FISH AND WILDLIFE SERVICE
RECORDS MANAGEMENT

Records Management **Part 284 Mail Management**

Chapter 3 Mail Security **284 FW 3**

3.1 What is the purpose of this chapter? This chapter describes the Service’s policies and procedures for ensuring mail security.

3.2 What are the responsibilities for mail security? See 284 FW 1 for the responsibilities for all the chapters in Part 284.

3.3 Where can employees find Federal mail security requirements? In addition to the laws, regulations, and policies in 284 FW 1, we must comply with the following policies relevant to security:

A. Department of Homeland Security's Interagency Security Committee (ISC) Physical Security Criteria for Federal Facilities,

B. Department of the Interior Mail Security Policy, and

C. 432 FW 1, Physical Security in Service Facilities.

3.4 What are the Service’s mail security requirements? All Service facilities and offices who conduct physical security assessments (see 432 FW 1 for information) must:

A. Include a site-specific risk assessment (see section 3.5) for mail operations in their overall physical security evaluation on the same cycle as required in 432 FW 1.

B. Include mail security procedures in their overall security procedures (see 432 FW 1, Table 1-1, Item M). The scope, level, and detail of the procedures must be commensurate with the physical security level determination.

C. Implement preventative measures and develop operational procedures based on the results of the site's physical security level, evaluation, and risk assessment.

D. Update mail security procedures on the same cycle as required in 432 FW 1 for physical security assessment renewals.

3.5 What is a risk assessment and what factors must Service facilities and offices consider? The objective of a risk assessment is to determine the likelihood that mail threats will harm our people or operations. Each facility or administrative office may have different threats and risk levels that may lead to the need for different mail security countermeasures. Risk assessments should:

A. Incorporate the components listed in Table 3-1.

Table 3-1: Risk assessment components

Component	**Description**
Asset and Mission Identification - *What are we trying to protect?*	Identify the assets and missions that might be damaged by threats that could come through the mail.

Table 3-1: Risk assessment components	
Component	**Description**
Threat Assessment - *What bad things could happen?*	Identify potential threats including natural events, criminal acts, accidents, and acts of terrorism (and include the likelihood of each).
Vulnerability Assessment - *What are your weaknesses?*	Analyze the extent to which the facility or office is vulnerable to each of the potential threats identified in the threat assessment.
Impact Assessment - *What would happen if your security measures failed?*	Determine the impact on the facility or office if a specific asset were damaged or destroyed, or if specific mission(s) were impaired or temporarily halted.
Risk Analysis - *What does it all add up to?*	Summarize the likelihood and extent of possible damage to facilities or operations based on the impact, threat, and vulnerability assessments.

(See the Service's *Mail Handbook* for more details and suggestions for completing the risk assessment.)

B. Include the minimum security measures listed in Table 3-2 based on the ISC Physical Security Criteria for Federal Facilities.

Table 3-2: Security operations and administration criteria	
If a facility physical security designation level is….	**Then at a minimum you must…**
Level I - Minimum See FWS Form 3-2417	1. Follow ISC guidelines (see section 3.3). 2. Provide employees with annual security awareness training.
Level II - Low See FWS Form 3-2418	1. Inspect all mail/packages and deliveries visually before distributing them throughout the facility. 2. Provide employees with annual security awareness training.
Level III - Medium See FWS Form 3-2419	1. Screen all mail and packages using an x-ray at a loading dock, if present, or at an existing screening location if there is no loading dock. 2. Comply with applicable ventilation requirements listed in the General Services Administration (GSA) Solicitation for Offers. 3. Physically inspect items that cannot be x-rayed. 4. Provide employees with annual security awareness training.

Table 3-2: Security operations and administration criteria	
If a facility physical security designation level is….	**Then at a minimum you must…**
Level IV – High*	1 Screen all mail and packages using an x-ray in a dedicated mail receiving facility located away from facility main entrances, areas containing critical services, utilities, distribution systems, and important assets. 2. Comply with applicable ventilation requirements listed in the GSA Solicitation for Offers. 3. Install an outside wall, door, or window designed to relieve blast pressures. 4. Physically inspect items that cannot be x-rayed. 5. Provide employees with annual security awareness training.
Level V - Very High*	1. Screen all mail and packages using an x-ray in an isolated, external, or off-site mail receiving facility. 2. Comply with applicable ventilation standards listed in the GSA Solicitation for Offers. 3. Physically inspect items that cannot be x-rayed. 4. Provide employees with annual security awareness training.

*At the time this policy was published, the Service did not have any Level IV or V facilities.

3.6 What other security measures should Service facilities/offices consider? All facilities/offices must consider the topics and countermeasures in Table 3-3 when developing site-specific risk assessments.

Table 3-3: Considerations for site-specific risk assessments	
Areas of consideration…..	**Countermeasures to consider…..**
Physical Security Measures	• Locked doors • Ventilation • Badges • Posters • CCTV cameras
Operating Procedures	• Cleaning requirements • Personal protective equipment (e.g., gloves, masks, etc.) • Procedures for handling suspicious packages
Mail Screening	• X-ray • Visual screening • Decontamination stations

Table 3-3: Considerations for site-specific risk assessments	
Areas of consideration…..	**Countermeasures to consider…..**
Training	• Review of mail procedures • Annual staff training • Email communications
Testing Procedures	• Annual reporting • Annual plan review
Plans	• Communications plan • Occupant emergency plan • Continuity of operations plan • Threat management

/sgd/ Rowan W. Gould
DEPUTY DIRECTOR

Date: January 3, 2012