TABLE OF CONTENTS

OVERVIEW

1.1 What is the purpose of this chapter? This chapter:

A. Establishes a baseline set of physical security measures that the U.S. Fish and Wildlife Service (Service) must apply to safeguard its employees, contractors, volunteers, and visitors while mitigating the risks to its assets at an acceptable level.

B. Introduces overall policy and responsibilities, while the following Service Manual chapters in Part 432 describe specific aspects of physical security in more detail:

(1) 432 FW 2, Physical Security Assessment Program; and

(2) 432 FW 3, Keys, Locks, and Locking Devices.

C. Describes the authorities and defines terms used in all the chapters in Part 432.

1.2 What is the scope of this chapter and the other chapters in Part 432? This chapter and the other chapters in Part 432:

A. Apply to all Service employees and facilities. Service facilities are those properties the Service either owns or leases, including those leased from both the General Services Administration (GSA) and other parties.

B. Address threat scenarios or Undesirable Events (UDEs) that are primarily caused by human acts. This covers all UDEs in the Interagency Security Committee's (ISC) "Design Basis Threat Report." Other threats to buildings, such as earthquakes, fire, or storms, are beyond the scope of this chapter.

1.3 What are the objectives of this chapter and the other chapters in Part 432? The Service's objectives are to:

A. Establish minimum standards for physical security for Service assets that meet or exceed, where needed, the ISC baseline Levels of Protection (LOP) established in *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (current edition)*.

B. Ensure Service facilities have an established Facility Security Level (FSL) determination and approved facility security plan, and that facility/station employees are provided physical security training and understand their responsibilities.

C. Standardize physical security countermeasures through the use of the Physical Security Risk Mitigation/Acceptance Justification Form (FWS Form 3-2502). Countermeasure standards must meet or exceed the ISC standard.

1.4 What are the authorities for this chapter and the other chapters in Part 432?

A. Controlled Unclassified Information (CUI) (32 CFR 2002).

B. Federal Information Processing Standard (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*.

C. FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*.

D. Federal Property Management Regulations System; Federal Management Regulation, Real Property; Facility Management (41 CFR 102-74).

E. Field Reference Guide for Aviation Security for Airports and Other Aviation Facilities, Department of the Interior (Department), March 2006.

F. Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors.

G. National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations.

H. NIST SP 800-116, r1, Guidelines for the Use of PIV Credentials in Facility Access.

I. Presidential Decision Directive (PDD)-62, Combating Terrorism.

J. Presidential Policy Directive (PPD)-21, Critical Infrastructure Security and Resilience.

K. The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (current edition), Department of Homeland Security, Interagency Security Committee.

L. 444 Departmental Manual (DM) 1, General Program and Physical Security Requirements**.**

1.5 What other Service Manual chapters are related to this chapter and the other chapters in Part 432?

A. 054 FW 1, Serious Incident Notification Procedures.

B. 270 FW 7, Information Technology (IT) Security Program.

C. 284 FW 3, Mail Security.

D. 310 FW, Personal Property.

E. 361 FW 1, Policy and Responsibilities for Dam Safety.

F. 361 FW 3, Emergency Action Plans for High and Significant Hazard Dams.

G. 371 FW 1, Policies and Responsibilities for Quarters Management.

H. 430 FW 1, Personnel Suitability and Security Program.

I. 431 FW, Information Security.

1.6 What terms do you need to know to understand this chapter and the other chapters in Part 432?

A. Baseline LOP. The degree of security that a set of countermeasures provides for each FSL and which facilities must implement unless they can justify a deviation (up or down) in a risk assessment.

B. Classified national security information. Documents that are marked "Confidential," "Classified," "Secret," "Top Secret," or a term for a higher level of security.

C. Consequence. The level, duration, and nature of the loss resulting from an undesirable event.

D. Countermeasure. Physical security device or control designed to protect personnel and property, including guards, fences and gates, Video Surveillance Systems (VSS), Intrusion Detection Systems (IDS), Physical Access Control Systems (PACS), lighting, locks, x-ray machines, and metal detectors.

E. Countermeasure recommendation. A countermeasure (or set of countermeasures) that personnel identify to mitigate against certain UDEs and meet minimum baseline LOPs as defined by the ISC. Personnel determine what these minimum required security standards are based on the FSL and risk assessment process.

