interagency Security Committee Standard	Current Edition
Risk Management Process: An Interagency Security Committee Standard, Appendix A: The Design Basis Threat Report	Current Edition
Risk Management Process: An Interagency Security Committee Standard, Appendix B: Countermeasures	Current Edition
Risk Management Process: An Interagency Security Committee Standard: Appendix C: Child Care Centers Template	Current Edition
Items Prohibited in Federal Facilities – An ISC Standard	Current Edition
ISC Violence in the Federal Workplace: A Guide for Prevention and Response	Current Edition
Planning and Response to an Active Shooter: An ISC Policy and Best Practices Guide	Current Edition
Best Practices for ASOs in Federal Facilities	Current Edition
GSA Mail Center Security Guide	Current Edition
ISC Occupant Emergency Programs: An Interagency Security Committee Guide	Current Edition

Order Number	Order Title	Publication Date
1600.1	Personnel Security Program	Current Edition
1600.2	Classified National Security Information	Current Edition
1600.6	Facility Security Policy	Current Edition
1600.8	Communications Security (COMSEC)	Current Edition
1600.12	Technical Surveillance Countermeasures Program	Current Edition
1600.25	Federal Aviation Administration (FAA) Official Credentials	Current Edition
1600.55	Reporting Threats Against the President, Other Government Officials, and Visiting Dignitaries	Current Edition
1600.61	International Travel Security Program	Current Edition
1600.71	Office of Security and Hazardous Materials Safety Special Agent Credentials, Badges and Job-Specific Credentials	Current Edition
1600.75	Protecting Sensitive Unclassified Information (SUI)	Current Edition
1600.78	Personal Identity Verification (PIV) Card and Other Identification (ID) Cards	Current Edition
1900.1	FAA Emergency Operations Plan	Current Edition
1910.1	FAA Continuity Plan	Current Edition

Appendix B. Construction Standards for Open Storage Secure Areas

B-1. Open Storage Secure Area. An open storage secure area is a room, suite, or special-purpose building with a mission requirement for recurring and/or continuous classified operations/work. This type of secure space can be approved for areas or rooms where the size of classified equipment, the nature of classified material, or the operational environment does not allow for storage in a GSA-approved security container. SSE approval procedures and requirements are listed in FAA Order 1600.2.

B-2. General Construction Requirements. The security measures identified in this appendix apply only to the secure room. The FSL of the facility that houses the room will determine other baseline LOP measures as described in chapter 4. The following criteria and standards apply to secure open storage areas. References to the secure area perimeter include all the walls that outline the secure area confines, floors, ceilings, doors, windows and penetration by ductwork, pipes, and conduit. It does not include interior walls that divide various work areas or conference rooms.

a. Walls Criteria.

(1) Construction Criteria. Walls will be of permanent construction materials, i.e., plaster over lath, gypsum wallboard, metal panels, hardboard, wood, plywood, concrete block, or other materials offering resistance to and evidence of unauthorized entry into the area. They will either extend from the true floor to the true ceiling and be attached with permanent construction materials or, if that is not feasible and visual access to classified material from outside the area is not possible, be secured with wire mesh, 18-gauge expanded steel screen or other equivalent barrier to extend and attach the perimeter wall up to the true ceiling. Existing walls that meet construction requirements may be used.

(2) Acoustic Criteria. See paragraph B-6 for additional information.

(a) To meet Sound Transmission Class (STC) 50 soundproofing, walls will consist of four layers of 5/8 inch-thick gypsum wallboard (GWB), two layers on the uncontrolled side of the secure area and two on the controlled side of the secure area to provide rigidity and acoustic protection (Sound Class 4).

(b) To meet STC 45 soundproofing, three layers of 5/8 inch-thick GWB, one layer on the uncontrolled side of the secure area and two on the controlled side of the secure area, to provide rigidity and acoustic protection (Sound Class 3).

(c) The following criteria apply for both STC 50 and STC 45 wall construction:

1. Attach wallboard to 3⅝ inch-wide metal studs placed 24 inches on center.

2. Anchor continuous runners (same gauge as studs) for securing studs to the true floor (bottom plate) and true ceiling (top plate) structures.

3. Mount the interior two layers of wallboard so that the seams do not align (i.e., stagger joints).

4. Install acoustical fill 3½ inches sound attenuation material, fastened to prevent sliding down and leaving a void at the top, between metal studs.

5. Seal the top and bottom of each wall with an acoustic sealant where it meets the slab and structural ceiling.

6. Treat and seal wall penetrations with acoustic material.

7. Finish and paint the entire wall assembly from true floor to true ceiling.

b. Ceilings and Floors Criteria. Ceilings and floors will meet the same standards for force penetration and acoustic protection as walls. All floor and ceiling penetrations will be kept to a minimum. False ceilings and raised floors are allowed but will not be considered as the actual perimeter boundary of the secure area.

c. Door Criteria.

(1) Perimeter doors will be a combination of wood core and metal clad equivalent to 18 gauge and 1¾ inch thick in total. Doors will either be designed to acoustical requirements (STC 45 or 50) or have sound seals and door sweeps installed and/or acoustic panels mounted on the inside door sleeve. They will comply with building, safety, and accessibility codes. Additionally,

(a) Hinge pins will be interior mounted or modified to prevent removal. They will be reinforced to a 7-gauge equivalent.

(b) Door closures will be reinforced to a 12-gauge equivalent.

(c) Pre-drilled lock areas will be reinforced to a 10-gauge equivalent.

(d) An automatic, non-hold door-closer will be installed on the interior.

(2) Primary entrance doors will be equipped with:

(a) A GSA-approved pedestrian door deadbolt meeting Federal Specification FF-L-2890B.

(b) A combination lock meeting Federal Specification FF-L-2740B.

(c) An approved access-control device (see Section B-11).

(d) An optional high-security keyway for use in the event of an access control system failure.

(3) Emergency exit doors will have no exterior hardware and be secured with deadlocking panic hardware on the inside that produces a local audible alarm when opened.

(4) Double doors will have one of the doors secured at the top and bottom with 1-inch deadbolts. An astragal strip will be attached to one door (could be either the secured or the movable door depending on the inward/outward swing of the door assembly).

d. Windows Criteria. Every effort must be made to minimize or eliminate windows, especially on a ground floor. Additionally, windows will be non-opening and be afforded visual and acoustic protection. Windows less than 18 feet above the ground or from the nearest platform affording access to the window, will be protected against forced entry and meet the perimeter protection standard for perimeter penetration described in paragraph B-2e. Acceptable methods are to fit windows with ½-inch-diameter steel bars, welded vertically and horizontally six inches on center, or 18-gauge expanded metal/wire mesh. Either will be fastened on the inside.

e. Perimeter Penetrations Criteria. All penetrations of the perimeter wall will be kept to a minimum. Utilities should enter the secure area at a single point.

