



U.S. General Service Administration

Office of Government-wide Policy • Office of Asset and Transportation Management
Mail Management Policy

Mail Center Security Guide

5th Edition - 2023





This Mail Center Security Guide, 5th Edition represents the collaborative efforts of the Interagency Security Committee (ISC), General Services Administration (GSA), and federal mail professionals to consolidate GSA's Mail Center Security Guide Fourth Edition published in 2014 and the ISC's Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors in 2012 documents into a single resource.

The ISC derives its authority from EO 12977 mandating the ISC enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States occupied by federal employees for nonmilitary activities, and to provide a permanent body to address continuing government-wide security for federal facilities.

Title 41, Code of Federal Regulations (CFR), Part 102-81, Physical Security further specifies ISC policies and recommendations "govern physical security at Federal facilities and on Federal grounds occupied by Federal employees for nonmilitary activities." This regulation is applicable to "federally owned and leased facilities and grounds under the jurisdiction, custody, or control of GSA, including those facilities and grounds that have been delegated by the Administrator of General Services."

Table of Contents

- Introduction 6**
- Purpose..... 6**
- 1.0 Mail Centers 7**
 - 1.1 Types of Mail Centers.....7
 - 1.1.1 Offsite Screening Facilities/Remote Delivery Sites7
 - 1.1.2 Isolated On-Campus Facilities.....7
 - 1.1.3 Primary Office Locations.....7
 - 1.1.4 Single Room Mail Center Operations8
 - 1.2 Mail Center Operations.....8
 - 1.2.1 Incoming Mail Procedures.....8
 - 1.2.2 Outgoing Mail Procedures9
 - 1.2.3 Accountable Mail.....9
 - 1.2.4 Classified Mail10
 - 1.2.5 Interoffice Mail10
 - 1.2.6 Deliveries for Senior Officials10
 - 1.2.7 Personal Mail.....10
 - 1.2.8 Mail Center Opening and Closing Procedures11
- 2.0 Key Roles and Responsibilities 12**
- 3.0 Threats in the Mail Stream 13**
 - 3.1 Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE).....14
 - 3.1.1 Chemical14
 - 3.1.2 Biological15
 - 3.1.3 Radiological/Nuclear.....15
 - 3.1.4 Explosives.....16
 - 3.1.5 Other Dangerous Mailings16
 - 3.2 Illegal or Contraband Items.....16
 - 3.3 Hoaxes.....16
 - 3.3.1 White Powder Envelopes17
 - 3.4 Threatening Content17
- 4.0 Risk Management and Threat Mitigation 17**
 - 4.1 Risk Assessment.....17
 - 4.2 Mail Center Classification18
 - 4.2.1 Daily Mail Volume19
 - 4.2.2 Staff.....19
 - 4.2.3 Number of Satellites.....19
 - 4.3 Staff Vetting.....20
 - 4.4 Mail Screening.....20
 - 4.4.1 Integrating Screening Procedures.....20
 - 4.4.2 Screening Process Best Practices.....22
 - 4.5 Mail Screening Technology25

4.5.1 Mail Processing Tracking Systems.....	26
4.5.2 Chemical Detection/Screening	26
4.5.3 Biohazards	26
4.5.4 Radiation/Nuclear Detection.....	27
4.5.5 Explosive Detection	27
4.5.6 Negative Pressure Environments.....	28
4.6 Sorting and Delivery Best Practices	28
4.6.1 Mail and Parcel Sorting.....	28
4.6.2 Interoffice Mail.....	28
4.6.3 Outgoing Mail.....	29
4.7 Incident Response	29
4.7.1 Initial Response.....	29
4.7.2 Response to Specific Threats	30
4.8 Post Incident Actions.....	32
4.9 Communications.....	32
4.9.1 Internal Communications	32
4.9.2 External Communications.....	32
5.0 Training, Exercises, and Testing	33
5.1 Recommended Training.....	33
5.1.1 Identifying and Handling of Suspicious Mail	33
5.1.2 Screening Procedures	34
5.1.3 Proper Use of Personal Protective Equipment.....	34
5.1.4 Incident Response Procedures.....	34
5.2 Exercises, Drills, Rehearsals.....	34
5.2.1 Exercises.....	34
5.2.2 Drills.....	35
5.2.3 Rehearsals.....	35
5.3 Countermeasure Testing.....	35
6.0 Documentation	35
6.1 Mail Security Policy and Plan	35
6.2 Occupant Emergency Plan (OEP)	36
6.2.1 Key Elements of the OEP	36
6.3 Communications Plan	38
6.3.1 Communications Best Practices.....	38
6.3.2 Communications with Management.....	38
6.3.3 Relationship with Partner Organizations	39
6.4 Continuity of Operations Plan (COOP).....	39
6.4.1 Key Elements of a COOP.....	40
6.4.2 Incorporating the Mail Management Program in the COOP.....	40
6.4.3 Objectives of a COOP for a Mail Facility.....	40
6.5 Annual Review.....	41
7.0 Contracts	41
7.1 Performance-based Service.....	42

7.2 Reviews42

8.0 Conclusion.....42

Appendix A: Glossary43

Appendix B: Acronyms45

Appendix C: Online Resources.....47

Appendix D: Mail Center Security Checklist.....48

Appendix E: Mail Center Screening Requirements and Best Practices54

Acknowledgements62

Introduction

The Federal Agency Mail Management Act (FAMMA) of 2017 authorizes the Administrator of the General Services Administration (GSA) to ensure mail programs are operated economically and efficiently by the federal government. GSA's Office of Government-wide Policy (OGP) administers Code of Federal Regulations (CFR) Part 102-192: Mail Management, which, in accordance with FAMMA, promulgate standards, procedures, and guidelines for federal agencies in the administration of mail management programs. OGP also hosts interagency stakeholder meetings and websites dedicated to identifying and implementing best practices in federal mail programs.

To assist organizations with enhancing the security and protection of their mail programs, the GSA published the first edition of the *Mail Center Security Guide* in December 2001. This Fifth Edition represents updated guidance and practices for the securing of Federal mail centers. The ISC, GSA, and Federal mail professionals collaborated to create this edition.

Purpose

This document strives to capture the latest in mail center security from a broad range of federal organizations and is intended for use by department, agency, and component mail managers as well as individuals within mail centers. Other stakeholders identified in Section 2.0 below play critical roles in the development and implementation of written mail security plans and policies. This document provides mail center managers, their supervisors, and security personnel with a framework for understanding and mitigating risks posed to an organization or facility by the mail and parcels it receives and delivers. This guide offers guidelines and best practices for:

- Identifying types of mail centers and their classification
- Mail center operating procedures
- Identifying stakeholders and their roles and responsibilities
- Assessing and addressing threats in the mail stream
- Risk management and threat mitigation strategies
- Conducting training, exercises, and testing
- Developing security and response plans



1.0 Mail Centers

A mail center is defined as an organization and/or place within or associated with a federal facility where incoming and/or outgoing mail and materials are processed. The centers may be onsite or offsite and can only be designated for screening, sorting, or delivery. The required type and design of a facility depends on the assessed risk and classification of the mail center. Section 4.0 of this guide provides further information on risk assessment and management.



Smallest post office in the U.S. (Ochopee, FL)

1.1 Types of Mail Centers

The mail center type and location are considerations when selecting and implementing mail screening technologies and processes. This process should be done in collaboration with mail program staff, security organizations, and other relevant stakeholders.

1.1.1 Offsite Screening Facilities/Remote Delivery Sites

Organizations with critical functions determined to be of higher consequence associated with their mail and parcel operations may consider an off-site mail and parcel screening facility. Many organizations or subordinate components will incorporate this facility into a remote delivery facility where all deliveries, including supplies and equipment, must be processed. After mail and parcels are received, screened, sorted, and prepared for delivery, secure courier vehicles transport the items to office locations for internal distribution. Security can be enhanced for these facilities by implementing scheduled, permission-based delivery procedures and tracking.

1.1.2 Isolated On-Campus Facilities

Organizations that have critical functions of lower consequence associated with their mail and parcel processing operations may create an isolated, on-campus facility operating similarly to an offsite facility. Although these facilities lack some of the stand-off capability that an offsite facility may provide, they significantly reduce the ability of a suspicious mail piece or parcel to disrupt organization operations for extended periods of time. Separate mail screening facilities isolate any potential threat and enable first responders to address the issue without typically requiring a complete campus evacuation. Whenever possible, these on-campus screening facilities should be physically isolated or separated from other operations and should have separate security and heating, ventilation, and air conditioning (HVAC) systems.

1.1.3 Primary Office Locations

The mail center can consist of multiple rooms or a single room. When the security level, mail volume, and budgetary constraints make separate facilities infeasible or impractical, mail center screening activities can be located within the building that serves as the primary office location for the organization. The mail

center should be placed in an area with direct access to the outside of the building to limit the movement of mail and parcels within the building prior to screening activities. If direct outside access is also not feasible, as a best practice, mail and parcels should be transported in a secure, negative pressure mail cart, or a sealed container if a negative pressure cart is not available, to minimize the spread of any potential biological contaminants. Use of a negative mail pressure cart will not guarantee full containment.

1.1.4 Single Room Mail Center Operations

Due to their minimal mail volumes or severe space limitations, many mail center operations are required to operate from a single room and frequently share a loading dock with other organizations or tenants in the building. These types of mail centers should seek to implement as many of the security capabilities found in larger facilities as possible. There are scalable, configurable, stand-alone, negative pressure mail rooms and small blast containment systems that can provide many benefits of systems designed for multi-room mail centers with large footprints.

1.2 Mail Center Operations

Every federal facility has its own internal process for incoming and outgoing mail based on the risk assessment, facility type, and organizational policies. For specific screening requirements, refer to the risk assessment or *The Risk Management Process for Federal Facilities, Appendix B: Countermeasures* (For Official Use Only - FOUO).

Mail facilities should have standard operating procedures (SOPs) designed to increase the safety and efficiency of mail programs, improve standardization, and reduce training times. Below are some suggested topic areas for SOPs, as well as best practices to consider.