F. **Design-Basis Threat (DBT).** A profile of the type, composition, and capabilities of an adversary.

G. Designated Official (DO). The primary tenant's senior representative or designated senior staff member with decision-making authority. The DO may have responsibility for multiple facilities (e.g., DO for a refuge complex).

H. Facility Security Committee (FSC). The committee responsible for addressing facility-specific security issues and approving the implementation of protective measures and practices (see section 1.12).

I. Facility Security Level (FSL). A categorization determined by analyzing several security-related factors for a specific facility, including mission criticality, symbolism, facility population, facility size, and threat to tenant agencies. The FSL serves as the basis for the implementation of physical security measures specified in ISC standards. Each FSL corresponds to a level of risk, which then relates directly to an LOP and associated set of baseline security measures (countermeasures). FSLs range from I to V, with an FSL I facility having a minimum level of risk and an FSL V facility having a very high level of risk. The Service does not have any FSL V facilities.

J. Facility Security Officer (FSO). The designated and trained station employee responsible for duties in section 1.9L that are specific to the implementation and continuance of physical security program requirements at their station or complex.

K. Facility Security Plan (FSP). A document that includes a facility profile; roles and responsibilities for security-related tasks; details about the PACS, IDS, and VSS; and details about other physical security countermeasures at the facility.

L. Intrusion Detection Systems (IDS). An externally monitored alarm system that can include door contact sensors, glass break sensors, and motion detectors.

M. Level of Protection (LOP). The degree of security provided by a particular countermeasure or set of countermeasures.

N. Level of risk. The combined measure of the threat, vulnerability, and consequence posed to a facility from a specified UDE. Risk is calculated as:

Risk = Threat x Vulnerability x Consequence

O. Necessary LOP. The minimum level of protection that must be implemented at a facility, using countermeasure recommendations, to adequately mitigate risks identified in the risk assessment process. The necessary LOP will take precedence over the baseline LOP.

P. Physical Access Control Systems (PACS). An electronic method of entering facilities that is compliant with FIPS 201-2 standards, including PIV card readers, door controllers, control panels, and access control software system.

Q. Risk assessment. The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.

R. Service facility. Service facilities include, but are not limited to, field stations, complexes, field offices, Regional offices, and Headquarters.

S. Threat. The intention and capability of an adversary to initiate an undesirable event.

T. Undesirable Event (UDE). A UDE is an incident caused by human acts that has an adverse impact on the facility occupants or visitors, operation of the facility, or mission of the agency.

U. Very Low Risk (VLR) facility. A mission asset whose incapacity or destruction would not likely cause loss of life and has little to no impact on security, local economic security, public health or safety, or any combination of those matters (444 DM 1).

V. Video Surveillance Systems (VSS). A VSS can include internal and external security cameras and a Network Video Recorder (NVR) to monitor areas such as facility entrances, secure areas, and parking lots.

W. Vulnerability. A weakness in the design or operation of a facility that an adversary can exploit.

1.7 What is the Service's overall policy for physical security?

A. Properly administered physical security controls at Service facilities should:

(1) Provide for a safe and secure working environment for employees, contractors, volunteers, and visitors;

(2) Minimize loss, damage, and destruction to Government property; and

(3) Ensure a comprehensive and realistic approach to:

(a) Meeting Federal facility security needs in today's threat environment, and

(b) Ensuring the scope (and cost) of security is commensurate with the risk posed to Service assets and facilities.

B. Employees who are responsible for facility management must ensure facilities meet security measures set by the ISC in *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (current edition)*. This ISC document includes minimum physical security standards for all Federal facilities based on mission criticality, symbolism, facility population, facility size, and threat to tenant agencies. There are five FSLs and associated security requirements.

C. A Service location with multiple land-based or real property assets (facilities) at a single location (i.e., refuges and hatcheries) may be categorized as a "Federal campus." This type of asset is assigned an FSL for the facility or campus as a whole, which is usually set at the highest of the FSL determinations for individual assets on the property.