(1) Electrical wiring, to include unclassified data and telephone cables, for the secure area can be installed within the walls, below raised floors, above false ceilings, and routed to receptacle or switch boxes mounted in the wall. Apply acoustical caulk in the area between the receptacle box and the wallboard to improve sound attenuation.

(a) Any unused extra wires must be removed or tied to earth ground.

(b) Metallic penetrations may require dielectric breaks.

(c) Installation of additional conduit penetration for future utility expansion is permissible provided the expansion conduit is filled with acoustic fill and capped (end of pipe cover).

(2) Vents and ducts will be protected to meet the acoustic requirements of the secure area. Walls surrounding duct penetrations will be finished to eliminate any opening between the duct and wall. All vents or duct openings that penetrate the perimeter walls of the secure area and exceed 96 square inches must be protected with permanently affixed bars or grills unless one dimension of the penetration measures less than six (6) inches or metal fire dampers are permanently installed and set no further than six (6) inches apart.

(a) If bars are used, they must be a minimum of ½-inch-diameter steel, welded vertically and horizontally six inches on center. Bars must be secured to the vent with tamperproof security screws.

(b) If grilles are used, they must be ¾-inch mesh, #9 (18 gauge), case-hardened, expanded metal; installed with tamperproof security screws.

(c) An access port installed within the secure area perimeter to allow for inspection of the area to ensure the access portal hasn't been tampered with or removed.

(3) Unencrypted cables and wiring carrying classified data must be readily accessible, easy to identify and inspect, and contained within the perimeter of the secure area. All classified data must be encrypted before it is transmitted outside the of perimeter of the secure area unless it is protected by an approved protected distribution system in accordance with CNSI No. 7003, Protected Distribution System (PDS).

B-3. Emergency Notification Systems Criteria. The introduction of electronic systems that have components outside the secure area perimeter is prohibited unless required for security purposes or by life-safety regulations. If so, all incoming wiring must enter the secure area perimeter at one point and one-way (audio) communication systems will have a high-gain amplifier.

B-4. Intrusion Detection Systems (IDS) Criteria. Secure areas will be protected by IDS when not occupied or otherwise protected by authorized personnel or inspected once every four (4) hours by a contracted security force or by an authorized employee. Interior areas of the secure area through which access could be gained, including walls common to areas not protected at the Secret (or higher) level, will be protected by the IDS.

a. System Requirements. IDS components and monitoring stations will comply with Underwriters Laboratories (UL) Standard for National Industrial Security Systems for the Protection of Classified Material, UL 2050, Extent 3 installation references. Installation will be completed by UL 2050 certified alarm service companies using persons with national security clearances equal to the level of classification the space(s) will protect. A copy of the UL 2050/CRZH (National Industrial Security Systems) certificate will be furnished to the SSE after installation of the IDS.

(1) Secure area perimeter doors, including the main entrance and emergency exit doors, must be protected by UL 634 High Security Sensors (HSS) that meet UL Level II requirements. Level II rated switches include Balance Magnetic Switch (BMS). All doors will be alarmed and monitored 24 hours per day.

(2) Areas will be protected using UL 639 listed infrared motion sensors. A sufficient number of UL 639 listed motion detection sensors will be installed in each conference room or work area, and one located to monitor the primary entrance door and emergency exit door, if necessary. Place motion detection sensors to detect four-step movement within the area.

(3) Intrusion detection equipment (IDE) wiring/cabling that extends beyond the secure area perimeter will employ supervised line security.

(4) Sensors are not required above false ceilings and below false floors.

(5) Wiring between all the sensors and the alarm control panel (ACP) will be dedicated to the system and have supervised line security.

(6) Access to IDS technical drawings, installation instructions, specifications, and all other applicable law and policy for the type(s) of SUI involved will be restricted in accordance with FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI).

b. Alarm Control Panel (ACP). The preferred location of the ACP is within the secure area, but if that is not possible, and it is located outside of the secure area, it will be protected with a shock or vibration detector to detect tampering of the equipment. ACPs will be protected with a tamper switch (plunger or magnetic).

(1) When the primary entrance door employs a delay to allow for changing the system mode of access, the delay will not exceed 30 seconds.

(2) Logins and passwords for the IDS and access codes will be protected and controlled by the Classified Information Security Manager (CISM) and/or Alternate CISM (ACISM).

(3) The CISM/ACISM will change maintenance and master profiles, PINs, or passcodes from their default settings to a unique PIN or passcode.

c. Alarm monitoring. Alarm status should be continuously displayed at the monitoring station. Additionally, alarms associated with a change in power status will include local annunciation. Alarms will include audible and visual annunciation for each and identify each activated sensor. Immediate and continuous alarm annunciations must occur for:

(1) Intrusion Detection

(2) Failed Sensor

(3) Tamper Detection

(4) Maintenance Mode (a maintenance message displayed in place of an alarm)

(5) IDE Sensor Points shunted or masked during maintenance mode

(6) A change in power status (AC or backup).

d. Testing.

(1) Acceptance testing will be conducted by the regional SSE on systems prior to operational use to provide assurance that the IDS meets all requirements of this section prior to the secure area accreditation for classified operations.

(2) Semi-annual IDS testing will be conducted to ensure continued performance.

(3) Records of testing and test performance will be maintained for three years in accordance with NARA GRS 5.6.

(4) Motion Detection Sensor Testing Criteria.

(a) All motion detection sensors will be tested to ensure activation of the sensor by movement of no more than four consecutive steps.

(b) The test will be conducted by taking a four-step trial, stopping for three to five seconds, and taking another four-step trial.

(c) Tests will be repeated throughout the secure area and from different directions.

(d) An alarm must activate at least three out of every four consecutive tests made by moving progressively through the secure area/work areas.

(5) Door Sensor Testing Criteria. All HSS devices will be tested to ensure that an alarm signal activates before the non-hinged side of the door opens beyond the thickness of the door from the closed position, e.g., the sensor initiates before the door opens 1¾ inch for a 1¾ inch door.

(6) Tamper Testing Criteria. Each IDS equipment cover will be individually removed or opened to ensure there is alarm activation at the Premise Control Unit (PCU) or monitoring station in both the secure and access modes. Tamper detection devices need only be tested when installed.

B-5. Physical Access Control System (PACS) Criteria. Secure area access is controlled by the CISM/ACISM assigned to the secure area to ensure access is restricted to authorized personnel.

a. System Requirements. Access will be controlled using an HSPD-12 PIV-card-compliant system. Two-factor authentication (PIV card and PIN) is required for entry. PIN compromises or lost PIV cards will be reported to the CISM/ACISM and removed from the system immediately upon discovery. Components will be secured as follows:

(1) Card readers, keypads, communication interface devices, and other access control equipment located outside the secure area will be tamper-protected and be securely fastened to a wall or other fixed structure.