1.2.1 Incoming Mail Procedures

Incoming mail comes into a facility delivered by any service provider, such as DHL, FedEx, UPS, and USPS. The following are best practices for processing incoming mail:



Delivery Vehicle/Driver Processing

- Drivers and anyone accompanying them must have an approved visit request
- Establish procedures for unmarked vehicles or vehicles that are unannounced
- All occupants of the delivery vehicle must present an approved ID
- All occupants will be checked into the visitor's system
- All delivery vehicles should be searched by canine, or other inspection methods, prior to entering the inspection facility
- All mail/parcels, including pallets, that cannot be properly screened should be disassembled and thoroughly inspected



Mail/Parcel Processing

- All mail and/or parcels should be first x-rayed by screeners, if available
- Screeners will count and record number of parcels by carrier
- All mail and parcels will be inspected. Items meeting unsolicited or suspicious criteria should be placed in a safety cabinet or other designated area and processed in accordance with established procedures for suspicious mail
- All mail will have a corner cut and be placed into a paper jogger machine
- All parcels should have a probe inserted into a corner and an air sample taken
- Once all mail and/or parcels from individual carriers have been processed, biological screening should be conducted utilizing established methods by appropriate personnel
- Once all deliveries for the day have been processed and cleared, they may be taken for distribution

1.2.2 Outgoing Mail Procedures

Outgoing mail is generated within a federal facility that is going outside that facility. The following are best practices for processing outgoing mail:

- When the staff goes onto their floors for mail delivery, they should also pick up outgoing mail
- Customers may also take outgoing mail to the mailroom for processing
- Each piece of mail should contain a cost code or information identifying the office that should be charged for the outgoing mail item
- Before metering, the mail clerk logs his or her name, time, and metering station on a sign-in log next to the meter
- Once the mail is metered, it is put into a bin and brought to the loading dock at the close of business and left with security personnel where it is picked up by the USPS or other vendors
- Mail clerks then go through a closing list, checking off everything and writing down the day's final postage numbers and final mail count. All outbound mail is processed for pick up the same day as received in the mail center, except in the case where mail has been dropped off to the mail center after the mail has been picked up for the day

1.2.3 Accountable Mail

Accountable mail is any piece of mail for which a service provider and the mail center must maintain a record that shows the location of the mail item at any given time and when and where it was delivered. Examples of accountable mail include USPS registered mail and all expedited mail.

When handling accountable mail, consider these best practices:

- Require a signature for each piece of accountable mail whenever possession changes
- Verify the delivery manifest sheet to ensure receipt of all parcels listed and accept complete shipments only

- Do not leave any accountable mail at an unoccupied desk or mailbox. Have someone else in the department sign for the piece and contact the recipient via email with directions to pick up the piece at the mail center
- Upgrade technology when applicable such as utilizing an electronic manifest system to speed up the process and increase accuracy. Mail tracking software automates the ability to conduct research on past deliveries
- Retain physical copies of all accountable mail manifests or electronic records in an online software system for at least two (2) years

1.2.4 Classified Mail

Classified National Security Information must be protected pursuant to Executive Order (EO) 12958¹, as amended, against unauthorized disclosure. Part 4 of this EO outlines methods for safeguarding classified information.

1.2.5 Interoffice Mail

Interoffice mail should be visually screened and if suspicious characteristics are noted, the security provider should be notified.

1.2.6 Deliveries for Senior Officials

Some agencies may need to give extra care and attention to letters and parcels addressed to senior officials whose names or positions have increased visibility. Coordinate with representatives from the agency security provider and management (senior executives, executive secretariat, administrators, etc.) to establish procedures for mail addressed to senior officials as needed.

1.2.7 Personal Mail

In most circumstances, policy at the agency and/or facility level should prohibit handling incoming or outgoing personal mail in a federal mail center. The federal regulation on mail management, 41 CFR, 102-192.130(i), authorizes agencies and federal mail managers at the facility level to adopt this policy as well as make exceptions when appropriate.

All employees should be notified that any mail sent to the office is considered “delivered” by the USPS once it is received in the mail center and may be opened by the agency mail center if warranted. However, personal mail should remain sealed against inspection without legal authorization. The only exception is when mail is addressed with an attention line that may render it official.



Pony Express Mail | Smithsonian Institution

¹ [Executive Order \(EO\) 12958](#)

1.2.8 Mail Center Opening and Closing Procedures

Opening and closing procedures, some listed below, that are routinely followed contribute to a safe and secure mail center. Prepare detailed procedures for opening and closing the mail center and ensure logs and checklists are filled out and signed daily. Further, use of a standardized checklist will help ensure all procedures are followed.



Opening Procedures

- Check all locks/entrances
- Start visitor log
- Verify contents of safe/vault
- Take meter readings for manual backup records
- Ensure to deactivate all relevant electronic security system



Closing Procedures

- Take meter readings for manual backup records
- Secure meters
- File visitor log
- Secure all mail
- Create safe/vault contents log
- Ensure that all locks/entrances are closed
- Follow daily procedures for cleaning the area and equipment used to process inbound mail All flat work areas should be wiped down daily with disinfectant²
- Ensure to activate all relevant electronic security system



² Note: All machines should be cleaned with disinfectant wipes and vacuums equipped with high-efficiency particulate absorbing (HEPA) filters. Do not use pressurized air to clean equipment and machinery. Additional cleaning measures may be warranted during extraordinary circumstances such as pandemics and will likely be facility specific.

2.0 Key Roles and Responsibilities

Government mail facilities rely on interdisciplinary teams consisting of organizational leadership, mail managers, security organizations, security providers, and a range of administrative support to ensure regulatory compliance, secure government facilities and assets, and accomplish organizational goals and missions. Each organization should consider and recognize the inputs necessary to ensure their mail program follows organizational policy, FMR Part 102-192, and ISC policies and standards.

Below is a list of key roles for mail program administration and the general responsibilities associated with each of them. Agencies should carefully consider identifying relevant stakeholders and strive to ensure roles are communicated and fulfilled.

Federal Agency Leadership	Bestow appropriate authority and ensure the coordination between cross-functional units (security, mail handling, finance, and procurement) to develop and implement an FMR-compliant federal mail program.
Agency Mail Manager	Manages the overall mail management program of a federal agency and advises agency leadership on regulatory requirements, facility and programmatic needs, and best practices in implementation; expected to apply operational expertise and advocate for adequate implementation of FMR-compliant mail programs; play a central role in the coordinated actions of cross-functional teams following agency mail policy.
Component Mail Managers	Oversee specific agency components and develop and implement policies for the facilities operated by their component.
Mail Center Managers	Oversee the operation of a specific mail center or facility and are typically on-site directing front-line staff in the operation of a mail center; complete mail center classification.
Facility Managers	Interface with the security organization or provider and agency and component mail managers to ensure recommendations and assessments conducted by the security provider are communicated to mail managers and implemented.
Facility Security Committee (FSC)	Addresses facility-specific mail security issues and approves the implementation of security measures and practices in multi-tenant facilities.

Security Organization	The government agency or an internal agency component either identified by statute, interagency memorandum of understanding/memorandum of agreement, or policy responsible for physical security for the specific facility. It coordinates with government-wide resources (ISC, Federal Protective Service (FPS), and United States Postal Inspection Services (USPIS)) to ensure mail facilities, processes, and equipment are adequate to ensure the protection of government assets, facilities, and personnel; coordinates security measure implementation with the tenants; completes risk assessments; assists with completion of facility security plans (FSP) described in chapter 6.0; reviews security plans; and, provides feedback on annual basis.
Security Provider	Oversees the conduct of security assessments; installation and/or maintenance of security countermeasures and components of countermeasures; or contracts with federal agencies to provide security guard services and the personnel employed by them. Ensure performance measurement is conducted on all security systems and practices in accordance with ISC standards. ³
Interagency Security Committee (ISC)	Promulgates security standards and recommendations for all executive branch non-military government facilities.
Procurement Specialists	Provide regulatory support to agency leadership, agency mail managers, and security providers regarding service or equipment procurements.
Budget Officers	Collaborate with agency mail managers and agency leadership to develop sensible budget estimates and ensure appropriate financial controls.
GSA Office of Asset and Transportation Management	Interprets and formalizes the government's statutory responsibilities enumerated by Title 44 of the United States Code Sections 2901-2906 via the FMR Part 102-192. Assists in the development of agency policy and guidance in mail management and mail operations.
Agency Customers	Program offices who routinely send and receive mail as part of their program; engage in mail program operations; communicate program needs to agency leadership, agency mail managers, and other agency staff to ensure the mail program meets the agency's mission requirements.

3.0 Threats in the Mail Stream

Personnel at federal facilities consistently face potential threats in the mail stream. The mail stream provides an opportunity for a threat actor to introduce a hazard to a facility by bypassing traditional

³ [ISC Publications | CISA](#)

security measures. Threats include mail/parcels containing chemical, biological, radiological, nuclear, or explosive (CBRNE) materials and other types of contraband. Although federal facilities were likely less attractive targets during the COVID-19 pandemic due to the irregular manning of nearly all federal facilities, mail operations are likely to face increased threats as federal employees return to the workplace. In many instances, the suspicious mail/parcels are hoaxes; at other times, they present a legitimate threat. All suspicious items should be treated as legitimate threats until a final determination is made.

Suspicious parcel investigations contribute to the large number of improvised explosive device (IED) response incidents tracked annually within the DHS TRIPwire⁴ incident database. Threats that involve CBRNE substances are both dangerous and disruptive. Some, like white powder hoaxes and threatening letters, are merely intended to disrupt the activities of an organization or to express dissatisfaction with a particular individual or policy. The mail center screening process must be able to identify hazardous mail and reduce the risk to an organization's employees, facilities, and daily operations.

3.1 Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE)

3.1.1 Chemical



Chemical threats include nerve agents, blood agents, pulmonary (choking) agents, blister agents, toxic or hazardous industrial chemicals, and irritants and can be presented in solid, liquid, or gaseous/vapor form. Chemical weapons present challenges for both the attacker and for those trying to detect their presence in the mail stream. Chemical threats can manifest with different physical characteristics including appearance and texture and require specific screening procedures. If the goal is to target a particular facility or individual, both liquids and gases must be contained while the mail or parcel is being processed and then released when the item is opened by the recipient, by a timer, or by a remote electronic device.

The procedures described above make it more difficult to use chemical agents as mail-borne weapons. However, chemical weapons can be packaged and deployed using almost any of the courier or local delivery services. Because of their light weight, some gases can also be compressed into small containers that can be mailed using USPS drop boxes. Therefore, mail and parcel screening systems must be capable of identifying the release of chemical agents and, to the extent possible, containing the exposure to limited areas within the mail center or mail screening facility.

⁴ [TRIPwire | \(dhs.gov\)](https://www.dhs.gov/tripwire)

3.1.2 Biological

Biological agents include bacteria, viruses, fungi, other microorganisms, and their associated toxins. They can adversely affect human health in a variety of ways, ranging from relatively mild, allergic reactions to serious medical conditions—even death.⁵

2001 Anthrax Attacks

Considered the worst biological attack in American history, the 2001 Anthrax Attacks killed 5 people, including 2 postal service employees, and infected 17 others. As a result of 4 letters containing powdered anthrax spores and threatening messages, the Brentwood and Trenton mail facilities were closed for several years for decontamination.