1.8 What is the Service's physical security policy for airfields, airports, and dams?

A. Employees who are responsible for service assets such as airfields, airports, and dams have unique physical security considerations. Employees responsible for these types of assets should refer to the following security policy and guidance:

(1) 352 DM 5, Aircraft and Aviation Facility Security;

(2) 753 DM 2, Dam Safety and Security Program, Program Requirements;

(3) 444 DM 2, National Critical Infrastructure and Key Resource Security; and

(4) National Infrastructure Protection Plan (NIPP): Partnering for Critical Infrastructure Security and Resilience, Department of Homeland Security.

B. Employees who have additional questions regarding the security for airfields, airports, and dams should contact their Geographic Emergency Management and Physical Security Manager (GEMPS). The responsive GEMPS will coordinate with the National Aviation Manager and

respective Regional Aviation Manager or the National Dam Safety Coordinator and respective Regional Dam Safety Officer when responding to questions or when providing a technical consultation on security considerations and countermeasures for aviation or dam facility design and construction.

RESPONSIBILITIES

1.9 Who is responsible for physical security for the Service?

Table 1-1: Responsibilities for Physical Security

These employees…	Are responsible for…
A. The Director	**(1)** Reviewing and approving national Service policy for physical security; and **(2)** Ensuring resources are available to protect and manage the personnel, structures, operations, and contents of Service facilities.
B. The Chief - National Wildlife Refuge System (NWRS)	**(1)** Advising the Director about physical security incidents at Service facilities; **(2)** Overseeing the Office of Emergency Management and Physical Security (OEMPS); and **(3)** Ensuring that physical security becomes an integral part of the planning, design, and construction/renovation of Service facilities.
C. The Assistant Director - Management and Administration (also known as the Joint Administrative Operations [JAO] program)	**(1)** Advising the Director and the Physical Security Program Manager about security incidents at Service-leased facilities; **(2)** Serving as the DO for the Headquarters facility (see section 1.9K); **(3)** Maintaining a current list of all facilities that Service personnel occupy and providing the list to OEMPS; **(4)** Coordinating with GSA on physical security elements for leased space and for landlord responsibilities; **(5)** Coordinating with the Federal Protective Service (FPS) on law enforcement matters, building security assessments, and other related security services that FPS provides; **(6)** Ensuring security is an integral part of the budget, acquisition, and leasing of Service facilities and their planning, design, and construction/renovation;

These employees…	Are responsible for…
	(7) Installing, managing, and developing operational procedures for physical access control and other physical security systems in the Headquarters facility; and **(8)** Developing policy and procedures for issuance and revocation of PIV cards and coordinating these operations.
D. The Associate Chief Information Officer (i.e., Assistant Director – Information Resources and Technology Management)	**(1)** Ensuring the physical security of Service information technology systems (see 270 FW 7) and data centers; **(2)** Developing and maintaining standards for integrating electronic security systems (e.g., PACS, IDS, and VSS) into existing Service network infrastructure; and **(3)** Maintaining standards for employee emergency notifications, including standards for the notification and alert system interface with Service internet and other systems.
E. Chief, Office of Emergency Management and Physical Security (OEMPS, within the NWRS program)	**(1)** Overseeing the Office of Emergency Management and Physical Security (OEMPS); **(2)** Providing resources for the Physical Security Program Manager to comply with the requirements in this chapter; **(3)** Overseeing Servicewide compliance of the physical security program; **(4)** Briefing the Director annually on the Service physical security program, physical security incidents at Service facilities, and the threats facing Service facilities and personnel; and **(5)** Supervising and providing resources to the cadre of GEMPS to comply with this chapter.
F. Physical Security Program Manager (within the OEMPS program)	**(1)** Serving as the principal advisor to the Chief, OEMPS on Service physical security matters; **(2)** Developing physical security management policy; **(3)** Maintaining a list of Service facilities with their category designation (FSL) and providing annual updates to the ISC and the Department's Office of Law Enforcement and Security (OLES); **(4)** Ensuring Service compliance with Presidential Directives, ISC standards, and Departmental policy on physical security for all Service facilities;