(2) Electrical components, associated wiring, or mechanical links will be accessible only from inside the secure area.

(3) System data that is carried on transmission lines (e.g., access authorizations, personal identification, or verification data) to and from equipment located outside the secure area will be protected using Federal Information Processing Standards (FIPS) Advanced Encryption Standard (AES) certified encrypted lines. Equipment containing access-control software programs will be in the secure area.

(4) Electric door strikes installed in conjunction with a personnel PACS will have a positive engagement and be approved under UL 1034 for burglar resistance.

b. PACS Recordkeeping.

(1) Records will reflect the active assignment of authorized persons, level of access, entries, and other system-related information.

(2) Records and information concerning ID data, PINs, operating system software, or any other PACS-associated data, will be secured in the open storage secure area or, when unattended, secured in a GSA-approved container.

(3) Records of personnel removed from the system must be retained for three years from the date of removal in accordance with NARA GRS 5.6.

B-6. Acoustical Security. Sound travels through walls, above false ceilings, through ductwork, and through the opening between the door and its frame. A commonsense approach to acoustic security must be applied to protect classified conversations from being inadvertently overheard outside the perimeter of the area. If an area is specifically being planned and designed for amplified classified discussions/conferencing, contact the SSE early in the design process for enhanced acoustical security secure area [wall, ductwork] construction specification and products.

a. Sound Attenuation Determination. The acoustical standard for Secret and Top Secret classification levels is STC 45, which specifies that loud speech can be faintly heard but not understood from outside of the area, while normal speech is inaudible. STC 50 achieves the same standard when amplified conferencing is used.

b. Sound Attenuation Testing. A reasonable, practical, non-technical assessment of sound attenuation relative to the potential threats and associated risks at FAA facilities is achieved by conducting a sound test with two people. A person inside the area should speak in normal (or amplified, if conferencing systems are used) tones while a person outside determines if any of the speech can be heard or understood. The test will be conducted from multiple places inside/ outside of the area, with an emphasis on areas that have known attenuation concerns (e.g., doors, wall penetrating areas).

c. Improving Sound Attenuation Results. If the sound test fails to meet the standard, the techniques noted below may improve/raise the STC to an acceptable level.

(1) Determine if there is any additional stand-off distance within the secure area and the perimeter wall. If the additional space resolves the sound transmission concern, designate the compromised area as a “no [classified] discussion” area.

(2) Determine if there is additional stand-off/clear space available outside of the secure area that can be cleared or otherwise controlled to resolve any transient sound leakage.

(3) Install sound gaskets, seals, and/or floor sweeps on the door sleeve and/or its frame.

(4) For existing secure areas, replace the exterior doors with doors described in Door Criteria section above (see paragraph B-2c).

(5) Install sound absorption material to the interior walls and doors, as applicable. Use materials such as sound-absorbing tiles/panels, sound-absorption paint, or an extra layer of drywall.

(6) Install a sound masking system that generates white noise onto interior wall surfaces and/or interior side of door.

(7) Install insulation within a wall or floor/ceiling cavity.

(8) Install metal sound baffles or “Z” [shaped] sound reduction duct sections in the secure area HVAC system.

Appendix C. Security Requirements for Flight Standards District Offices (FSDO)

C-1. Purpose. FSDOs are designated administrative facilities. The baseline LOP security countermeasures identified in chapter 4 for the respective facility security level apply except where adjusted below in Table C-1.

C-2. Adjusted Security Countermeasures. Table C-1 lists chapter 4 LOP baseline countermeasures that are adjusted for FSDOs.

Table C-1. Adjusted Security Countermeasures for FSDOs

Security Countermeasure	Reference	See:
Blast Resistance – Windows	Table 4-2-1 and paragraph 4-2-2	C-3
Security of Critical Areas	Table 4-4-1 and paragraph 4-4-4	C-4
VSS Coverage	Table 4-5-1 and paragraph 4-5-2	C-5
Duress Alarms or Assistance Stations	Table 4-5-1 and paragraph 4-5-8	C-6

C-3. Blast Resistance – Windows. The receptionist position will:

a. Have bullet-resistant glass installed at the customer service window. The glazing will be UL-752 rated at level 3, which protects against handguns with ammunition of a muzzle velocity of 1,175 to 1,485 feet per second.

b. Utilize a customer service window that includes a pass-through shelf at the receptionist's position. The pass-through shelf will not allow a typical person's hand to reach into the security side of the window.

c. Have the limited area surrounding the customer service window hardened and provide at least the same protection as the installed glass (five feet on each side extending from floor to ceiling). *Note: AXF can provide installation designs that accommodate this requirement.*

d. Doors that allow entry into the FSDO working areas from the public areas that are located directly to the left or right of the customer service window shall meet the UL-752 rating at level 3.

C-4. Security of Critical Areas. Access to telecommunication rooms (demarcation points) will be secured as specified for critical areas in paragraph 4-4-4 and Table 4-4-1.

C-5. VSS Coverage. Entry control video and a capability to remotely unlock the door will be provided at the main door that allows public access to the FSDO vestibule.

C-6. Duress Alarms or Assistance Stations. A duress alarm will be installed at the receptionist position and in each interview and examination room. The alarm, at a minimum, will alert employees in the FSDO working areas of a duress situation. If the capability exists, the FM may arrange for the duress alarm to be monitored at an off-site facility (e.g., commercial alarm company, local law enforcement).

Appendix D. Security Requirements for Child Care Centers (CCC)

D-1. Purpose. This appendix establishes security requirements for childcare centers (CCC) housed in FAA facilities or located on FAA property. Because of the varying contract arrangements associated with FAA CCCs, they do not align well with ISC standards and guidelines. It is also assumed that state, local, territorial, and tribal licensing obligations will impose security and safety requirements. In the event of a conflict, the more stringent security measure will take precedence.

D-2. Security Countermeasures. CCCs that are housed within FAA facilities are supported by the security measures associated with the sponsoring facility in addition to those listed in Table D-1. For those CCCs not housed within an FAA facility, only those security measures listed in Table D-1 apply. CCCs will be assessed at the frequency of the sponsoring/co-located FAA facility.