These attacks prompted the U.S. Postal Inspection Service to make several changes, such as the installation of Biohazard Detection Systems at all mail processing facilities and new investigative protocols. Also, they improved intelligence gathering capabilities, and trained Postal Inspectors to be in a constant state of readiness for future incidents.

Biological agents are a well-known and recognized category of mail-borne threat since the discovery of the anthrax letters in October 2001. Additionally, the biological agents that cause anthrax, plague, smallpox, and tularemia are potential mail-borne biological weapons. As demonstrated with the anthrax letters, large quantities of dangerous spores can be distributed and disseminated using a common envelope. They can also be distributed via aerosol, although this would require a more sophisticated delivery or dissemination device enclosed in a parcel or envelope. The DHS BioWatch Program⁶ provides early warning of a bioterrorist attack in more than 30 major metropolitan areas across the country.

Due to their small size and the high volumes of dust and paper residue common in most mail centers, biological agents can often go undetected by traditional visual inspections. The incubation period for biological agents can be days or even weeks in some cases, further delaying threat detection. Individuals can be treated successfully once exposed. Early detection will improve the probability and time it takes to recover.

Ricin, another biological threat, can be made from the waste material of processed castor beans, which are considered readily available to anyone. Though this toxin cannot be easily absorbed through the skin, ricin is usually fatal when it enters the bloodstream through a cut or open wound. Small particles of ricin can also be inhaled leading to death in two to three days. These factors make ricin a potentially dangerous substance when deliberately

introduced into a mail center environment.

Agencies and offices that receive mail from sites like jails or other penal facilities should exercise caution. A biological substance that can also be sent via mail is human waste. While not likely capable of transmitting a serious health hazard they do have the potential to carry various bacteria.

3.1.3 Radiological/Nuclear

Radiation threats are derived from various sources ranging from medical grade materials to an explosive combined with radiological material, or "dirty bomb", in the mail stream. Individuals exposed to radiation

⁵ [Biological Agents - Overview | Occupational Safety and Health Administration \(osha.gov\)](#)

⁶ [Detecting Bioterrorism | Homeland Security \(dhs.gov\)](#)

can suffer both immediate and long-term effects. Radiation detection systems used in mail screening operations can detect and identify various types of radiation particles (alpha, beta, and gamma).

3.1.4 Explosives

A wide range of explosive devices and explosive materials have been used in letter and parcel bombs. Military explosives (C-4, "det cord," ammonium nitrate, pentaerythritol tetranitrate (PETN)-based explosives) are all readily available and commonly used. Fortunately, explosives have a variety of characteristics that can be used to help detect them. In addition to their appearance and density, explosive substances emit a vapor trace that can be collected from letters and parcels by using explosive detection canine teams or modern electronic sensors.

Motives for mail bombs are often revenge, extortion, terrorism, or business disputes. Although the likelihood of receiving a mail bomb is very remote, the threat must be taken seriously because a detonation will likely kill or seriously injure those in the vicinity.

Letter mail and parcels are both susceptible to being used as mail bombs. New explosives and the miniaturization of the components necessary to initiate an explosion have made letter bombs more destructive and difficult to detect. The similarity between components of letter bombs and many common electronic devices has further exacerbated this trend. Fortunately, there are many detection technologies and approaches that can be used in even very small mail centers to identify explosive substances.

3.1.5 Other Dangerous Mailings

Beyond containing intentionally dangerous items, mail can contain items that can cut, shock, or explode, such as cell phone or computer batteries, when an item is opened. Although unlikely to cause permanent harm, they do temporarily disrupt the activities of an individual or an organization.

3.2 Illegal or Contraband Items

Drugs, guns, knives, swords, and similar items are also frequently shipped through the mail. Mail center screening processes must be prepared to identify and segregate these items according to organizational policies. For example, some security and law enforcement agencies may allow these items to be received through the normal mail center process while another agency may not allow them.

3.3 Hoaxes

Hoaxes are suspicious mail items designed to present the appearance of a dangerous substance or other threat but do not contain the actual hazardous substance. Hoaxes can be as disruptive to a mail center, facility, or operation as an actual threat.

3.3.1 White Powder Envelopes

The most common type of hoax is the “white powder envelope.” Since the original anthrax letters, any white powdery substance can now create the impression of anthrax. Sugar substitutes, baby powder, corn starch, and many other similar substances have successfully been used to simulate anthrax, leading to the evacuation of mail centers and office buildings. In addition, these hoaxes led to thousands of mail center personnel receiving prescriptions for medications as preventative measures. Frequently, white powder letters also contain threatening markings such as “anthrax inside” to create further suspicion and fear in the minds of the recipients. Screening processes must be able to identify these letters whenever possible and, in all cases, rule out the possibility that the white powder is a dangerous biological substance or toxin.



3.4 Threatening Content

Suspicious mail may contain threatening language on the envelope itself or in the contents of the envelope. This can range from the aforementioned “anthrax inside” to language such as “Death to the President”. Some letters contain detailed descriptions of potential murders or terrorist attacks. Threatening letters must be identified and segregated as early as possible in the mail stream to both maintain their integrity as evidence and to limit any potential emotional harm to the intended recipient.

4.0 Risk Management and Threat Mitigation

Risk management is a comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and when necessary, risk acceptance. The primary goal of risk management is to reduce or eliminate risk through mitigation measures (avoiding the risk or reducing the negative effect of the risk) but also includes acceptance and/or transfer of responsibility for the risk as appropriate. While risk often cannot be eliminated, risk management principles acknowledge that actions can usually be taken to reduce risk.

4.1 Risk Assessment

A risk assessment is the process of evaluating credible threats, identifying vulnerabilities, and assessing consequences. Per ISC standards⁷, risk assessments will be conducted by the security organization once every five years for the Facility Security Level (FSL) I & II (lower risk) facilities and once every three years for FSL III-V (higher

Risks associated with mail facilities must be included as part of the recurring risk assessment for federal facilities.

⁷ [ISC Publications | CISA](#)

risk) facilities. Risks associated with mail facilities must be included as part of the recurring risk assessment for federal facilities. Risk assessments are crucial at the onset of designing a facility that will receive or handle mail. Security organizations conducting risks assessments must coordinate with mail center managers to ensure the correct mail center classification as this may influence outcomes.

Mail center managers have an integral role in the risk assessment and risk management process and should be consulted during the actual assessment as they are best positioned to describe potential threats, vulnerabilities, or consequences for their specific mail facility. Mail center and agency mail managers should attend Facility Security Committee (FSC) meetings and final risk assessment presentations by the security organization to learn of any identified risks and recommended countermeasures. At minimum, mail center managers should be provided a briefing and copies of the risk assessment sections that apply to mail management.

Mail center managers have an integral role in the risk assessment and risk management process.

A risk assessment is credible when it considers threat, vulnerability, and consequence.

Threat is defined by the ISC as the intention and capability of an adversary to initiate an undesirable event (UE). To determine applicable threats, organizations should consult *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, Appendix A: The Design-Basis Threat Report-* (FOUO) (DBT). The DBT outlines UEs that can potentially impact the mail stream and includes scenarios and the probabilities associated with each. Applicable UEs extend beyond traditional threats that may occur in the mail stream such as theft of mail facility assets like stamps.

A **vulnerability** is a weakness in the design or operation of a facility that an adversary can exploit. For example, biological material or an explosive device can be introduced to a facility through the mail stream in an undetected manner.

Consequence is the level, duration, and nature of the loss resulting from an undesirable event. Some questions to consider are: 1) If the mail center shut down, would the entire facility also have to shut down? 2) If a mail center incident requires evacuation of the building, what effect will that have on the daily operations of the organization? 3) Will critical functions be disrupted? 4) Will clients be affected?

4.2 Mail Center Classification

Mail center classification supports risk assessments and development of mail facility operational procedures. An initial mail center classification is calculated by the mail center manager followed by department or agency guidance for final approval and validation of classification.

Table 1 below presents a basic strategy for the sizing of mail centers (departments or agencies may develop their own classification guides). The size classification is derived by quantifying a range for the factors described below, driven primarily by daily incoming mail volume. This approach provides a basic level of classification which can then be integrated with other elements to arrive at the recommended type of facility and associated screening technologies to be employed in each situation.

The classification of mail centers as small, medium, or large depends on several factors. The generally accepted view is that incoming mail is screened, and outgoing mail is not. The rationale for this approach is that outgoing mail poses a low probability of threat. The greatest threat, as demonstrated by actual events, comes from external sources who are attempting to use the mail stream to introduce their threat to an area, organization, group, office, or individual. Therefore, when focusing on best practices and procedures for mail screening, incoming mail is most important.

The following sections outline considerations when sizing mail centers for mail screening. The final classification is determined by the highest rated criteria. For example, a facility that processes greater than 10,000 pieces of mail, has 15 employees, and no satellite locations would be classified as a large-mail center.

4.2.1 Daily Mail Volume

The daily throughput of a given mail center will have a significant impact on the design and operation of any proposed mail screening and handling procedures. When considering volume, it is necessary to include the number of First-Class letters and flats received, the number of parcels, and the number of parcels or letter envelopes received from third-party couriers (e.g., FedEx, UPS, DHL, etc.). Notably, in a wide range of operational areas there is general acceptance that “marketing mail” (magazines, newspapers, and other types of mail that can be processed and delivered in “bulk” form) is exempt from the normal screening processes, is not considered a threat because it is from a known originator and is not considered when establishing daily mail volume for screening processes.

4.2.2 Staff

The staffing level of a given mail center will be a direct result of the factors described above. The number of full-time and part-time personnel, their skill sets and levels of training, as well as the ability to augment the staff factor into the design and selection of mail screening and handling procedures.

4.2.3 Number of Satellites

The number of satellites represents the number of associated subordinate facilities supporting an agency’s mail management program. Satellite mail centers may require redundancy in any proposed mail screening and handling procedures. Although the type of incoming mail screening may be similar, such as X-ray scanning, the scale of the screening solution could vary between primary mail centers and satellite locations that support the same organization.

Classification	Daily Mail Volume	Staff	Number of Satellites
Small	<1000	<10	None
Medium	1000 – 9,999	10-49	<3
Large	10,000+	50+	3+

Table 1, Mail Center Classification Criteria

4.3 Staff Vetting

Personnel vetting is the process by which individuals undergo investigation, evaluation, and adjudication. It encompasses the policies, processes, and tools used to determine whether personnel should be trusted-

- a. with a credential granting access to government IT systems or facilities (*Credentialing*)
- b. to work for—or on behalf of—the government (*Suitability/Fitness*)
- c. to occupy a sensitive position, which may include having access to classified information (*National Security*)

Trusted Workforce 2.0⁸, or TW 2.0, aims to better support agencies' missions by reducing the time required to bring new hires onboard, enabling mobility of the Federal workforce, and improving insight into workforce behaviors.