These employees…	Are responsible for…
	(5) Serving as the Service representative for physical security at Departmental or other security-related meetings; **(6)** Chairing the Service's Physical Security Advisory Board (PSAB) and coordinating incident-related information through that entity; **(7)** Providing technical guidance; assisting Facility Security Officers (FSOs) with security-related issues; and interpreting Federal, Departmental, and Service security policies; **(8)** Monitoring performance of the Service's physical security management programs, including managing the physical security assessment program (see 432 FW 2); **(9)** Recording lessons learned from incidents, exercises, and other events to help improve the program and developing an after-action matrix for improvement for consideration by the PSAB; **(10)** Ensuring that security is an integral part of the operations, planning, design, construction/renovation, and acquisition of Service facilities; **(11)** Reviewing submitted Physical Security Risk Mitigation/Acceptance Justification Forms (FWS Form 3-2502) for facilities; and **(12)** Developing the annual briefing for the Director on the Service physical security program. The briefing includes information on the security program's annual recommendation status, training compliance, other accomplishments, physical security incidents occurring at Service facilities, and the threats facing Service facilities and personnel.
G. Geographic Emergency Management and Physical Security Managers (GEMPS)	**(1)** Coordinating facility compliance with the chapters in Part 432 and working with Regional Directors to develop Regional strategic plans and priorities; **(2)** Serving as physical security subject matter experts and advisors to DOs, FSOs, and management and as the primary points of contact for physical security for the Regions for which they are responsible; **(3)** Providing technical assistance to field station personnel (including DOs and FSOs) and facility security committees about

These employees…	Are responsible for…
	physical security assessments and implementation of necessary countermeasures; **(4)** Collecting reports of security-related incidents or issues from FSOs and sending them to line management, along with a copy to the Chief, OEMPS and Physical Security Program Manager, as appropriate; **(5)** Coordinating with the Physical Security Program Manager to resolve technical and Servicewide issues, as needed; **(6)** Serving as the concurring authority for security upgrades that FSOs or DOs submit and providing written reasoning when the upgrades are not approved; **(7)** Reviewing construction documents and drawings during all planning phases and, if necessary, conducting on-site reviews for new construction and significant renovation projects for physical security compliance with ISC standards; **(8)** Conducting off-cycle security reviews and providing consultations, if needs dictate (i.e., to address break-ins, investigate events, etc.); and **(9)** Notifying the Physical Security Program Manager and Chief, OEMPS of any shortcomings or needs regarding the national physical security program that affect personnel, facilities, or assets in their assigned Regions.
H. Physical Security Advisory Board (PSAB) (a Headquarters-based team of employees who meet quarterly)	**(1)** Acting as a resource for OEMPS and helping provide oversight, leadership, policy development, and guidance on physical security matters of institutional importance. The board is comprised of experts in the following fields: **(a)** Physical security; **(b)** Dam safety and security; **(c)** Law enforcement; **(d)** Personnel security; **(e)** Information technology security; **(f)** Facility, personal property, and fleet management;

These employees…	Are responsible for…
	(g) Employee safety and health; and **(h)** Aviation security; **(2)** Ensuring Service compliance with ISC standards; **(3)** Reviewing changes to Service and Departmental policies; and **(4)** Recommending any necessary customized levels of protection for Service facilities.
I. Regional Directors	**(1)** Providing resources to ensure compliance with the chapters in Part 432, and **(2)** Approving risk acceptance when countermeasures at a facility do not meet the necessary LOP as mandated in ISC standards.
J. Assistant Regional Directors	**(1)** Ensuring the appointment of DOs for the facilities in their programs, **(2)** Helping the GEMPS to coordinate activities and share information with other employees, and **(3)** Finding funding for Project Leaders to implement countermeasure recommendations.
K. Designated Officials (DO)* (may be any individual primarily responsible for the overall operation of a Service facility such as a refuge manager, hatchery manager, or Ecological Services field station manager)	**(1)** Authorizing physical security activities and ensuring compliance with the chapters in Part 432 and 444 DM 1 at the facilities for which they are responsible; **(2)** Establishing and maintaining specific security measures that comply with ISC standards and that are based on the types of risks associated with the facility and the programs and activities carried out at the facility; **(3)** Assigning an FSO for their facility or acting in that capacity themselves; **(4)** Serving as a member or chairperson of the FSC, if applicable; **(5)** Ensuring that physical security is part of the planning, design, and construction/renovation of Service facilities as Part 360 of the Service Manual describes; **(6)** Ensuring a physical security assessment has been coordinated and documented with the servicing GEMPS prior to occupying a new facility;

