



U.S. FISH AND WILDLIFE SERVICE TRANSMITTAL SHEET

PART 432 FW 1	SUBJECT Physical Security Physical Security in Service Facilities	RELEASE NO. 367
FOR FURTHER INFORMATION CONTACT Div of Contracting & General Services		DATE June 17, 2001

EXPLANATION OF MATERIAL TRANSMITTED:

This chapter:

- Requires that facility managers ensure establishment of building security committees (1.4D).
- Requires security surveys to determine the effectiveness of the physical security safeguards (1.5).
- Reiterates managers' responsibility to ensure that items with high theft potential such as cameras, binoculars, power tools, televisions, video cassette recorders, laptop computers, postage stamps, are kept in a locked cabinet or otherwise secured by a locking device within the office (1.4C).
- Includes guidance on denying employees, contract personnel, and visitors access to Service facilities or portions of facilities controlled by Service organizations (1.9 and 1.10).
- Provides a link to list of Federal Protective Service Regional Offices (<http://hydra.gsa.gov/pbs/fps/framest/t04fs.htm>)


Acting Deputy
DIRECTOR

FILING INSTRUCTIONS:

Remove:

432 FW 1, FWM 123, 10/20/93 (1 sheet)

Insert:

432 FW 1, FWM 367, 06/17/01 (2 sheets)
Exhibit 1, FWM 367, 06/17/01 (1 sheet)
Exhibit 2, FWM 367, 06/17/01 (2 sheets)

**FISH AND WILDLIFE SERVICE
SECURITY**

Security

Part 432 Physical Security

Chapter 1 Physical Security in Service Facilities

432 FW 1

1.1 What is the purpose of this chapter? This chapter establishes requirements for physical security in all Service-owned facilities and space that we lease through the General Services Administration (GSA). Physical security encompasses people, personal property, and buildings and their contents. As used in this chapter, the term "We" refers to the Fish and Wildlife Service.

1.2 What is Service policy regarding physical security?

We will manage all Service facilities to minimize loss, damage, and destruction to Government property, and to provide a safe and secure working environment for all employees and visitors.

1.3 What are the authorities for this chapter?

A. 41 CFR Part 101-20.1, Federal Property Management Regulations (Buildings Operations, Maintenance, Protection, and Alterations) establishes procedures for maintenance, operation, protection, and management of Government-owned and leased buildings and grounds under the assignment responsibility of GSA.

B. 444 DM 1 (General Program Requirements - Physical Protection and Building Security) establishes Departmental requirements for bureau physical security programs. This chapter incorporates the U.S. Department of Justice study entitled, "Vulnerability Assessment of Federal Facilities," June 28, 1995.

1.4 Who is responsible for physical security?

A. Assistant Director - Business Management and Operations (AD-BMO) is the principal advisor to the Director regarding security of Service facilities. Through the Division of Contracting and General Services, Washington Office (CGS-WO), the Assistant Director oversees development and maintenance of policies and procedures to adequately protect Service facilities, equipment, and personnel and to ensure the establishment of building security committees.

B. Regional Directors will (1) ensure compliance with all provisions of this chapter, (2) designate a Regional point of contact for physical security related information and provide his or her name, telephone number, and fax number to Chief, CGS-WO, and (3) ensure the establishment of building security committees.

C. Managers will ensure adherence to physical security procedures for facilities and will:

(1) Work with both Service and non-Service facility managers to address Service concerns, including all elements identified in paragraph 1.4D. To meet your specific needs, you may develop physical security procedures apart from those for the facility, if they do not conflict with the facility procedures. However, you should make every effort to work with the facility manager to address Service concerns.

(2) Ensure that your areas are secure at the end of each work day.

(3) Ensure that visitors have access to your work areas only as needed.

(4) Conduct security surveys of your work areas in accordance with paragraph 1.5.

(5) Inform the Assistant Regional Director for Budget and Administration of significant security incidents or threats and any corrective action that you take to prevent recurrence. In the Washington Office, advise the AD-BMO through the Chief, CGS-WO. Consider a security incident or threat significant if it is potentially life-threatening, has potential for public and/or employee outcry, or affects Service or Departmental interests in such a manner that it is likely to require a Service or Departmental response.

(6) Account for access keys to your work areas in the same manner as personal property assigned to the custody and care of an employee. To establish a chain of custody, obtain a signed Receipt of Property (DI-105) or some other written record from each employee who has an access key.