4.4 Mail Screening

For efficiency and effectiveness, mail screening processes should be well-designed and properly integrated into the overall process of receiving, sorting, and delivering mail and parcels. A best practice is to identify and map out the current end-to-end mail receiving and delivery processes before inserting screening technologies or processes. When practical, mail screening operations should take place in a location isolated from other facility operations and separate from areas where personnel are screened.

Many aspects of screening technology selection will require a solid understanding of mail and parcel volumes, accountability procedures, transfer requirements, and courier routes. This is particularly important in small mail centers where a few individuals must perform multiple tasks sequentially. Process mapping enables the mail center manager to ensure the screening workflow does not create any unexpected security violations or unnecessary contamination.

Any deviation from approved procedures can easily lead to suspicious mail or parcels being missed or the inadvertent cross contamination of other items, equipment, facilities, or employees. Most screening procedures, including the visual identification of suspicious parcels, are focused on identifying threats (biological, chemical, etc.) while a few, such as x-ray scanners and vapor trace detectors, have multi-substance capabilities.

4.4.1 Integrating Screening Procedures

The following top-level processes represent a partial list for mapping and evaluating mail screening requirements. Though not applicable to every mail center operation, each step in the process presents opportunities for suspicious mail to enter the mail sorting system or be transferred from one employee to the next. Each step also provides an opportunity for suspicious mail to be identified, isolated, and contained before it can cause harm to the intended recipient.

⁸ [Trusted Workforce 2.0](#) - Launched in 2018, Trusted Workforce 2.0 is the most far-reaching reform of the Federal Government's personnel vetting system ever.

4.4.1.1 Mail and Parcel Pickup from Designated U.S. Postal Service Facility

If mail is being picked up at USPS facilities, only authorized personnel specifically identified by the organization should be allowed to sign for materials. Mail center staff should designate and identify personnel authorized to sign for mail at the USPS facility.

4.4.1.2.1 Transportation to the Mail Center or Mail Screening Facility

Courier vehicles provided by the agency should be secured (e.g., padlock, locked seal, one-time locks) when loaded with mail and parcels during transport. Vehicles should be locked and attended at all times. When receiving mail and parcels from couriers or other delivery services, personnel should be positively identified before accepting any items, and recipients should then validate that they are receiving the actual items on the manifest before signing for them.

4.4.1.2.2 Tracking and Accountability Process

All accountable mail items and parcels should be tracked by digital scanner or ledger from the moment they are picked up or received until they are delivered to and signed for by the intended recipient. Agencies should consider adopting digital tracking methods for accountable mail items.



4.4.1.2.3 Transfer of Mail and Parcels to Mail Center Screening Personnel

Mail and parcels should not be left unattended on the loading dock or in a publicly accessible area. Mail and parcels should not be left outside mail facilities after hours. Agencies should mandate a “warm handoff” as mail and parcels are transferred.

4.4.2 Screening Process Best Practices

Individual screening processes may vary based on the risk assessment and the specific technology employed. Mail center personnel must be observant for suspicious mail and parcels at every stage during the receipt, sorting, and delivery of mail. Many suspicious items, such as hoax letters and parcels containing hazardous materials, are capable of being detected early in the sorting process by properly trained mail handlers. USPS Publication 52, *Hazardous, Restricted, and Perishable Mail*⁹ provides important information to help mailers determine what may be mailed and how certain items must be packaged to keep the mail safe.

The following are indicators that further scrutiny may be required:

- Excessive postage, no postage, or non-canceled postage
- No return address or obvious fictitious return address
- Unexpected parcels or parcels from someone unfamiliar to you
- Improper spelling of addressee names, titles, or locations
- Unexpected envelopes from foreign countries
- Suspicious or threatening messages written on parcels
- Postmark showing different location than return address
- Distorted handwriting or cut-and-paste lettering
- Unprofessionally wrapped parcels or excessive use of tape, strings, etc.
- Parcels marked as "Fragile - Handle with Care," "Rush - Do Not Delay," "Personal" or "Confidential"
- Rigid, uneven, irregular, or lop-sided parcels
- Parcels that are discolored, oily, or have an unusual odor
- Parcels that have any powdery substance on the outside including powder under tape used to secure the parcel
- Parcels with soft spots, bulges, or excessive weight
- Protruding wires or aluminum foil
- Visual distractions
- Suspicious objects visible when the parcel is x-rayed

Figure 1 is an example visual aid for how to respond when identifying suspicious mail and parcels.

⁹ [Publication 52 - Hazardous, Restricted, and Perishable Mail | Postal Explorer \(usps.com\)](#)

SUSPICIOUS MAIL OR PACKAGES

Protect yourself, your business, and your mailroom.

If you receive a suspicious letter or package:

- Stop. Don't handle.
- Isolate it immediately.
- Don't open, smell, or taste.
- Activate your emergency plan. Notify a supervisor.



If you suspect the mail or package contains a bomb (explosive), or radiological, biological, or chemical threat:

- Isolate area immediately
- Call 911
- Wash your hands with soap and water



Figure 1, Identifying Suspicious Mail or Packages Poster

For individual item screening, mail should be perforated, cut, and tumbled or opened prior to a sample being taken. These processes will enhance the likelihood that an adequate volume of material will be collected for proper identification. They will also help identify suspicious powders not detected by systems focused on actual biological agents.

[Note: Sample collection should be conducted according to American Society for Testing and Materials (ASTM)¹⁰ guidance.]

Mail trays, tubs, and individual items must be inspected for obvious signs of white powder, liquids, or suspicious markings as they are unloaded from a courier or mail vehicle at the loading dock. If detected, the suspicious items and the tray or tub used for transport should be immediately segregated.

4.4.2.1 Chemical

Continuous screening of the environment in and around the mail screening facility and/or mail center should be conducted.

4.4.2.2 Biohazards

Samples should be collected from mail and parcels and tested for common biological hazards at a Centers for Disease Control (CDC) Laboratory Response Network (LRN) laboratory or using onsite polymerase chain reaction (PCR) equipment. As a best practice, it is strongly recommended that any on-site testing that results in a positive detection event be verified and confirmed by the LRN. All mail items should be kept under quarantine in a negative pressure environment until negative test results have been obtained.

4.4.2.3 Radiation/Nuclear

Trucks and delivery vehicles should be screened as they are approaching the mail screening facility, and again at the loading dock. Screening methods should be based on the assessed risk of the threat.

4.4.2.4 Explosives

Screening of vehicles, mail, and parcels should be done using explosive detection canine teams prior to bringing items into the mail screening facility. Mail tubs or trays and individual parcels should be screened using an X-ray scanner equipped with explosive detection software. Other options include portable and handheld vapor trace detection systems.

4.4.2.5 Dangerous Items and Contraband

Screening for dangerous items should be done using aggressive, visual screening and the X-ray scanner.



¹⁰ [ASTM International - Standards Worldwide](#)

4.4.2.6 Alternate Worksite Procedures

It is the agency's responsibility to develop a plan for receiving mail and parcels at an alternative worksite such as a telework center or employee residence. As a best practice, incoming mail should be screened at a federal facility before sending it to employees at alternative worksites.

Agencies should consider the following when developing alternate worksite policies:

- How employees will receive official mail (USPS, FedEx, UPS, other service provider(s) considering who the sender is)
- Refrain from sharing home addresses, when possible
- Consider setting up post office boxes (prevents release of home address)
- Accountable tracking for sending mail from alternative worksites
- Mail security steps employees must implement for receiving, sending, and storing official mail

4.4.2.7 Personal Protective Equipment

Personal protective equipment (PPE), including gloves, aprons, safety glasses and respirators, should be available for all mail center personnel. Use of respirators may not be required if the risk assessment does not support it. Consider special measures for mail facilities that routinely receive medical devices or other potential hazards.

If PPE is in use, mail center managers should ensure all equipment is kept clean and properly serviced and that all personnel receive training on its proper use. Further, these managers should establish a log to monitor employee initial training and periodic retraining since the equipment can be problematic. For example, removing gloves the wrong way can spread contamination. Likewise, respirators can induce respiratory problems in some people.

The CDC provides guidance on selecting PPE to protect against bioterrorism. For the most current information, refer to the Centers for Disease Control¹¹ or Occupational Safety and Health Administration¹² website.

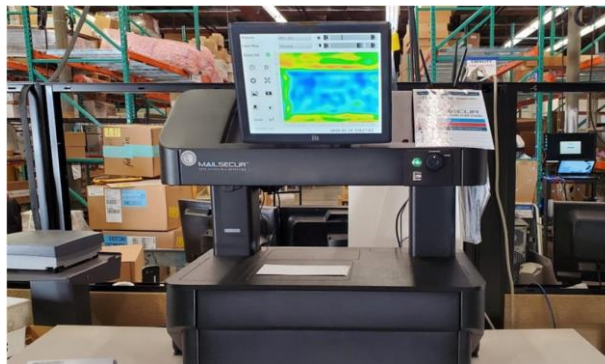
Decontamination facilities such as emergency showers and eyewash stations should be in easily accessible areas within proximity to mail screeners.

4.5 Mail Screening Technology

Mail screening technologies are used to improve safety at mail processing locations where professionals have determined the threat is sufficient to justify their employment.

Technologies are complimentary to screening done by humans and are only as good as the procedures that accompany them.

Standardized procedures strengthen the effectiveness of screening technology by adding



¹¹ [Welcome to PPE-Info \(cdc.gov\)](https://www.cdc.gov/ppe/)

¹² [Personal Protective Equipment - Overview | Occupational Safety and Health Administration \(osha.gov\)](https://www.osha-slc.gov/Personal-Protective-Equipment-Overview)

a heightened level of integrity while minimizing opportunities to circumvent these countermeasures. It is essential mail center staff learn how to use, implement, and integrate relevant mail screening technologies into their standard operating procedures.

When implemented, screening equipment should be accompanied by an appropriate maintenance plan and incorporated with an overall performance measurement program.

This section provides an overview of various mail screening technologies that may be implemented in mail facilities. To identify appropriate screening methods and technologies for a specific facility, refer to the facility's risk assessment and mail center classification.