These employees…	Are responsible for…
	(7) Annually reviewing and approving the FSP; **(8)** Ensuring station funding and documents for IDS monitoring services are completed and submitted as applicable; **(9)** Ensuring security equipment is integrated into the facility's normal maintenance, repair, and replacement scheduling systems to make certain of continuous operations; **(10)** Informing Service officials, FPS, GSA, and law enforcement, where appropriate, of significant physical security incidents or threats and any corrective actions taken to prevent reoccurrence. Also reporting serious physical security incidents or threats using guidelines in 054 FW 1 for significant, life-threatening, or the types of events that could prompt media attention. This includes notifying: **(a)** In Headquarters, the Chief, Division of Acquisition, Property and Project Management and the Chief, OEMPS; **(b)** In a Regional office or field station, the affected Regional Director; and **(c)** The appropriate GEMPS; and **(11)** Completing online DO physical security awareness training as specified in section 1.10 within 12 months of the date that this policy goes into effect or from when they become the DO, whichever is longer.
L. Facility Security Officers (FSO) (may be the same person as the DO in smaller facilities)*****	**(1)** Ensuring the effective implementation of security policies, programs, directives, and training within the facility; **(2)** Ensuring that visitors entering federally controlled building space have appropriate screening, are escorted or closely monitored, and have the appropriate visitor's pass; **(3)** Ensuring, per facility-specific standard operating procedures, that facilities, gates, vehicles, heavy equipment, water control structures, etc. are secure during the workday when unattended and at the end of every workday; **(4)** Ensuring station management and staff have established/implemented procedures for accountability of equipment and articles that may have security significance such as, but not

These employees…	Are responsible for…
	limited to, computers, flash drives, vehicle license plates, uniforms, and identification badges; **(5)** Annually reviewing and updating the FSP and sending a copy to their GEMPS by March 1 of each year; **(6)** Ensuring that security guard contracts comply with the requirements in 444 DM 1, for sites that have a guard(s); **(7)** Conducting and reporting on security guard assessments for sites that have a guard(s) (see section 1.20); **(8)** Sending security concerns and security-related reports to their DO and GEMPS; **(9)** Notifying the GEMPS when a physical security countermeasure is degraded or is no longer functioning as designed; **(10)** Discussing physical security needs with the DO and GEMPS and incorporating physical security requirements into new construction and renovation projects; **(11)** Coordinating with the GEMPS for review and approval prior to starting any physical security upgrade, countermeasure selection, modification, purchase, or installation; **(12)** Ensuring all security equipment is tested annually to make sure it is in good working condition and being used as intended. To do so, they must keep a testing activity log and make it available to the GEMPS and Physical Security Program Manager; **(13)** Ensuring that when security equipment is not working, an interim measure is put in place within 30 days that provides equal or greater risk mitigation. If this is not possible, then documenting and retaining a description of the deviation and sending it to the DO and GEMPS for follow-on actions to resolve the matter, if feasible, through involvement of program and Regional management; **(14)** When applicable, coordinating completion of a risk assessment (see 432 FW 2) of their assigned facility, and attaching a copy of the results to the FSP; **(15)** Conducting a semiannual or annual inventory of keys, locks, and locking devices (see 432 FW 3);

These employees…	Are responsible for…
	(16) Accounting for access keys to work areas and tracking distribution using FWS Form 3-2384, Key Control Register and Inventory; **(17)** Annually training employees about the FSP and physical security procedures; **(18)** Serving as a member of the FSC, if applicable; and **(19)** Completing online FSO physical awareness training as specified in section 1.10 within 12 months of the date that this policy goes into effect or from when they become the FSO, whichever is longer.
M. Supervisors	**(1)** Denying access and retrieving employee identification, keys, access cards, or other media from employees when they separate from the Service or are suspended from duty (see 432 FW 3); **(2)** Keeping high theft-potential items (e.g., cameras, binoculars, power tools, televisions, laptop computers, vehicle license plates and decals, uniforms, credentials) in a locked cabinet or some other locked area when not in use; and **(3)** Notifying the DO when beginning the termination, suspension, or discipline process for someone because of security-related issues.
N. Employees	**(1)** Safeguarding Government property from damage, loss, and destruction by adhering to required facility physical security procedures and Part 310 of the Service Manual on personal property management; **(2)** Reporting suspicious activities or personnel or physical security incidents or threats to law enforcement, their immediate supervisor, the FSO, and others, as appropriate (also see section 1.13); **(3)** Informing supervisors whenever they intend to access or remain at the workplace outside of normal working hours; **(4)** Reporting to the DO and FSO missing or stolen equipment and articles that may have security significance such as, but not limited