(a) Make available access keys, including electronic entry keys or proximity reader cards, to buildings and individual offices to employees on an as-needed basis. Employees must not give access keys to friends or family members. We may deny or retrieve access keys from employees for inappropriate use or failure to safeguard Service facilities and property.

(b) Report immediately lost or stolen access keys.

(7) Keep items with high theft potential (e.g., cameras, binoculars, power tools, televisions, video cassette recorders, laptop computers, postage stamps) in a locked cabinet or otherwise secured by a locking device within the office when not in use.

D. Facility Managers of Service-owned or Leased Facilities. As the facility manager of a Service-owned or GSA-leased facility, you should establish and maintain written facility security procedures that address applicable components of the Minimum Security Standards for Service Facilities contained in paragraph 1.6 and Exhibit 1. Review or ensure review of security surveys and records at least annually to identify current security conditions and any changes needed to maintain an effective security program.

(1) **Service-owned facility or facility not leased through GSA.** As a facility manager of a Service-owned facility or a facility not leased through GSA, you are not required to follow Federal Protective Service (FPS) guidance or comply with FPS security alerts. However, you should follow FPS guidance appropriate for your facility. Station safety

**FISH AND WILDLIFE SERVICE
SECURITY**

Security

Part 432 Physical Security

Chapter 1 Physical Security in Service Facilities

432 FW 1

committees may serve as building security committees and a physical security representative from GSA is not required.

(2) GSA-leased facilities. If you are the facility manager of a GSA-leased facility, you should:

(a) Ensure compliance with FPS security alerts. The FPS issues security alerts within specific FPS regions as appropriate. FPS regional offices are available to provide assistance to Service GSA-leased facilities. The CGS-WO will advise Service Regional Offices of pertinent security alerts and other information and guidance received from FPS.

(b) Ensure that a building security committee evaluates and applies the appropriate minimum standards identified in paragraph 1.6. The committee should determine which of the minimum requirements need to be implemented and identify any additional requirements. The committee should document reasons for variance with the minimum standards. The committee should be comprised of a physical security representative from GSA and a representative from each agency at the facility. An existing station safety committee may serve as a building security committee, and a committee may cover more than one building.

E. Employees should:

(1) Safeguard Government property from damage, loss, and destruction by adhering to the facility security procedures.

(2) Not use personally-owned property in performing official duties without specific authority from the Director in accordance with 310 FW 1.

(3) Report any personal or physical security incident or threat to your immediate supervisor.

(4) Inform your supervisor whenever you intend to access or remain at the workplace outside of normal working hours. Such notification can be for a period of days.

1.5 What is the role of the manager regarding physical security surveys?

A. The facility manager should conduct security surveys of the workplace at least annually to determine the effectiveness of the physical security safeguards. Note deficiencies and any corrective action instituted as soon as possible. Surveys should include procedural security safeguards as well as physical safeguards. Exhibit 2 (Department of the Interior Physical Security Survey Data) will assist managers in completing the survey. All data items will not be appropriate for all stations.

B. For Service-owned facilities, the facility manager, manager, or supervisor, as appropriate, will discuss security needs with the building contractor and engineers while the project is still in the planning stage. After construction,

conduct an onsite security survey prior to occupancy of the facility to make sure security requirements have been met.

C. In facilities leased through GSA, the appropriate manager should work with the servicing Regional CGS Office and the GSA-leasing office to make sure that appropriate safeguards are in place prior to occupancy.

1.6 Are there minimum security standards for Service facilities? The Department of Justice has established minimum security standards for all Federal facilities based on facility size, activities, and public access. The standards are designed to minimize loss and injury to life and property resulting from workplace violence, vandalism and terrorism or from unauthorized access. There are five security levels for assignment to Federal facilities and security requirements associated with each security level (see subparagraphs A through E below). Facility security programs should meet minimum standards appropriate for the facility's size and scope of operations as identified below, except as modified by building security committees. You may modify minimum requirements if the building security committee (1) determines that the requirement is not necessary, (2) identifies alternative measures to meet the intent of the standard, or (3) documents the need for additional or enhanced requirements. Safety committees may serve as building security committees in accordance with paragraph 1.4D. (See item 23, Exhibit 2, to determine low, moderate, and high volumes of public contact.)