Table D-1. Security Countermeasures for CCCs

Security Countermeasure	Reference	In Facility	On Property
Perimeter Doors and Door Locks	Table 4-3-1 and paragraph 4-3-13	D-3	D-3
Security of Critical Areas	Table 4-4-1 and paragraph 4-4-4	D-4	
VSS Monitoring and Recording	Table 4-5-1 and paragraph 4-5-3	D-5	D-5

D-3. Perimeter Doors and Door Locks.

a. In cases where the main entrance to the CCC opens into an interior CCC reception area, the main entrance door can be a storefront door. In this situation, the interior door (control door) must be a metal or solid core wood door with a view panel and remote release capability and will be installed between the CCC reception area and the actual childcare space. The main entrance (storefront) door may also have a remote release capability if desired by CCC management.

b. In cases where the main entrance door opens directly into the childcare space, it becomes the control door and must meet standard exterior door construction standards in paragraph 4.3.13. This door must also be equipped with remote release capability.

c. Stand-alone electronic or mechanical access control will be installed at the control door in addition to the FAA standard lock system.

D-4. Security of Critical Areas. Except for PACS, which is not required for CCCs, the requirements for security level 3 CI facilities apply. Facility CCCs will be treated as critical areas and will limit access into the area, install FAA standard locks on doors, and use VSS to monitor entry.

D-5. VSS Monitoring and Recording. If it can be accommodated, VSS will be monitored by CSOs. If CSOs are not utilized or it is not feasible to integrate cameras into the existing monitoring system, cameras will be recorded.

Appendix E. Security Requirements for the MMAC and WJHTC

E-1. Purpose. This appendix identifies security requirements for MMAC and WJHTC. Because of the size and unique operations at these Centers, some of the baseline LOP measures contained in chapter 4 do not readily apply. Security requirements specifically addressed in this appendix supersede those identified elsewhere in this order. Where this appendix is silent, the requirements elsewhere in this order apply.

E-2. Comprehensive Assessments. As the Centers are designated FSL 4 campus facilities that contain several lower FSL facilities within the perimeter, an annual comprehensive assessment of each Center's "shared" security countermeasures (CSOs, fences, etc.) will be conducted. Separate assessments will be completed for each facility at the frequency required for the facility's FSL. Risk assessment tools will be adjusted to accommodate these variations.

E-3. Adjusted Security Countermeasures. Table E-1 lists chapter 4 LOP baseline countermeasures that are adjusted for the Centers.

Table E-1. Adjusted Security Countermeasures for MMAC and WJHTC

Security Countermeasure	Reference	See:
Pedestrian Access to Site	Table 4-1-1 and paragraph 4-1-4	E-4
Site Lighting	Table 4-1-1 and paragraph 4-1-6	E-5
Vehicle Access to Controlled Parking	Table 4-1-1 and paragraph 4-1-11	E-6
Blast Resistance – Façade and Structure	Table 4-2-1 and paragraph 4-2-3	E-7
Visitor Access Control	Table 4-3-1 and paragraph 4-3-5	E-8
VSS Coverage	Table 4-5-1 and paragraph 4-5-2	E-9
Security Force Fixed Post – Exterior	Table 4-6-1 and paragraph 4-6-5	E-10
Security of Critical Areas	Table 4-4-1 and paragraph 4-4-4	E-11

E-4. Pedestrian Access to Site. The SSE may approve the installation of non-standard fencing to mitigate RADAR interference issues and other operational requirements. The deviation from the baseline and the rationale will be documented by the SSE in the assessment report(s).

a. MMAC. Perimeter fencing for facilities within the campus perimeter are met by the MMAC perimeter fence that is currently installed and related protections.

b. WJHTC. The WJHTC is enclosed by a 10-foot security fence with a 1-foot top guard/outrigger in most areas. Perimeter fencing for facilities within the campus perimeter are met by the WJHTC perimeter fence and related protections.

E-5. Site Lighting. Perimeter lighting is not required. Lighting will be designed for the typical movement and protection of personnel around buildings and parking areas and will be sufficient for security operations and camera systems. Installation of non-visible (infra-red), energy-efficient, and sensor-controlled lighting systems is permitted.

E-6. Vehicle Access to Controlled Parking. Electronic access during non-peak or elevated security conditions is permitted.

E-7. Blast Resistance – Façade and Structure. Blast resistance countermeasures will be assessed at the individual facility level. The Centers' controlled perimeter further mitigates risk.

E-8. Visitor Access Control.

a. Entry Control for Public Areas. Public areas are defined as streets, parking areas, and facilities where access within the facility perimeter is not controlled.

(1) FAA employees permanently assigned or on temporary duty, and non-FAA personnel with mutually honored ID are authorized unescorted access to public areas. At WJHTC, FAA personnel assigned to the facility who have a valid temporary PIV card are allowed unescorted access provided they sign in at the Security Operations Center (SOC) each day until a permanent PIV card is issued.

(2) MMAC. Visitors on official business (to include non-FAA students) and their vehicles may be authorized unescorted access to public areas as determined by the FM and the SSE. Frequent visitors on official business may be issued the appropriate ID/vehicle media provided FAA security requirements (or their equivalent) are satisfied. Non-frequent or one-time visitors must be screened, and their vehicles inspected by security guards. The SSE will take additional measures to control infrequent or one-time visitors by limiting their number, designating specific parking, etc.

(3) WJHTC. Visitor vehicles are not normally permitted past the main gate. Visitors are required to use the shuttle bus. Exceptions for deliveries and frequent visitors may be made. Procedures for these activities will be documented in the Center's FSP.

b. Escort Exceptions. The MMAC FM may waive continuous escort requirements for foreign national students (see paragraph 4-3-5i).

E-9. Video Surveillance System (VSS) Coverage. Perimeter surveillance may be met by exterior pan-tilt-zoom (PTZ) or fixed CCTV cameras that allow guards to observe activity in approach and travel areas and allow the guard force to virtually patrol the campus. Cameras supporting exterior alarmed points will provide an external view to assist in recording suspect activity and persons in the immediate area of the alarmed point. At MMAC, alarm assessment is required at each special entry door identified through the assessment process.

E-10. Security Force Fixed Post – Exterior. Armed CSOs will control vehicle and pedestrian entry points, respond to alarms, and perform screening duties as required. Unarmed security personnel may be used for escort, loss prevention duties, screening of mail, and other support roles as needed in coordination with the SSE. These site-specific procedures must be included in guard post orders.

E-11. Security of Critical Areas. WJHTC has critical areas that may not meet the definition of critical operations areas, as defined in paragraph 4-4-4, but based on specific operations at WJHTC, are critical to the FAA. The FM and SSE will identify these areas and determine what security countermeasures are needed using the BOE process described in paragraph 3-4.

Appendix F. Security Requirements for Air Route Surveillance RADAR Joint Surveillance System (ARSR-JSS) Facilities with COMSEC and Common ARSR (CARSR) Facilities

F-1. Purpose. ARSR-JSS and CARSR facilities are protected as FSL 2 CI facilities whether they are considered staffed or unstaffed. However, due to the unique mission and design of these facilities, there are several adjustments made to the baseline LOP. Table F-1 identifies the adjusted security countermeasures. These adjustments take precedence over chapter 4. If the countermeasure is not listed, the requirements in chapter 4 for FSL 2 CI facilities apply.