These employees…	Are responsible for…
	to, computers, flash drives, license plates, uniforms, PIV cards, and badges; **(5)** Properly displaying identification as required by the FSP; **(6)** Properly escorting and supervising visitors within the facility as required by the FSP; and **(7)** Completing security awareness training within 60 days of employment and annually thereafter.

***NOTE:** DOs and FSOs may service several facilities within a geographic area or multiple buildings at a campus facility. Neither assignment needs to be limited to a single building or facility, but no one person should be assigned responsibility for so many facilities that they cannot reasonably perform the functions of DO or FSO, or if the multiple facility assignments will have a negative impact on their normal duties.

TRAINING REQUIREMENTS

1.10 What are the training requirements for Designated Officials and Facility Security Officers?

A. See Table 1-2 for requirements for DOs and FSOs.

Table 1-2: Training for Employees Involved in Security Management

Training Description	DO	FSO
IS-1170: Introduction to the Interagency Security Committee (ISC)	X	X
IS-1171: Overview of Interagency Security Committee (ISC) Publications	X	X
IS-1172: The Risk Management Process for Federal Facilities: Facility Security Level (FSL) Determination	X	X
IS-1173: Interagency Security Committee Risk Management Process: Levels of Protection and Application of the Design Basis Threat Report	X	X
IS-1174: Interagency Security Committee Risk Management Process: Facility Security Committees	X	X
2 hours of annual security training (recommended)		X

B. The first five requirements in the table above are set by the ISC. The recommended 2 hours of annual security training for the FSO can be achieved through security workshops or other training courses. Recommended courses can be found on the Physical Security Information Portal.

1.11 What are the security awareness training requirements for employees and contractors?

A. The Department requires that all Service employees and unescorted contractors complete security awareness training within 60 days of employment and annually thereafter (444 DM 1).

B. Training must, at a minimum, include information security and operations security, active shooter response, suspicious activity and incident reporting process, and security plans. The training is provided online, bundled with other annual mandatory training.

DAY-TO-DAY OPERATIONS AND SECURITY

1.12 What is a Facility Security Committee (FSC)?

A. An FSC:

(1) Is established when a facility has two or more Federal tenants with funding authority;

(2) Is the committee responsible for addressing facility-specific security issues and approving the implementation of protective measures and practices;

(3) Meets biannually or as needed, as determined by the committee chairperson;

(4) Maintains records of meetings and committee decisions for a minimum of 5 years; and

(5) Consists of a chairperson, tenant representatives, security organization, owning/leasing authority, and other support personnel.

B. FSC members vote to determine whether the necessary LOP is used, some of the necessary LOP is used and some risk is accepted, a lower LOP is used and some risk is accepted, or no countermeasures are used and all the risk is accepted (see 432 FW 2).

1.13 What are employees' responsibilities for reporting criminal activity?

A. In Service facilities, employees must immediately report all suspected criminal activity and suspicious behavior to the appropriate authorities and in accordance with Service policy (see 054 FW 1 for serious incident reporting). Appropriate law enforcement authorities may include local law enforcement, NWRS law enforcement, and the FPS.

B. Employees must also:

(1) Inform their supervisor of the criminal activity they reported, and

(2) Obtain a copy of the incident report generated by the investigating law enforcement agency and provide it to the FSO or FSC chairperson.

1.14 What are employees' responsibilities for access control of a Service-controlled facility?

A. If employees or contractors believe an individual poses a threat to Service employees or other contractors, resources, or property, they must immediately notify their supervisor and an appropriate law enforcement officer who may deny the individual access to Service facilities and assets.

B. The DO, FSO, or any Service employee or contractor may deny access to a non-employee.

(1) If someone other than the DO or FSO denies access to a non-employee, the DO and FSO must be notified of the denial within a reasonable timeframe.