4.5.1 Mail Processing Tracking Systems

Automated tracking systems will enable easier “back tracking” and identification of potentially contaminated areas of a mail center if a dangerous item or contaminant is discovered downstream from the mail center. Organizations may implement a barcode, radio-frequency identification, or other tracking system enabling positive control over individual trays, tubs, and other mail equipment throughout the entire screening, sorting, and delivery process.

4.5.2 Chemical Detection/Screening

Chemical detectors and sensors are used to verify the presence of toxic chemical agents or substances in the mail stream. When screening individual mail items, perforating, cutting, and tumbling or opening mail prior to a sample being taken will increase the likelihood of collecting an adequate volume of material for proper screening. Targeted sampling is also an effective method of detection. It will also help identify suspicious powders not detected by systems focused on actual/specific chemical agents.

Mail centers with chemical detection sensors located in the loading dock area and in mail and parcel screening rooms should be capable of detecting and identifying a wide range of chemical weapons and toxic and hazardous industrial chemicals through adequate and targeted sampling. The chemical sensors should provide an obvious audible and visual alarm in the immediate area and link to the organization's security command center to be monitored on a continuous basis.

4.5.3 Biohazards

Biohazard detection systems, also called autonomous pathogen detection systems, are designed to monitor the air and detect the presence of airborne toxins, pathogens or other biological agents. Refer to CDC guidelines¹³ for environmental air sampling methods and equipment. Biohazard screening can be implemented on an individual mail item as well as in bulk (tray). Piece-level screening increases the likelihood of identifying biological agents, but significantly decreases the speed of mail processing.

When required, biohazard screening of individual mail should be executed by perforating, cutting and tumbling, or opening mail prior to a sample being taken, increasing the likelihood an adequate number of

¹³ [Environmental Sampling | Background | Environmental Guidelines | Guidelines Library | Infection Control | CDC](#)

biological materials including spores (test sample) is collected for proper screening. This will also help identify suspicious powder not detected as biological agents that may still be hazardous (e.g., aluminum, magnesium). [Note: Sample collection should be conducted with CDC-approved collection media and devices using ASTM guidelines.]

In addition to collecting samples from the mail itself, screeners should collect samples from the trays and tubs used to transport the mail and from the mail screening and processing equipment. If preliminary tests result in a positive detection event or a biological test substance, it is strongly recommended such samples be evaluated by a CDC LRN laboratory for verification, if available. Such mail and parcels should continue to be kept in local quarantine under biosafe procedures to prevent release from the storage location until the results of the CDC LRN lab tests are established.

4.5.4 Radiation/Nuclear Detection

Radiation/nuclear detectors are devices that sense and relay information about possible radiation threats. Radiation takes the form of alpha particles, beta particles, gamma rays, and X-rays. Some of these are more easily detected than others, but all are invisible to the human eye. To enable detection, pedestal or wall-mounted radiation detection equipment may be placed at the first vehicle point of entry to the secure perimeter. Additional radiation detection devices including handheld and portable devices may be mounted in the loading dock area and monitored by personnel within the organization's security command center.

Screening personnel working on the loading dock while radiation/nuclear precautions are in place should be required to wear personal radiation detection pagers while they are unloading mail.

4.5.5 Explosive Detection

Virtually all mail bombs can be detected by skilled X-ray inspection of letters and parcels. To ensure that X-ray inspectors are paying close attention, consider using software that randomly inserts a test image of a suspicious parcel among the images of actual letters and parcels being scanned.

Hand-held and tabletop explosives trace detection equipment can be used to detect the presence of explosives within items or explosive residue on the exterior of mail and parcels. Though most trace detection systems are of limited use in high-volume mail screening operations because of the requirement to collect an air sample, or a swipe from each item being tested, they can be used effectively for second-level evaluations of suspicious items and for testing courier vehicles and personnel.

X-ray scanning systems have long been the most widely used technology to detect bombs and other dangerous items in mail and parcels. Mail and flats can be screened while in trays or tubs while parcels should be screened individually. Most modern X-ray systems have software designed to help the screener identify explosives based on the density of the substance. The effectiveness of X-ray screening is highly dependent on the training level and attentiveness of the equipment operator.

Mail centers that process a large volume of electronics will find X-ray scanning of parcels is especially challenging because many electronic devices look like explosive devices when viewing them with an X-ray

system. X-ray scanning systems should be capable of producing and saving digital images during the scanning process to be viewed remotely for additional evaluation purposes.

Explosive detection canines (EDCs) can also be used to inspect courier vehicles as well as mail trays or tubs before they are brought into the primary mail screening facility. Properly trained canines can detect most, if not all, common explosives and screen a high volume of mail and parcels for explosives in a relatively short period of time.

In addition to detection equipment, there are several types of explosive containment devices for use in mail centers intended to enclose an explosive and to some degree contain the explosive effects resulting from detonation of a device. Reference the facility's risk assessment for containment device design and capability requirements.

4.5.6 Negative Pressure Environments

Negative air pressure combined with the use of air filtration (usually high-efficiency particulate air (HEPA) filters) is used to protect people and the environment outside the negative pressure room or facility. Potentially hazardous molecules, toxins, and drugs can be separated from the work area and/or the entire building. Negative air pressure rooms are designed to achieve an appropriate number of air changes per hour (ACH) according to CDC guidelines, reducing the potential threat to personnel and facilities and making cleanup of any actual contamination easier. These systems can be built as integral components of the mail screening facility or can be provided as separate, portable configurations. In all cases, the systems will need access to heated and cooled air, or provide their own, for the comfort of the mail screening personnel. Negative pressure systems should not be connected to the facility's centralized HVAC systems. Additional guidance on creating negative pressure environments can be obtained from the American Society of Heating, Refrigerating and Air Conditioning Engineers.¹⁴

4.6 Sorting and Delivery Best Practices

4.6.1 Mail and Parcel Sorting

Mail and parcels should be sorted in a secure facility that provides access only to mail center personnel.

Mail transported from the screening facility to the delivery locations should always be secured. An organization's mail transport vehicles should be locked and sealed from the time they leave the screening facility until they are opened by an authorized individual at the delivery site.

Items being delivered should not be left unattended. The intended recipient or an authorized individual should sign for accountable mail and parcels.

4.6.2 Interoffice Mail

Interoffice mail should be treated like all other mail and delivered only to the intended recipient or an authorized individual. Further, these pieces should be picked up from a designated individual and "drop sites" should not be accessible to the public. Best practices include use of special accountable interoffice envelopes that can be tracked from sender to recipient using the mail center tracking system.

¹⁴ [Home | ashrae.org](http://ashrae.org)

If the organization's risk assessment suggests interoffice mail may be accessible to external personnel, mail center personnel should transport interoffice mail back to the mail screening facility for screening processing. If this is not possible due to distance or time limitations, mail center personnel should conduct an aggressive visual screening of interoffice mail while it is being sorted for delivery.

4.6.3 Outgoing Mail

Outbound mail should be picked up only from secure drop boxes or authorized individuals and always be secured until it arrives at the mail center for further processing. Outbound "drop sites" should not be accessible to the public.

Outbound mail should be inspected for suspicious indicators and items containing authorized, hazardous materials should be properly marked.

Outbound mail should not be left unsecured on the loading dock or at other locations while awaiting pickup by the USPS or express couriers. Mail being transported to USPS facilities should always be secured with courier vehicles attended and locked.

4.7 Incident Response

4.7.1 Initial Response

Suspicious mail response procedures will vary by organization and will be based on a combination of factors, such as the type of item discovered, the location of the mail screening facility, internal facility configuration, the number of personnel in the facility, and specific organization emergency response protocols. Procedures should be established and codified in occupant emergency and facility security plans. These steps are common to every event:

- Remain calm
- Alert others in the immediate area that you have identified a suspicious item
- Notify command center/first responders. If in a multi-tenant facility, building management and FSC Chair should also be contacted
- Activate the occupant emergency plan (OEP) and/or facility security plan (FSP)
- Stabilize the suspicious item and do not attempt to move it
- Put the envelope or parcel on a stable surface if it is currently being carried or handled by mail center personnel
- Do not sniff, touch, or taste any contents that may have spilled
- Do not shake or share the letter or parcel

[Note: If X-ray inspection shows a secondary container that may contain an unknown material, or if you open a letter or parcel and discover such a container, do not open or otherwise disturb the secondary container. Treat the secondary container as suspicious mail and call the addressee to see if they can identify the container. If the addressee cannot be located, then call in the first responder designated to open suspicious mail.]

Consideration should be given to whether the air distribution system in the building should be shutoff. Facility design, location of the mail center within the facility, and type of incident are factors that contribute to this decision. If the mail center has an isolated HVAC system, it may be better to leave it running to ventilate contaminants outside the building. Conversely, if the center is integrated with the entire facility's HVAC system, it may be best to shut it off to prevent further distribution of contaminants throughout the facility. When required, provide an emergency shutoff switch in the HVAC control system that can shut down air distribution throughout the building. The switch (or switches) should be located to be easily accessible by building occupants.

To minimize exposure to chemical or biological-laden envelopes and parcels, mail handlers should use gloves when handling mail and have several large sealable bags nearby for isolating suspicious mail and discarding all clothing worn when in contact with a suspicious parcel. Surgical masks or protective masks and a change of clothing should also be kept in mailrooms. Powder coated gloves should be avoided as the powder may be associated with a chemical or biological contamination from the mail.

Suspicious mail will often lead to an investigation by local police, the U.S. Postal Inspection Service (USPIS), or the Federal Bureau of Investigation. Mail center personnel should be taught not to destroy evidence by vacuuming up white powder, shredding suspicious letters, disposing of dangerous parcels, or similar activities.

Managing threats encompasses the procedures for examining letters and parcels, identifying suspicious ones, and calling in an expert when necessary. If a suspicious item is identified, first responders will assess the suspicious item and identify potential for CBRNE devices. They will also provide direction for mail room occupants.

4.7.2 Response to Specific Threats

4.7.2.1 Chemical Substance

In chemical attacks, a solid, liquid, or toxic gas is used to contaminate people or the environment. If faced with such an attack, leave the mail screening area and close any doors to prevent others from entering the area. If possible, shut off all fans and the ventilation system of the local facility and leave as soon as possible and go outside, moving upwind and away from the area. Be aware of prevalent symptoms of chemical attacks: tightness in the chest, difficulty breathing, blurred vision, stinging of the eyes, or loss of coordination.

The United States Postal Inspection Service uses the acronym "**S.A.F.E.**" to address potential threats:

- **S**afety comes first.
- **A**ssess the situation before acting.
- **F**ocus your efforts on the hazard, avoiding contact and access
- **E**valuate the situation and notify authorities.