F-2. Adjusted Security Countermeasures. Table F-1 lists chapter 4 LOP baseline countermeasures that are adjusted for ARSR-JSS and CARSR facilities. For ARSR-JSS facilities that no longer house COMSEC and do not process CNSI, the facility will be assessed as a CARSR.

Table F-1. Adjusted Security Countermeasures for ARSR-JSS/CARSR Facilities

Security Countermeasure	Reference	CARSR	ARSR-JSS
Restricted Areas and Significant Areas and Assets	Table 4-1-1 and paragraph 4-1-7		F-3
Vehicle Access to Controlled Parking	Table 4-1-1 and paragraph 4-1-11	F-4	F-4
Burglary Resistance of Windows	Table 4-2-1 and paragraph 4-2-6		F-5
Walls and Non-window Openings	Table 4-2-1 and paragraph 4-2-7		F-3
Protection of Air Intakes	Table 4-2-1 and paragraph 4-2-9	F-3	F-3
Employee Access Control	Table 4-3-1 and paragraph 4-3-4	F-6	F-6
Visitor Access Control	Table 4-3-1 and paragraph 4-3-5	F-7	F-7
Perimeter Doors and Door Locks	Table 4-3-1 and paragraph 4-3-13		F-8
Control of Keys and Access Media	Table 4-2-1 and paragraph 4-3-14		F-8
Emergency Exit Doors	Table 4-3-1 and paragraph 4-3-16		F-8
Security of Critical Areas	Table 4-4-1 and paragraph 4-4-4		F-8
Building Systems and Roof Access	Table 4-4-1 and paragraph 4-4-5		F-3/F-8
VSS Coverage	Table 4-5-1 and paragraph 4-5-2	F-9	F-9
VSS Monitoring and Recording	Table 4-5-1 and paragraph 4-5-3	F-9	F-9
VSS Surveillance Advisory	Table 4-5-1 and paragraph 4-5-5	F-9	F-9
IDS Coverage	Table 4-5-1 and paragraph 4-5-6		F-10
IDS Monitoring	Table 4-5-1 and paragraph 4-5-7	F-11	F-11
Security Operations Management	Table 4-6-1 and paragraph 4-6-4	F-12	F-12
Facility Security Plan	Table 4-6-1 and paragraph 4-6-9	F-13	F-13
Occupant Emergency Plan Testing	Table 4-6-1 and paragraph 4-6-10	F-13	F-13
Availability of Emergency Plans and Documentation	Table 4-6-1 and paragraph 4-6-11	F-13	F-13

F-3. Restricted Areas and Significant Areas and Assets. Vents, ducts, and other openings that penetrate the ARSR-JSS building and have an area of 96 square inches or greater will be protected by using ½-inch steel bars installed on not more than 6-inch centers, with cross bars to prevent spreading. The bars must be securely anchored or fastened to the structure by welding. As an alternative measure to using bars, the openings can be covered with expanded metal (18 gauge) affixed to a 1-inch metal channel frame secured to the building structure with security

screws. Entry hatches to RADAR facilities will be secured with dead bolts that meet FAA standard lock requirements.

F-4. Vehicle Access Points. GCV is not required at CARSR/ARSR-JSS facilities.

F-5. Burglary Resistance of Windows. New ARSR-JSS buildings will not include windows in the design. For pre-existing buildings with windows, the windows will be secured in a permanent manner to prevent them from being opened. Any windows in the equipment room will be opaque to deny observation of internal operations. Windows in the interior administrative area do not need to be opaque. Windows less than 18 feet above ground level will be protected in the same manner as other building openings (see F-3).

F-6. Employee Access Control. PACS is not required at CARSR/ARSR-JSS facilities.

F-7. Visitor Access Control. The use of visitor IDs is not required at unstaffed CARSR/ARSR-JSS facilities.

F-8. Perimeter Doors and Door Locks.

a. Doors Accessing COMSEC Secure Rooms at ARSR-JSS Facilities. ARSR-JSS facilities are configured with a secure room (often referred to as the 'equipment' room) that protects classified COMSEC equipment. Doors leading into this area will be kept to a minimum. The main door leading into this area, whether from outside the facility or from another interior room of the facility, will be of sufficient strength to resist forceful entry and will be equipped with a combination lock meeting Federal Specification FF-L-2740B. Combinations to the lock will be controlled as required in FAA Order 1600.2. Any additional or alternate doors to this area will be of the same construction and be protected with an FAA standard locking system with a unique key and 1-inch deadbolt. The unique key will be maintained by the SOC desk at the servicing ARTCC. Panic hardware is authorized, but it must operate the FAA standard locking system installed on the door. Any doors leading to this area will be equipped with heavy-duty automatic door closers. Doors that are used in pairs will incorporate an astragal.

b. Telecommunications (TELCO) Rooms. TELCO room doors will be uniquely keyed from other site keys.

F-9. VSS Coverage. VSS and associated monitoring, recording, and advisory notices as well as GCV and ECV are not required at CARSR/ARSR-JSS facilities.

F-10. Intrusion Detection System (IDS) Coverage. IDS coverage for CARSR/ARSR-JSS facilities will adhere to paragraph 4-5-6 for FSL 2 CI facilities. However, ARSR-JSS COMSEC secure areas (equipment room) have these additional requirements:

a. A level II high-security switch on each perimeter door.

b. A 360-degree IR motion sensor within the room.

c. An arming/disarming unit installed to enable operation modes (access and secure). The 'access' mode will be used for authorized entry and will not generate an alarm. The 'secure' mode will generate an alarm. The arming/disarming unit's preferred location is near the facility's (not the secure area's) main entrance door. Doors that have the potential to be used for exit will incorporate a request-to-exit device that will prevent alarm generation upon egress.

F-11. IDS Monitoring. SSEs must ensure that the SOC Desk at the servicing ARTCC conducts real-time monitoring of the IDS, and has updated emergency contact information, in response to alarms, including 7-digit number to emergency responses, as the facility may be in a different jurisdiction. Alarm data is maintained within the Environmental Remote Monitoring Subsystem (ERMS). Alarm signal line supervision and protection against tampering will be provided between the monitoring station, control unit, IDS sensors, and arming/disarming unit.

F-12. Security Operations Management. The manager who has oversight of these facilities will assign a FM.

F-13. Facility Security Plan (FSP). FSPs OEP testing, and FRBs are not required at unstaffed CARSR/ARSR-JSS facilities. For staffed CARSR/ARSR-JSS facilities, FSPs and FRBs will follow the template provided by AXF for FSL 1 facilities. Plans availability only applies to staffed CARSR/ARSR-JSS facilities.