(2) The DO must:

(a) Ensure that appropriate law enforcement authorities and other facility employees are notified about the denial, and

(b) Prepare a denial of access letter for the facility security records that identifies the individual and documents the circumstances.

(3) In cases of an overt threat or potential violence, all facility personnel should be notified in the most expedient fashion available and informed when the issue has been resolved or is no longer credible.

C. Personnel may request an individual's official identification to validate authorized access.

D. If a Service employee is denied access, the employee's supervisor/manager must coordinate with the servicing Human Resources (HR) office and document it in a denial letter to the individual as soon as possible, but no later than 48 hours after denying access.

(1) The letter should identify:

(a) The individual denied access;

(b) Circumstances for denying access;

(c) Conditions, if any, under which the Service will grant the individual temporary access to the facility; and

(d) Contact information for the servicing HR office.

(2) The employee's management team must continue to consult with the servicing HR office to ensure that the denial of access complies with applicable labor-management agreements and existing personnel policy.

(3) When an employee is denied access, the employee's management team must ensure access to the facility is revoked (see 432 FW 3).

1.15 What is the policy concerning the purchase, installation, maintenance, and use of certain countermeasures?

A. A FIPS 201-2 (or subsequent version)-compliant PACS is required at all Service facilities with an FSL of III or IV.

B. If a PACS is used at an FSL I or II facility, it must be FIPS 201-2 compliant.

C. FSOs and DOs, in coordination with the Infrastructure Management Division, must identify and determine funding avenues for necessary countermeasures during any new construction planning, modernization/renovation, or before upgrading or replacing existing countermeasures in Service facilities.

D. FSOs and DOs must consult their GEMPS prior to contracting to purchase, install, or implement countermeasures to ensure that items purchased are of commercial grade and are adequate to meet ISC and industry standards.

E. Security equipment must be integrated into the facility's normal maintenance, repair, and replacement scheduling systems to ensure continuous operations with minimal downtime in case the system or a component of the system fails.

F. Staff must test all security equipment on site annually to ensure it is in good working condition and being used as intended. The FSO must keep a testing activity log and make it available to OEMPS and the Department's OLES upon request.

1.16 What is the policy concerning weapons in Federal facilities?

A. The Service strictly prohibits the possession of firearms or other dangerous weapons in Federal facilities, except for law enforcement officers, Federal officials performing law enforcement duties, or where the possession is authorized by Federal law (see 18 U.S.C. 930 and 41 CFR 102-74.440). This prohibition also applies to non-law enforcement individuals who have a valid permit to carry a concealed weapon.

B. Employees must not store or transport non-Government-owned firearms or other dangerous weapons in Service vehicles unless they are authorized to do so as part of their official duties (e.g., law enforcement duties or wildlife management).

C. For more information about carrying dangerous weapons onto Service lands, see:

(1) For Service-managed hunts, 50 CFR 32;

(2) For tenants in Service quarters, 371 FW 1; and

(3) When authorized by State or other regulations, 50 CFR 27, Subpart D.

1.17 What are the requirements for security guards? The FSO must work with a servicing Contracting Officer or the employee responsible for managing the guard force to ensure program effectiveness and that the following requirements are met if their facility has one or more guards (this includes any protection or patrol services):

A. For Service-contracted protection services, the FSO must evaluate the service provided on a quarterly basis to ensure contract compliance. The FSO must report deficiencies to the Contracting Officer so that the company can develop a Corrective Action Plan. For FPS services, the FSO must also report any identified or known deficiencies to the Contracting Officer for FPS action.

B. The FSO must conduct an effectiveness assessment of the guard program (see section 1.20).

C. The FSO must ensure all guard contracts include the applicable requirements from this section.

D. A security guard force/team may consist of unarmed and armed guards and security personnel with various levels of skill to minimize operational costs (not all protection services require the same caliber of training and equipment).

E. All security guards must comply with the latest applicable DMs (such as 446 DM) and any other Service, tate, local, or other laws, regulations, policies, and guidelines.

F. Armed security guards must also comply with the latest ISC policy on guards (currently "Armed Contract Security Officers in Federal Facilities: An Interagency Security Committee Best Practice").