If you witness a suspected chemical attack outdoors, move upwind and away from the area as quickly as possible. If this is not possible, move to a safe location inside a building and shelter-in-place. If you suffer any of the symptoms mentioned above, try to remove any clothing you can and wash your body with soap and water. Do not scrub the area, as this may wash the chemical into the skin. Seek medical advice as soon as possible.

4.7.2.2 Biological Substance

Effective countermeasures are available against many of the bacteria, viruses, and toxins that are potential threats to the mail stream. Understanding the biological threats and how to respond to them can prevent or minimize many effects. Some response best practices are:

- Remain in the negative pressure mail screening environment until directed to leave by first responders/HAZMAT personnel.
- If there is no negative pressure system, shut off any fans and the ventilation system of the local facility and await arrival of first responders/HAZMAT personnel.
- Follow guidance from emergency response personnel.

Remember that unlike chemical and radiological agents, biological agents are not as immediately recognizable, and consequences may be delayed. For example, victims of biological agents may require therapy or vaccination that is not performed by first responders.

4.7.2.3 Radiation or Nuclear Substance

Leave the immediate area where the radiation source appears to be located without touching any source material or the packaging materials surrounding it. Consider ALARA (as low as reasonably achievable)¹⁵ principles of putting as much time, distance, and shielding between people and the radiation source when developing response plans. First responders that specialize in these types of events should conduct secondary assessments and provide further guidance.

4.7.2.4 Explosive Device

A mail bomb can be enclosed in either a letter or a parcel. Its outward appearance is limited only by the imagination of the sender.

When a suspected explosive device is discovered, personnel should leave the mail screening area and initiate notification procedures immediately. Seek shelter inside a building putting as much distance and shielding between you and the potential device as possible and wait for directions from first responders. Refer to facility's OEP for specific guidance. If the mail or parcel is inside an x-ray scanner, leave it there. Do not use cell phones or radios within the immediate proximity of the suspicious parcel, a critical prohibition that should be included in all mail screening training.

America's History of Mail Bombings

- **1919 Mail Bombs:** USPS intercepted 36 mail bombs that targeted prominent Americans.
- **1936 Cigar Box Bomb:** A bomb hidden in a cigar box sent through the mail killed a father and son in Wilkes-Barre, PA.
- **1947 Letter Bombs sent to President Truman:** A letter bomb intercepted by White House mail room and was defused.
- **1975-1996 – Unabomber:** Ted Kaczynski killed 3 and injured 23 others utilizing mail bombs.
- **2018 Austin Bomber:** Mark Conditt terrorized Austin, TX for a 3-week bombing spree, killing two people.

¹⁵ [Radiation Studies - CDC: ALARA](#)

Dirty bombs are regular explosives that have been combined with either radiation-causing material or chemical weapons. While most news reports talk about radiological dirty bombs, chemical agents may be used as well. A blast from this type of weapon normally looks like a regular explosion and the contamination spread is often not immediately noticeable.

For more information on mail bombs, check with your local postal inspector or visit the USPS website¹⁶.

4.7.2.5 Dangerous Mailings and Contraband

Report suspicious items to the mail center manager and/or security command center for further inspection. Notify local law enforcement as required.

4.7.2.6 Threatening Content

Documented threats directed towards a facility, agency, or employees should be evaluated by the security provider, security organization, and/or law enforcement, not dismissed as administrative issues.

4.8 Post Incident Actions

Following an incident, the mail center manager and the organization's security personnel should conduct a joint review of the incident and response actions with mail center employees and first responders. Employees should be given an opportunity to speak with medical personnel, human resources representatives, environmental health and safety professionals, and other organization personnel as desired. The mail center manager should also document and share information about the incident with other mail center managers as permitted by organization security protocols and general policies and procedures.

4.9 Communications

All incidents involving suspicious mail and parcels must be reported immediately to mail center management personnel and/or security or local law enforcement and first responders. If the facility is a multi-tenant facility, building management and the FSC Chair should be contacted as well.

4.9.1 Internal Communications

Within the mail center, managers should provide employees an initial briefing and regular updates during an ongoing incident. This is especially important when a suspicious item has necessitated the evacuation of the mail center. Further, mail center personnel should be briefed as soon as possible on any required or recommended medical treatment in accordance with guidance provided by emergency medical personnel, first responders, and/or public health officials.

4.9.2 External Communications

The mail center manager should work directly with organization management and security personnel to outline procedures and protocols for initiating contact with external agencies (public health agencies).

In emergency situations, the mail center manager must be able to place calls directly to local first responder personnel. This matter should be addressed in response planning prior to a potential event occurring. Further, designated security personnel within the organization or the mail center manager

¹⁶ [United States Postal Inspection Service \(uspis.gov\)](https://www.uspis.gov)

should serve as the primary point of contact for local law enforcement and first responders at the mail center during an ongoing incident.

Mail center personnel should never speak directly to the media about an ongoing incident. All external communications about an incident should be controlled by the organization's public affairs office or similar office, in conjunction with the controlling federal, state, or local authorities.

5.0 Training, Exercises, and Testing

Education and awareness are essential components to preparedness. Through training and exercises, a security awareness culture can be developed in any organization. Rehearsals provide critical lessons that are ingrained and retained. The actions taken before an incident have a lasting impact on the safety of everyone while the actions taken during an incident have an immediate impact. Preparing the mail center staff to handle a threat is imperative.

Agency, component, and mail center managers as well as agency training managers play central roles in accomplishing the security training needs of federal facilities. Security providers maintain comprehensive training plans for response to various situations. Mail staff at all levels are encouraged to take advantage of these resources, which should be available upon request from the security provider.

Agency and component mail managers, in coordination with agency training managers and security providers, should ensure training plans are responsive to the mission and scope of each facility. Training needs may reflect unique facility specifications, including mail piece volume and type, equipment, and processes. To assist with this effort, consider the following tips:

- Identify the security countermeasures in the mail facility
- Assess the capabilities of staff to operate security countermeasures and take note of knowledge or training needs
- Coordinate with security providers, facility management, and agency leadership to identify and access training

To be effective, any training plans must be continuously reviewed and updated as needed. This is especially true with security issues. Schedule sessions to update employees on a regular basis. Agencies should maintain a training log, with course name and completion date, for all mail center employees.

5.1 Recommended Training

The training outlined in this section should be conducted annually and is not all inclusive. While posters, videos, and online training packages are available to help mail center managers conduct training, organization security personnel, USPS, and commercial security contractors can also provide training.

5.1.1 Identifying and Handling of Suspicious Mail

Mail center staff should understand the risks associated with the various threats that can be introduced through the mail, the characteristics of each, and the proper response to suspicious items. At minimum, all mail center personnel should receive annual training on these topics.

5.1.2 Screening Procedures

Well-designed and consistently executed screening processes are essential for both identifying suspicious items and limiting their impact once discovered. This training is best accomplished by highly qualified trainers supplied by the equipment vendors themselves. The record of training should be maintained and tracked for all employees.

5.1.3 Proper Use of Personal Protective Equipment

When PPE is provided, mail center personnel should receive training on the proper use and storage of PPE. This includes fit testing, donning, removal, and disposal of the PPE.

5.1.4 Incident Response Procedures

Mail center personnel should receive training in established response procedures. The specific procedures (e.g., personal decontamination) required for each mail center vary based on the organization's respective risk assessment, security countermeasures, and characteristics of the mail center's customized level of protection per ISC standards. This training should include communications with other mail center personnel and the organization's management and security personnel. It should also be coordinated with the occupant emergency program and other facility-specific security plans.

When conducting incident response training, it is important to involve all first responder and public health organizations likely to be called to an incident at the facility to increase collaboration and decrease the likelihood of an overreaction causing a major disruption.

USPIS Publication 166¹⁷ can provide additional guidance.


5.2 Exercises, Drills, Rehearsals

One key to performance during an actual emergency is testing plans in advance of an incident. Test response plans and emergency scenarios at least annually with employees to ensure they will know how to respond. It reinforces the training so the plans can be effectively implemented in the event of an actual emergency. Exercises, drills, and rehearsals can be employed to facilitate testing of plans. All exercises, drills and rehearsals should be documented, and records maintained.

5.2.1 Exercises

Exercises are used to examine and/or validate plans and programs. Exercises can involve multiple response elements to validate the coordination, command, and control between various response entities (e.g., a coordinated response to an explosive device).

Exercise participants should cooperate fully with facility management and security providers during these events. Mail managers should work with facility management and security providers to ensure exercise schedules are adhered to.



Tabletop exercises can test procedures in a way that does not alarm employees and customers but follows the steps taken during an incident.

¹⁷ [Additional Resources - USPIS](#)

5.2.2 Drills

A drill is a coordinated, supervised activity usually employed to test a single, specific operation or function within an organization (e.g., a decontamination drill).

5.2.3 Rehearsals

In addition to, and between times when exercises and drills are conducted, mail center managers and the organization's security provider should conduct regular rehearsals and evaluate the performance of mail center personnel. Individual performance standards are reviewed and measured during these rehearsals.

These rehearsals will help ensure the lines of communication function as planned and everyone knows their role. Hold post-test meetings to address problems and resolve them before the next test.

5.3 Countermeasure Testing

Routinely request and cooperate fully with facility management and security providers in the implementation and functionality testing of security equipment and processes. In coordination with security providers, mail managers should:

- Review manufacturer requirements to routinely assess the state of security equipment and processes in their facilities
- Document the dates and frequency of these assessments
- Coordinate with their security provider and facility management to ensure regular testing
- Agencies, in collaboration with mail program managers and security providers, should develop and ensure their training plans account for local procedures countering local threats

Mail screening equipment purchased by departments and agencies should follow manufactures' guidelines for testing and certification requirements.

Additional countermeasures may be implemented as new threats are identified based on external and internal security considerations made by the security provider. Mail staff should remain vigilant and adaptable in the implementation and execution of security countermeasures.

6.0 Documentation

6.1 Mail Security Policy and Plan

As noted in 41 CFR part 102-81: Physical Security, "organizations use risk assessments to evaluate security risk, implement countermeasures, and allocate security resources effectively. Each agency is responsible for implementing, maintaining, and upgrading physical security standards". The best practice for mailroom security policies and plans is to include them as an annex to the FSP. The FSP must be reviewed annually. Mail managers and the security professionals should participate in the annual review to ensure accuracy and viability. Formatting for the plans should be consistent with the agency FSP provided templates. If the agency does not have a template, the ISC's *Facility Security Plan: An Interagency Security Committee Guide* provides an FSP template¹⁸ that may be used. The mail security annex can reference

¹⁸ [ISC Publications | CISA](#)

specific OEP sections for appropriate emergency guidance. The USPS Publication 166, Guide to Mail Center Security¹⁹ provides an additional reference for developing local mail security plans.