Appendix G. Security Requirements for Sponsor-Owned or Sponsor-Leased Federal Contract Towers (FCT)

G-1. Purpose. Sponsor-owned/leased Federal Contract Towers are air traffic control towers not owned by the FAA but "sponsored" by another entity, typically an airport authority, and are designated facility security level (FSL) 1A facilities under this order. Security countermeasures for these facilities will use the FSL 1 criteria in chapter 4 unless adjusted in Table G-1 below. FAA-owned/leased FCTs are considered FSL 1 facilities and the criteria in chapter 4 apply without adjustment.

G-2. Adjusted Security Countermeasures. Table G-1 lists chapter 4 LOP baseline countermeasures that are adjusted for sponsor-owned or sponsor-leased FCTs.

Table G-1. Adjusted Security Countermeasures for Sponsor-Owned/Leased FCTs

Security Countermeasure	Reference	See:
Identification of a Federal Facility	Table 4-1-1 and paragraph 4-1-2	G-3
Pedestrian Access to Site	Table 4-1-1 and paragraph 4-1-4	G-4
Regulatory Signage	Table 4-3-1 and paragraph 4-3-3	G-5
Employee Access Control	Table 4-3-1 and paragraph 4-3-4	G-6
Visitor Access Controls	Table 4-3-1 and paragraph 4-3-5	G-7
Facility Security Plan	Table 4-6-1 and paragraph 4-6-9	G-8
Occupant Emergency Plan Testing	Table 4-6-1 and paragraph 4-6-10	G-9
Availability of Emergency Plans and Documentation	Table 4-6-1 and paragraph 4-6-11	G-10
Protection of Construction Information	Table 4-6-1 and paragraph 4-6-12	G-11

G-3. Identification of a Federal Facility. "US property" signs are not required.

G-4. Pedestrian Access to Site. The use of fence standards prescribed in chapter 4 are not required. The FCT requirement is a 6-foot chain link or ornamental fence with no special security (e.g., barbed wire or outriggers) additions.

G-5. Regulatory Signage. Required signs are limited to "No Weapons" and "Restricted"/ "Closed" Area (as applicable) signs. Sponsor owned/leased FCTs cannot request signs through the Logistics Center Support System (see paragraph 4-3-3). Locally produced signs are authorized.

G-6. Employee Access Control. Facility managers may allow unescorted entry to personnel who do not possess FAA ID consistent with operational requirements. When doing so, the FM must restrict access to non-sensitive areas and, when not possible, provide some oversight or controls over the person's activities. Personnel allowed access under these provisions must still be entered on a Visitors Register (see paragraph G-7).

G-7. Visitor Access Controls. Unless exempted under paragraph G-6, visitor access controls in paragraph 4-3-5 apply. Visitors and those exempted under paragraph G-6 will be recorded on a Visitors Register.

G-8. Facility Security Plan (FSP). An FSP is not required.

G-9. Occupant Emergency Plan (OEP) Testing. Associated OEP testing and an FRB are not required.

G-10. Availability of Emergency Plans and Documentation. See paragraphs G-8 and G-9.

G-11. Protection of Construction Information. There are no requirements or special measures that apply.

Appendix H. Security Requirements for Mobile Asset Deployment Centers (MADC)

H-1. Purpose. MADC facilities store FAA assets and stage mobile tower units until deployed and are used to conduct maintenance and report activities. MADC facilities are designated FSL 2 critical infrastructure, and baseline LOP countermeasures in chapter 4 apply except where modified by this appendix.

H-2. Adjusted Security Countermeasures. Table H-1 lists those chapter 4 LOP baselines countermeasures that are adjusted for MADCs.

Table H-1. Adjusted Security Countermeasures for MADCs

Security Countermeasure	Reference	See:
Video Surveillance System (VSS) Coverage	Table 4-5-1 and paragraph 4-5-2	H3
Facility Security Plan (FSP)	Table 4-6-1 and paragraph 4-6-9	H4
Occupant Emergency Plan Testing (OEP)	Table 4-6-1 and paragraph 4-6-10	H4
Availability of Emergency Plans and Documentation	Table 4-6-1 and paragraph 4-6-11	H4

H-3. Video Surveillance System (VSS) Coverage. GCV and ECV are not required at MADCs.

H-4. Facility Security Plan (FSP). FSPs and FRBs are not required at unstaffed MADCs. When staffed, OEP testing, FSPs and FRBs are required and will follow the template provided by AXF for FSL 2 facilities. FSP availability only applies to staffed facilities.

Appendix I. Definitions

Term (Acronym)	Definition
Access	A means of entering or approaching a place, or the opportunity or right to experience or make use of something.
Agency Checks	Checks made to Departments or Agencies that are responsible for maintaining investigation or clearance databases.
Air Route Surveillance RADAR/Joint Surveillance Site (ARSR/JSS)	One in a network of long-range surveillance RADARs, primarily operated and maintained by the FAA, but providing communication and RADAR data to both FAA and USAF control centers.
Air Traffic Control System Command Center (ATCSCC)	The principal element of the Systems Operations Division of the Air Traffic Organization (ATO) and is responsible for the real-time command, control, and oversight of the NAS.
Based On Evaluation	The process of adjusting the baseline LOP during a facility security assessment by adding or removing countermeasures. When this occurs, the baseline LOP is adjusted to become the necessary LOP for that specific facility.
Baseline Level of Protection	The degree of security provided by the set of countermeasures for each facility security level that must be implemented unless a deviation (up or down) is justified by the risk assessment.
Camera Site Mapping or Site Plan	A graphic representation of where cameras are located at the facility. This is typically found in the PACS (e.g., P2000 or Lenel).
Campus	Two or more federal facilities located on one site and typically sharing some aspects of the environment, such as parking, courtyards, private vehicle access roads, fencing or gates, and entrances to connected buildings.
Civilian Process Server	An individual who is not a LEO and who delivers important court documents to officially notify an individual or party of their involvement in a legal court proceeding.
Classified National Security Information (CNSI)	Information that has been determined pursuant to Executive Order 13526 or any successor order thereto to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
Closed Circuit Television (CCTV)	A closed television system used within a building or complex to visually monitor a location or activity for security. Broadcasting in analog or digital format, it transmits over a closed circuit comprised of electrically conducting cable, fiber-optic cable, or wireless transmission.
Comprehensive Assessment	A formal onsite review and evaluation of all aspects of the FSMP at a facility by AXF.
Compromise	The unauthorized disclosure of classified information to persons who are not authorized to receive it. (Note: Generally, persons