G. The FSO must optimize the use of security systems to help minimize costs. A system of detection, delay, and access control can prevent the need for a guard in some places.

H. The FSO must work with the employee responsible for managing the guard force to:

(1) Ensure guard training includes regular tests, exercises, and drills so that guards can adequately perform their assigned duties and protection services. The level of training received must be commensurate with the level of protection services provided. For example, unarmed guards are there to deter and detect, so they require less training than armed guards. Response-level guards need more training so they can potentially deny aggressors.

(2) Maintain and regularly exercise a response plan (e.g., guard post orders). The plan must, at a minimum, describe responsibilities, post duties, and other requirements and require response force personnel to only depart from their posts when they are relieved or in a life-threatening situation.

PLANS AND ASSESSMENTS

1.18 What is a Facility Security Plan (FSP)?

A. The FSP establishes and maintains a strong, efficient security program to support the Service's mission and operations at each facility. The security program protects personnel, visitors, records/information, equipment, facilities, property, and other assets. Plans must document the specific measures, responsibilities, and equipment (e.g., VSS, IDS, PACS) that provide for the enhanced security of assets/facilities based on the Department of Homeland Security National Terrorism Advisory System (NTAS) levels. The FSO should use the FSP template, available online on the Service's Physical Security Information Portal to write the FSP.

B. FSP requirements:

(1) The FSO must develop an FSP if one is not already on file or revise it whenever a new format is distributed nationally.

(2) The FSO and the DO must review the FSP annually and revise it as necessary to ensure it accurately reflects protective measures to be implemented at the facility under elevated threat conditions.

(3) The FSO must store the approved plan in a secured area of the facility and send a copy to their servicing GEMPS.

(4) The FSO may allow employees with a need-to-know to access the plan.

(5) The DO must review security procedures with facility employees annually.

(6) The DO and FSO must ensure that they and any support personnel mark and handle completed FSPs as Controlled Unclassified Information (CUI) (marked as CUI//SP-PHYS) and safeguard it when in electronic or printed form or shared outside of the Service, in accordance with laws, regulations, and policy regarding the handling, storage, and disposition of CUI (32 CFR Part 2002).

1.19 What is a physical security assessment?

A. A physical security assessment is an independent evaluation of the current physical security status of a facility to identify if any additional countermeasures are necessary to enhance the Service's ability to safeguard employees, visitors, and property.

B. The Service has established a physical security assessment program, managed by OEMPS, which meets the ISC standards (see 432 FW 2).

1.20 What is a contract security guard effectiveness assessment? If a facility has one or more contract guards, the FSO must assess the effectiveness of the guard program in compliance with the following requirements:

A. The FSO must assess the guard program every 3 years at FSL III and IV facilities, and every 5 years elsewhere.

B. For Service-contracted protection services, in addition to the assessments we describe above, the FSO must conduct an assessment at least 18 months before the current contract is set to expire to implement any lessons learned into the new contract language.

C. The goal of assessments is to evaluate effectiveness of the guard program to accomplish the mission of protecting the highest risk assets against current threats versus the capability and costs (e.g., guard numbers, training/exercises, equipment, documentation, etc.).

D. The FSO must document, track, retain, and make available the assessment and associated findings and corrective actions to OEMPS and to the Department's OLES, upon request.

ANNUAL REPORTING REQUIREMENTS

1.21 What information does the Service have to report to the ISC? OEMPS must provide an annual submittal to the ISC that updates the bureau facility inventory and category designation and any requested countermeasure compliance data for the Service's FSL I - IV facilities.

1.22 What information does the Service have to report to the Department's Office of Law Enforcement and Security (OLES)?

A. OEMPS must maintain the Service's facility category designation list of FSLs and provide it to OLES annually or as changes occur.

B. OEMPS must also provide OLES with an annual summary document describing the Service security program's recommendation status, training compliance, and any other requirements and accomplishments (see 444 DM 1).

C. OEMPS must create and maintain physical security assessment reports and make them available to OLES upon request.

D. OEMPS must document, track, and retain security guard effectiveness assessments and associated findings and corrective actions and make them available to OLES upon request.

/sgd/ Stephen Guertin
DEPUTY DIRECTOR

Date: October 19, 2021