A strong plan for mail center security, supplemented with regular training, rehearsals, and reviews, instills a culture that emphasizes the importance of security. Involving all members of the agency mail team (executives, managers, employees, contractors, security managers, building management personnel, union representatives, etc.) during development and throughout the plan is critical to its success.

6.2 Occupant Emergency Plan (OEP)

An occupant emergency is an event that may require evacuation from an occupied space or relocation to a safer area. In the event of an emergency, the mail center manager must protect those who are present and ensure they are evacuated to safety.

The ISC's *Occupant Emergency Programs: An Interagency Security Committee Guide*²⁰ defines an OEP as "a written set of procedures to protect life and property in a facility under specific emergency conditions." Some emergency situations include explosion, discovery of an explosive device, severe weather, earthquakes, chemical or biological exposure or threat, hostage takeover, or physical threat to building occupants or visitors. Effective OEPs reduce the threat of harm 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 Occupant Emergency Organization is a group of employees from the agency or facility who carry out the Occupant Emergency Program. It is comprised of a designated official and other employees assigned responsibilities and to perform specific tasks outlined in their OEP. The designated official is responsible for establishing, developing, applying, and maintaining the plan and is the highest-ranking official in a federal facility. Alternately, the designated official may be another person chosen by tenant agencies. In the absence of a designated official, an alternate may be selected to carry out additional responsibilities. The mail center manager should be actively involved in the development of the OEP.

For additional information refer to CFR 41, Public Contracts and Property Management, Part 102-74, Facility Management, Subpart B, Facility Management, Section 102-74.230 through 260, Occupant Emergency Program, which outlines the details of an Occupant Emergency Program. The designated official and/or FSC can provide access to a facility's OEP and other associated security plans.

6.2.1 Key Elements of the OEP

6.2.1.1 Incorporation of Mail Management Program

As stated in the introduction, mail center personnel should perform an integral role in developing and implementing OEP plans. After the plan is developed, training is an important part of communicating the plan and familiarizing personnel. Additionally, time should be dedicated during every meeting with mail center personnel to discuss emergency preparedness so that it becomes the norm. This section briefly addresses the OEP subject; additional information can be found in the ISC OEP guide mentioned above.

¹⁹ [USPIS Publication 166](#)

²⁰ [ISC Publications | CISA](#)

6.2.1.2 Evacuation Plans

Specific evacuation procedures will vary from site to site and should be captured within the OEP. They must be coordinated in advance with the organization's property or facility managers, along with safety and security personnel. Utilizing and training the procedures identified in the OEP will save lives.

Depending on the circumstances and nature of the emergency, the first important decision is whether to stay put or get away. It is critical to understand and plan for either option. In some circumstances, employees may be instructed to shelter-in-place (SIP). For more information on SIP visit the CDC website. Be sure to specify where mail center staff should gather to enable the supervisor on duty to account for every mail center employee and visitor. They must know the exact route specified.

All suspicious items should be maintained as evidence as part of a criminal investigation until released by the appropriate law enforcement agency. Prior to evacuating, and when conditions allow it, write down information regarding the appearance of the letter or parcel and photograph the item with a digital camera.

6.2.1.3 Emergency Notification

All personnel should know who to contact in case of emergency. A list of all emergency phone numbers should be available to everyone and updated as assignments change. The list should be published with the OEP for the facility and be included in the disaster supply kit.

A daily roster of facility occupants can be maintained to facilitate personnel accountability. This roster can also be passed to public health authorities to coordinate with other cognizant public health jurisdictions as needed based on the employee population.


As part of mail center procedures, a call tree for employees and managers should be established, tested semi-annually, and updated when new personnel arrive/depart. Compilation of this data creates a record of Personally Identifiable Information (PII). The Privacy Act of 1974 prohibits disclosures of PII contained in records and should be stored based on the specifications for either electronic or paper. Minimally, the call tree list should include:

- Names
- Physical addresses
- Email addresses
- Work phone numbers
- Home phone numbers
- Mobile phone numbers
- Names of persons to contact in an emergency

6.3 Communications Plan

Good communication, which is part of any successful mail operation and critical for addressing security issues, involves at least three audiences: management, customers, and mail center personnel.

Relationships between these personnel are key to successful communication. Prepare a list of trusted resources to acquire timely and accurate information (e.g., GSA, USPIS, CDC, National Terrorism Advisory System (NTAS), etc.). Organize protocols for distribution of information on the status of the mail operation. For more information, see the section 6.2 in the Occupant Emergency Plan (OEP) and GSA's National Guidelines for Assessing and Managing Biological Threats in Federal Mail Facilities.



The mail center should develop an internal communications plan to be executed when responding to a threat that includes how to acquire and distribute information.

6.3.1 Communications Best Practices

As discussed in the previous chapter, clear, consistent, and factual communications are critical during any emergency. Past biological attacks (e.g., ricin, anthrax, etc.) demonstrated that inconsistent, vague, and opinionated information negatively impacts the morale and performance of everyone involved in an emergency. Appropriate authorities must be very careful to check facts and maintain familiarity with the appointed spokesperson throughout every aspect of the emergency.

Occupational Safety and Health Administration (OSHA) standards require employers to make health and safety information available to any employee who requests it. However, it is preferable to communicate all relevant information about apparent and credible biological threats to employees as quickly as possible without waiting for a request.

Every federal agency must provide a safe working environment for all employees, including those with special needs. Security procedures should specifically address communications with individuals who may need assistance during an emergency. Care should be taken to be sure all employees are aware of those with special needs. Additional information on emergency preparedness for disabled employees can be found at the National Organization of the Disabled website.²¹

6.3.2 Communications with Management

Schedule regular meetings with representatives of agency senior management (executive secretariat, administrators, etc.), regional offices, and facility. Review the steps you have taken to secure the mail, employees, and facility and address any outstanding issues. It is considered a best practice to include a discussion on the continuity of operations (COOP) for mail handling at an alternate site including a discussion on the status and availability of the mail equipment at the alternate site. Although the procurement of the equipment may be a facility management role, the responsibility is on the mail manager to explain the need for specific equipment.

When familiarizing yourself with your facility security plan, begin with monthly meetings. As events dictate, the frequency may change to quarterly or semi-annually; however, do not allow more than six months to pass between meetings.

²¹ [National Organization on Disability \(nod.org\)](http://nod.org)

6.3.3 Relationship with Partner Organizations

Development and maintenance of relationships with key partners (first responders, public health authorities, FBI, FPS, USPIS, fire, hazmat, and law enforcement officials) is critical to coordinating an effective emergency response. The first task is to establish and maintain relationships with:

- Local first responders to federal mail centers (fire, hazmat, and law enforcement)
- Local public health authorities (disease control and laboratory)
- Regional FBI contacts
- Regional USPIS inspectors
- ISC Regional Advisors

Once the first responders are identified, take the following steps:

- Research and consider local protocols for emergencies
- Determine who will be responsible for opening suspicious letters and parcels (e.g., specially trained federal personnel, first responders) and establish a relationship with them
- Establish relationships and protocols with the internal emergency management office
- Ensure that the first responder organization(s) are ready, willing, and able to follow the established protocols
- Include others such as the security provider, designated official, and FSC in your planning

Many of the above preparedness activities and local government contacts can be initiated through and coordinated with the Local Emergency Planning Committee (LEPC) responsible for the mail center's geographic location. LEPC contact information can be found on the EPA website.²²

Best practice calls for mail managers to contact USPIS and report incidents via the USPIS page²³ or by calling the postal inspectors at 1-877-876-2455 and stating "Emergency". Contact can also be made after the incident is cleared. Reporting is important because USPIS maintains a database on incidents. Contact is usually made by law enforcement, but it is a good idea to follow up.

6.4 Continuity of Operations Plan (COOP)

The COOP ensures continuance of essential federal functions across a wide range of potential emergencies once personnel safety has been addressed. Federal Continuity Directive (FCD) 1²⁴, establishes the framework, requirements, and processes to support the development of continuity programs and defines continuity as the ability to provide uninterrupted services and support, while maintaining organizational viability, before, during, and after an event that disrupts normal operations. Essential functions enable federal agencies to provide vital services, exercise civil authority, maintain the safety and well-being of the general populace, and sustain the industrial/economic base in an emergency.

Because mail remains a critical function for federal programs, the mail manager should be involved in the COOP process. The actual steps included in the COOP to keep incoming and outgoing mail flowing in the event of an emergency depend on the degree to which mail is essential to agency operations.

²² [Finding Your LEPC | US EPA](#)

²³ [Report Mail Fraud & Postal Fraud | USPIS](#)

²⁴ [Federal Continuity Directive 1](#)

6.4.1 Key Elements of a COOP

The following are only some of the recommended elements to be included in a COOP:

- Outline the primary mission essential functions (PMEFs)
- Plan decision process for implementation
- Identify critical assets
- Establish a roster of authorized personnel
- Provide advisories, alerts and COOP activation, and associated instructions
- Provide an easy reference guide for emergency response
- Establish accountability
- Provide for attaining operational capability within 12 hours
- Establish procedures to acquire additional resources for continuity operations in an emergency scenario

6.4.2 Incorporating the Mail Management Program in the COOP

The following are key issues that the COOP should address:

- Should an alternate facility be planned for incoming and/or outgoing mail?
- How quickly should the alternate facility be ready to operate?
- How much of the original operation will be reconstituted in the alternate facility?
- Consider doing a tabletop exercise (TTX) or walk through regarding alternate sites specific to mail processing
- Mail managers should advocate for adequate mail screening equipment at the alternate site (e.g., x-ray, pitching table) and can address this with the security provider or acquisition team if necessary

6.4.3 Objectives of a COOP for a Mail Facility

The following objectives should be considered when conducting COOP planning:

- Reduce loss of life and minimize damage and losses
- Ensure the safety of employees during an emergency
- Ensure the continuous performance of essential functions/operations
- Reduce or mitigate disruptions to operations
- Protect essential facilities, equipment, records, and other assets
- Identify, maintain, and operate alternate locations from which organizations can perform essential functions
- Dedicate the resources required to sustain essential functions
- Facilitate decision-making during an emergency
- Achieve orderly recovery from a wide range of potential emergencies or threats, including acts of nature, accidents, or technological and attack-related emergencies
- Establish a realistic and challenging test, training, and exercise program to verify continuity capabilities

6.4.4 Fly-Away Kits

To be prepared for various types of breaches of security or different types of emergencies, each mail center should have a "fly-away kit." At a minimum, the kit should consist of COOP checklists; key contact

lists; CDs or thumb drives with critical files; any specialized tools that are routinely used; maps to alternate sites; records; and any other information and equipment related to an emergency operation. A “fly-away kit” should contain those items considered essential to supporting contingency operations at an alternate site. Additionally, a duplicate fly-away kit should be located at the backup facility. A key official and one or more alternates should be designated to pick up the kit in an emergency. Further, it is considered a best practice for the fly away kits be inventoried at least semi-annually.