Term (Acronym)	Definition
	who do not have a valid security clearance and need to know, as well as meet all other applicable access requirements, are not authorized for access to CNSI. See Order 1600.2 for additional information.)
Consequence	The level, duration, and nature of the loss resulting from an undesirable event.
Controlled Unclassified Information (CUI)	The term Controlled Unclassified Information (CUI) has the meaning given that term in 32 C.F.R § 2002.4(h).
Critical Area	An interior or exterior area to which unescorted access is limited to specified personnel. Critical areas may be termed critical operations areas (those that house critical NAS components or operations) or critical administrative areas (those that involve the use, storage, or processing of information requiring special protections, such as CNSI or CUI).
Critical Infrastructure (CI)	For the purposes of this order, FAA CI includes those air traffic facilities that provide air navigation services, which enable the operation of the National Airspace System (NAS) or house air navigation service capabilities that contribute to national defense, homeland security, law enforcement, and national response efforts to protect the nation from threats involving the air domain. Those facilities are ARTCCs, TRACONs, ATCTs, Combined ATCT/TRACONs, CERAPs, ATCSCC, CARSRs, and ARSR/JSSs.
Design-Basis Threat (DBT)	An ISC report published annually that establishes a profile of the types, composition, and capabilities of adversaries.
Designated Official (DO)	The highest-ranking official of the largest agency occupying a multi-agency federal facility, or a designee mutually agreed upon by officials of each occupant agency.
DOT/FAA ID Media	A term that encompasses all forms of authorized DOT/FAA ID including, but not limited to, PIV cards, other ID cards, credentials, and badges (refer to the latest editions of Orders 1600.25 and 1600.78).
Entry Control	Practices, processes, procedures, and/or equipment intended to deny or limit access into an area, facility, or designated room in order to protect personnel, infrastructure, and critical assets.
Entry Control Video (ECV)	A specialized CCTV surveillance system that allows remote audio/visual monitoring and activation of electronic door release systems.
Escort	An authorized FAA employee or contractor assigned to accompany a visitor or a visiting group to maintain visual and voice control of the visitor(s) and ensure they are not permitted access to areas, information, or equipment beyond the scope of their visit.

Term (Acronym)	Definition
Exterior Setback	The distance from the face of the facility's or building's exterior (the building's skin) to the uncontrolled perimeter accessible by any motorized vehicle.
FAA Personnel	FAA federal employees, FAA contractors, and non-employees (see definition below) as defined in FAA Order 1600.1, Personnel Security Program, regardless of their assigned duty location.
Facility	Space built or established to serve a particular purpose. The facility is inclusive of a building or suite and associated support infrastructure (e.g., parking or utilities) and land.
Facility Manager (FM)	The highest-ranking resident manager (or as otherwise identified by the owning line of business (LOB) or staff office (SO) in an FAA-owned or leased facility. When there is no resident manager, it will be the manager(s) having responsibility for facility operations and/or maintenance.
Facility Security Checkpoint	A designated location staffed and equipped to verify identification, screen visitors, inspect vehicles, process deliveries, and receive mail.
Facility Security Committee (FSC)	A committee responsible for addressing facility-specific security issues and approving the implementation of security measures and practices. The Facility Security Committee consists of representatives of all federal tenants in the facility, the security organization, and the owning or leasing department or agency. In the case of new construction or pending lease actions, the FSC will also include the project team and the planned tenant(s).
Facility Security Level (FSL)	A numeric categorization based on the analysis of several security-related facility factors, which serves as the basis for the implementation of countermeasures specified in ISC standards.
Facility Security Management Program (FSMP)	The FSMP establishes security requirements at facilities for which the FAA is responsible for security oversight, as described in chapters 3 and 4 of this order.
Facility Security Plan (FSP)	A plan that provides direction to key personnel on the security management and policies of a building or facility.
Facility Security Team (FST)	FAA Order 1600.6 identifies FST, formerly the FSRM program office, as the office responsible for FSMP implementation.
Federal Contract Tower (FCT)	A government-owned or airport sponsor-owned/leased Air Traffic tower staffed by non-government controllers under federal contract.
Foreign Civil and Military Dignitaries	Any person(s) holding a high, dignified position or office in the government of any foreign country or of any political subdivision of a foreign country. This includes senior leadership in foreign government aviation, foreign aviation industry

Term (Acronym)	Definition
	leadership, as well as senior officials in international aviation organizations.
Foreign National	Any citizen or national of a country other than the U.S. who has not immigrated to the U.S. and who is not a lawful permanent resident (LPR) of the U.S.
Gate Control Video (GCV)	A system that provides visual and audio coverage of facility access points and allows an operator to identify and assess persons prior to allowing access to the facility.
GSA-Approved Container	GSA-approved security containers are primarily used to store classified documents, components, and materials. GSA publishes uniform standards, specifications, and supply schedules for security equipment designed for secure storage. Containers used by the FAA must conform to GSA standards and specifications.
Hand-Held Metal Detector Device (HHMDD)	An electronic device for detecting the presence of metal objects to detect concealed weapons, explosives, etc.
Head of State	The chief public representative of a country, such as a president or monarch, who may also be the head of government.
Lawful Permanent Resident (LPR)	Any foreign national lawfully admitted to the United States as a permanent resident.
Level of Protection (LOP)	The degree of security provided by a particular countermeasure or set of countermeasures.
Line of Business (LOB)	A headquarters organization with a primary function of providing a safe and efficient aerospace system. The Agency's LOBs include Air Traffic Organization (ATO), Airports (ARP), Aviation Safety (AVS), Commercial Space Transportation (AST), and Security and Hazardous Materials Safety (ASH). (See FAA Order 1100.1)
Necessary LOP	The determined degree of security needed to mitigate the assessed risks at the facility.
Non-Employee	As defined in FAA Order 1600.1: "A person who is neither an FAA employee nor a contractor employee, who by agreement with the FAA, has access to FAA facilities, systems, SUI, resources and /or classified national security information (CNSI) similar to the access that FAA employees and contractor employees have.
Occupant Emergency Plan (OEP)	The occupant emergency plan is a set of procedures to protect life and property in federally occupied space under defined emergency conditions.
Open Storage	An open storage area/room is a "closed area" that meets the physical construction standards for open storage for safeguarding classified material that, because of its size, nature, or operational necessity, cannot be adequately protected by