A. Level I facilities have 10 or fewer employees, up to 2,500 square feet of office space, and a low volume of public contact or contact with a limited segment of the public. Level I facilities must meet the following requirements:

(1) Lighting with emergency power backup.

(2) Written receiving and shipping procedures that are reviewed and updated annually.

(3) Facility compliance with current Life Safety Code Standards for fire detection and suppression. Facility managers should contact Regional Safety Managers to confirm compliance.

(4) Installation of high security locks for which keys cannot be commercially duplicated.

(5) Emergency power to critical systems such as alarm systems, radio communications, and computer systems.

(6) Annual test, review, and update of facility Continuity of Operations Plan and Occupant Emergency Plan or Station Safety Plan.

(7) Establishment and maintenance of liaisons with local law enforcement organizations.

**FISH AND WILDLIFE SERVICE
SECURITY**

Security

Part 432 Physical Security

Chapter 1 Physical Security in Service Facilities

432 FW 1

(8) Employee orientation to facility security procedures and annual security awareness training.

B. Level II facilities have from 11 to 150 employees, up to 80,000 square feet of office space and a moderate volume of public contact. In addition to the security requirements for Level I facilities, the following apply:

- (1) A system for visitor control and accountability.
- (2) An evaluation of the threat to the day care center where day care centers exist at the facility.

C. Level III facilities have from 151 to 450 employees, up to 150,000 square feet of space, and a moderate to high volume of public contact. In addition to the security requirements for Level II facilities, the following apply:

- (1) Control of facility parking area if part of the facility (below, above, or attached as part of the structure), including posting signs to identify the area, providing placards or other identifiers for authorized access, arranging for towing of unauthorized vehicles, and adequately lighted parking areas.
- (2) Procedures to prevent unauthorized access to utility areas.

D. Level IV facilities have over 450 employees, more than 150,000 square feet of space, a high volume of public contact, and tenant agencies that may include high-risk law enforcement and intelligence agencies, courts, judicial offices, and highly sensitive Government records. (At this time the Service has no Level IV facilities.) In addition to security requirements applicable for Level III facilities, the following apply:

- (1) Closed circuit television monitoring with time lapse video recording.
- (2) X-Ray screening of all incoming mail and packages.
- (3) Agency photo identification cards displayed at all times.

E. Level V facilities house mission functions critical to national security. The Pentagon and the CIA Headquarters are examples of two Level V facilities. The Service has no Level V facilities.

1.7 Should I report criminal activity? You should report criminal activity to local law enforcement organizations. If you are in a GSA facility, provide a copy of all police reports to the FPS.

1.8 Can an individual be denied access to a Service facility or Service controlled space? We may deny a person access to Service facilities or Service controlled areas of a facility when managers/supervisors have reason to

believe they pose a threat to Service employees, resources, or property. Service managers should coordinate denials of access with the facility manager and consult the servicing personnel office to ensure that denials of access comply with applicable labor-management agreements and existing personnel policy.

1.9 What actions are necessary to deny access of an employee? The manager must document in writing the reason(s) for denying access and present such documentation to the individual. The letter denying access should include conditions, if any, under which we will grant the individual temporary access to the facility, including contact persons. Do not delay denial of access to the facility or area when the individual poses an immediate threat. In such instances, provide the denial letter to the individual as soon as possible, but no later than 48 hours after denying access.

1.10 What about terminated employees? Retrieve Government identification cards from employees and contract personnel when they are no longer employed with the Service. Treat terminated employees and contract employees as visitors when they request entrance to the facility. Supervisors will collect the identification card (as well as keys, badges, or any item that provides access to Service space or systems) of an employee who is suspended from active duty or placed on administrative leave with pay, goes on IPA, or in any situation where the supervisor feels it is necessary to protect the safety of employees or the public or to protect Government property (see 210 FW 1).

1.11 Are there any required records or reports?

A. Make facility security procedures, security programs, or plans available to all employees. Security procedures may be a part of the occupant emergency plan or station safety plan or other station or facility plan, provided the procedures are a distinguishable component and can be made available separately. Security procedures should contain a date of the most recent review and evidence of employee awareness. Dated employee signatures appended to the procedures or plan easily provide evidence of this requirement.

B. Maintain documentation of all security surveys and results at the facility for at least 5 years.

C. Facility security procedures and surveys are subject to inspection by the Assistant Regional Director for Budget and Administration and the Assistant Director - Business Management and Operations or their representatives on request.