Term (Acronym)	Definition
	normal safeguards or by being stored during non-working hours in GSA-approved security containers.
Real Estate Contracting Officer (RECO)	A government official who, under departmental or agency procedures, has the authority to enter and administer contracts, leases, agreements, grants, and other transactions for real property interests and utilities.
Remote Security Evaluation (RSE)	RSEs comprise a virtual assessment of the more critical components of a facility's necessary LOP.
Restricted Area	An area, interior or exterior to a facility, where access is controlled and limited.
Risk	A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence.
Risk Acceptance	The explicit or implicit decision not to take an action that would affect all or part of a particular risk.
Risk Management Process	A set of methods, principles, or rules used to identify, analyze, assess, and communicate risk and mitigate, accept, or control it to an acceptable level at an acceptable cost.
Secure Area	A room, suite, or special purpose building with a mission requirement for recurring and/or continuous classified operations/work.
Security Coordinator (SC)	The Facility Manager's designated representative and point of contact for coordinating with the responsible SSE on security matters for staffed FAA facilities. Previously referred to as the Facility Security Coordinator.
Servicing Security Element (SSE)	The SSE function resides within ASH. It is the ASH organizational element that is responsible for security support to a particular geographic area within the FAA.
Significant Areas and Assets	Significant Areas and Assets are those areas of the facility where any loss or damage to those assets and areas would have a significant impact on the overall facility (e.g., loading docks, exterior access to critical rooms, HVAC)
Sponsor	An FAA employee or contractor who has a current FAA email address and wishes to sponsor one or more visitors (including foreign national visitors) to visit one or more FAA facilities. The sponsor assumes responsibility for an individual visitor or a visiting group of persons for the duration of the visit to an FAA facility.
Staffed Facility	Any facility that is a permanent duty station for FAA personnel or a facility that is occupied most of a workday or work week by FAA personnel.
Supplemental Assessment	Onsite review and evaluation of specific areas of the FSMP at the facility, usually conducted to monitor progress on open findings from previous assessments, as a response to an incident, or as deemed necessary by the SSE.

Term (Acronym)	Definition
Threat	The intention and capability of an adversary to initiate an undesirable event.
Undesirable Event (UE)	An incident directed toward a federal facility that adversely impacts the operation of the facility, the mission of the agency, or personnel.
Unstaffed Facility	FAA sites or structures where no personnel are assigned but that FAA personnel may visit as needed.
Video Surveillance System (VSS)	A VSS is composed of a system of cameras, monitors/display units, and recorders.
Visitor	Any individual not issued a valid DOT/FAA ID media or not permanently assigned to an FAA facility. Individuals with valid DOT ID Media are not considered visitors at FAA facilities (i.e., non-NAS operational facilities).
Visitor Badge/ID Media	A form of DOT/FAA ID media to be worn by visitors while they are in an FAA facility.
Vulnerability	A weakness in the design or operation of a facility that an adversary can exploit. In other words, a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard; characteristic of design, location, security posture, operation, or any combination thereof, rendering an asset, system, network, or entity susceptible to disruption, destruction, or exploitation.
Walk-Through Metal Detection Device (WTMDD)	Equipment used in the security screening process to detect the presence of metal substances on persons passing through a magnetic field generated by a machine. Alarms are then resolved with additional screening measures, such as hand-held metal detection devices, and pat downs.

Appendix J. Frequently Used Acronyms

Acronym	Term (Acronym)
ADO	Airport District Office
AED	Automated External Defibrillator
AFSS	Automated Flight Service Stations
AGC	Office of the Chief Counsel
AMS	Acquisition Management System
ANSI	American National Standards Institute
AOA	Office of the Administrator
AOC	Office of Communications
API	Office of International Affairs
ARSR/JSS	Air Route Surveillance RADAR/Joint Surveillance Site
ARTCC	Air Route Traffic Control Centers
ATCSCC	Air Traffic Control System Command Center
ATCT	Airport Traffic Control Tower
ATR	Alternate Technical Representative
BHMA	Building Hardware Manufacturer's Association
BOE	Based on Evaluation
CARSR	Common Air Route Surveillance RADAR
CCC	Child Care Center
CCTV	Closed Circuit Television
CI	Critical Infrastructure
CMO	Certificate Management Office
CMS	Certificate Management Section
CNSI	Classified National Security Information
CO	Contracting Officer
COR	Contracting Officer's Representative
CPR	Cardiopulmonary Resuscitation
CSO	Contract Security Officer
CUI	Controlled Unclassified Information
DBT	Design-Basis Threat
DHS	Department of Homeland Security
DOS	Department of State
DOT	Department of Transportation

Acronym	Term (Acronym)
ECV	Entry Control Video
FAA	Federal Aviation Administration
FCT	Federal Contract Tower
FM	Facility Manager
FMP	Field Maintenance Program
FPS	Federal Protective Service
FRB	First Responder Book
FSC	Facility Security Committee
FSDO	Flight Standards District Office
FSL	Facility Security Level
FSMP	Facility Security Management Program
FSP	Facility Security Plan
FST	Facility Security Team
FSRS	Facility Security Reporting System
GCV	Gate Control Video
GSA	General Services Administration
HAZMAT	Hazardous Materials
HHMDD	Hand-Held Metal Detection Device
HQ	Headquarters
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilation, and Air Conditioning
ID	Identification
IDS	Intrusion Detection System
ISC	Interagency Security Committee
IVP	International Visitor Program
KCO	Key Control Officer
LEO	Law Enforcement Officer
LOB	Line of Business
LOP	Level of Protection
LPR	Lawful Permanent Resident
LSF	Logistics Support Facility
MERV	Minimum Efficiency Reporting Value

Acronym	Term (Acronym)
MFCR	Multi-Factor Card Reader
MMAC	Mike Monroney Aeronautical Center
NARA	National Archives and Records Administration
NAS	National Aerospace System
NIJ	National Institute of Justice
NEMC	National Enterprise Management Center
NTAS	National Terrorism Advisory System
OEP	Occupant Emergency Plan
PACS	Physical Access Control Systems
PIDS	Perimeter Intrusion Detection System
PIV	Personal Identity Verification
POC	Point of Contact
PPD	Presidential Policy Directive
PSEMS	Physical Security Enterprise Management System
RADAR	Radio Detection and Ranging
RAT	Risk Assessment Tool
RECO	Real Estate Contracting Officer
SAMHSA	Substance Abuse and Mental Health Services Administration
SAVI	Security Awareness Virtual Initiative
SC	Security Coordinator
SCC	Security Control Center
SFCR	Single Factor Card Reader
SO	Staff Office
SOM	Security Officer Manual
SOW	Statement of Work
SSC	Systems Support Center
SSE	Servicing Security Element
SSU	Systems Support Unit
STC	Sound Transmission Class
SUI	Sensitive Unclassified Information
TELCO	Telecommunication
TRACON	Terminal Radar Approach Control

Acronym	Term (Acronym)
UIS	Unstaffed Infrastructure Sustainment
VSS	Video Surveillance System
WebIRS	Web-Based Incident Reporting System
WJHTC	William J Hughes Technical Center
WTMDD	Walk-Through Metal Detection Device