6.5 Annual Review

The policies and plans described in this section should be reviewed annually by a security professional (e.g., agency headquarter security element, USPS, FPS, FBI, or local law enforcement emergency management professionals). The review must be documented, including any edits, updates, or corrections, and be provided to the mail center manager. Individual organizations establish mail manager annual reporting requirements.

7.0 Contracts

Many agencies use contractors to process their mail, either as outsource providers that manage mail centers or as letter shops that consolidate and/or pre-sort outgoing mail. It is important to remember that mail center security remains the responsibility of the agency, even when a contractor handles part of the process. Contracts should specify security procedures that the contractor and contract personnel must follow.

Consider addressing the following as part of the process of contracting for mail services:

- **Process:** The vendor should provide copies of all written procedures on how mail is handled.
- **Timeliness:** Standards should be established to reduce opportunities for mishandling.
- **Security:** The contract should specify steps the vendor will take to provide the best possible security, including hiring practices and employee screening checks.
- **Technology:** Evaluate the technology the vendor will deploy to process the mail and request presentations on electronic manifests for inbound mail, Coding Accuracy Support System (CASS) certification, Intelligent Mail barcode (IMb), National Change of Address, etc.
- **Discount sharing:** When using a presort agency/company to prepare and pre-sort mail, conduct on-site audits to ensure correct billing and appropriate discounts.
- **Scanning/electronic imaging:** Ask for vendor briefings on preparing and storing digital images in conjunction with the agency’s information technology department. The briefing should cover strategies for the long-term storage of electronic documents, retrieval from long-term storage, and how original documents will be prepared and indexed for storage

7.1 Performance-based Service

Develop a performance-based service contract that focuses on three critical elements:

- **A performance work statement:** The performance work statement defines the government's requirements in terms of the objective and measurable outputs and provides detailed information on what, when, where, how many, and how well enabling the vendor to accurately assess resources required and risks involved.
- **A quality assurance plan:** The quality assurance plan gives the government flexibility in measuring performance and serves as a tool to assure consistent and uniform assessment of the contractor's performance. A good quality assurance plan should include a surveillance schedule and clearly state the surveillance methods to be used in monitoring contractor performance.
- **Appropriate incentives:** Incentives should be used when they encourage better quality performance and may be either positive, negative, or a combination of both. They do not need to be present in every performance-based contract. Positive incentives are actions to take if work exceeds the standards. Standards should be challenging, yet reasonably attainable. Negative incentives are actions to take if work does not meet the standards.

More information on performance-based contracting can be found on the GSA website.²⁵

7.2 Reviews

Periodic reviews should be conducted separately from the acquisition process. Tour the shop to ensure procedures are being followed. Confirm that all mail is being processed in a timely manner and all other performance standards are being met.

8.0 Conclusion

Effective safety and security are critical to mail center operations regardless of its size. Though operating as an entry point for federal agencies, mail center security policies and procedures are often overlooked. Mail center personnel must understand their roles as gatekeepers charged with protecting not only the facility, but the personal safety, health, and welfare of the customers they serve.

Avoid underestimating the importance of mail center security with the following steps:

- Know your risks
- Be aware of alternative mail screening technologies
- Analyze workflow
- Know the current tools that help identify suspicious mail and parcels
- Implement contamination reduction strategies
- Train your employees
- Refer to this guide often

²⁵ [Steps to Performance-Based Acquisition \(SPBA\) | BUY.GSA.GOV](#)

Appendix A: Glossary

Accountable Mail – Items that require tracking, signature, or proof of delivery (registered mail, certified mail, FedEx, etc.).

Biological Agent – Bacteria, viruses, fungi, other microorganisms, and their associated toxins. They have the ability to adversely affect human health in a variety of ways, ranging from relatively mild, allergic reactions to serious medical conditions—even death.

Facility Security Committee – A committee that is responsible for addressing facility-specific security issues and approving the implementation of security measures and practices in multi-tenant facilities. The Facility Security Committee (FSC) 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).

Command Center – Emergency operations are directed from a command center. The command center should be centrally located and easily accessible for effective communication and control. The command center should have good communications capability, including at least two telephones and, if possible, portable radios and pagers.

Consequence – (ISC) The level, duration, and nature of the loss resulting from an undesirable event. Extended definition: Effect of an event, incident, or occurrence.

Continuity of Operations Plan (COOP) – A plan designed to ensure continuance of essential federal functions across a wide range of potential emergencies.

Designated Official (DO) – The designated official is the highest-ranking official in a federal facility or may be another person agreed upon by all tenant agencies.

Discount Sharing – A process whereby a vendor discounts similar services provided to multiple clients.

First Responder –The first person (an emergency medical technician or a police officer) who arrives at the scene of a disaster, accident, or life-threatening medical situation. First responders to federal mail facilities may be federal, state, and/or local organizations, depending on the circumstances.

Fly-Away Kit –An emergency supply kit containing items essential to supporting contingency operations at an alternate site. The kit should consist of COOP checklists, key contact lists, diskettes or CDs with critical files, any specialized tools that are routinely used, maps to alternate sites, records, and any other information and equipment related to an emergency operation.

Mail - All materials that pass through a federal mail center, including all incoming and outgoing materials. This includes: first class mail, standard mail, periodicals, package services, and express mail.

Negative Air Pressure –Air pressure in a room is influenced by whether air can enter and leave a room. A negative pressure room primarily keeps its air inside the room with controlled venting.

Occupant Emergency Organization – A group of employees from the agency who carry out the emergency program. It is comprised of a designated official and other employees designated to undertake certain responsibilities and perform specific tasks.

Occupant Emergency Plan (OEP) – A set of procedures to protect life and property under defined emergency conditions. The mail center manager should be actively involved in the occupant emergency program and in development of the OEP.

Paper Jogger – a machine that can vibrate a stack of paper or envelopes to align them for further preparation, such as punching, binding, and cutting.

Parcel – (USPS) Mail that does not meet the mail processing category of letter-size mail or flat-size mail. It is usually enclosed in a mailing container such as a carton.

Performance Work Statement (PWS) –A document that defines the government’s requirements in terms of the objective and measurable outputs. It should provide the vendor with answers to five basic questions: what, when, where, how many, and how well.

Personal Protective Equipment (PPE) – Protective gear used to process mail that may include gloves, aprons, and respirators.

Risk Assessment – The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.

Satellite Locations – Associated subordinate facilities supporting an agency’s mail management program.

Security Policy –A policy developed at headquarters level, with procedures tailored onsite in smaller locations.

Threat – (ISC) The intention and capability of an adversary to initiate an undesirable event.

Vulnerability – (ISC) A weakness in the design or operation of a facility that an adversary can exploit.

Appendix B: Acronyms

ACH	Air Changes per Hour
ASTM	American Society for Testing and Materials
FSC	Facility Security Committee
CASS	Coding Accuracy Support System
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CDC	Centers for Disease Control
CFR	Code of Federal Regulations
COOP	Continuity of Operations Plan
COVID-19	Coronavirus Disease – 2019
DBT	Design-Basis Threat Report
DHL	A German logistics company
DHS	Department of Homeland Security
EDC	Explosive Detection Canine
EO	Executive Order
FAMMA	Federal Agency Mail Management Act
FBI	Federal Bureau of Investigations
FEDEX	Federal Express
FEMA	Federal Emergency Management Agency
FMR	Federal Management Regulations
FPS	Federal Protective Service
FSL	Facility Security Level
FSP	Facility Security Plan
GSA	General Services Administration
HAZMAT	Hazardous Materials
HEPA	High Efficiency Particulate Air (filter)
HSPD-12	Homeland Security Presidential Directive - 12
HVAC	Heating, Ventilation, and Air Conditioning

IED	Improvised Explosive Device
IMb	Intelligent Mail barcode
ISC	Interagency Security Committee
LEPC	Local Emergency Planning Committee
LRN	Laboratory Response Network
NTAS	National Terrorism Advisory System
OEP	Occupant Emergency Plan
OGP	Office of Government-wide Policy
OSHA	Occupational Safety and Health Administration
PCR	Polymerase Chain Reaction
PETN	Pentaerythritol Tetranitrate
PII	Personally Identifiable Information
PMEF	Primary Mission Essential Function
PPE	Personal Protective Equipment
SIP	Shelter in Place
TTX	Tabletop Exercise
UPS	United Parcel Service
USPIS	United States Postal Inspection Service
USPS	United States Postal Service

Appendix C: Online Resources

[Bureau of Alcohol, Tobacco, and Firearms \(ATF\)](#)

[Centers for Disease Control \(CDC\)](#)

[Department of Homeland Security, Biological Attack: The Danger](#)

[DHS Security Assessment](#)

[Federal Bureau of Investigation \(FBI\)](#)

[Federal Emergency Management Agency \(FEMA\)](#)

[Federal Protective Service \(FPS\)](#)

[General Services Administration \(GSA\)](#)

[GSA Mail Communications Policy](#)

[Interagency Security Committee Policies, Standards, and Guidelines](#)

[U.S. Office of Personnel Management](#)

[U.S. Department of Labor \(DOL\), Occupational Safety and Health Administration \(OSHA\) –](#)

[US Postal Service \(USPS\)](#)

[USPS Suspicious Mail Alert Poster](#)

[USPS Postal Inspection Service](#)

[Workplace Risk Pyramid, OSHA](#)

The following publications are available from the US Postal Inspection Service (USPIS):

[Best Practices for Mail Center Security](#)

[USPS Publication 166, Guide to Mail Center Security](#)

[Preventing Mail Fraud Publication 300A](#)

[Identify Theft Brochure Publication 280](#)

[Notice of Reward \(Poster 296\)](#)

[Warning! Reusing Postage \(Poster 5\)](#)

Appendix D: Mail Center Security Checklist

The checklists included in this appendix are intended to assist federal agencies and mail center managers in developing and determining the requirements for security and to aid in determining the security requirements for their mail centers.

Security Assessment		
YES	NO	
		Alternatives for processing mail have been identified in the event of a mail center or building being closed.
		Annual inspections of the mail center are done with building operations and security personnel focusing on potential vulnerabilities.
		A written contingency plan for continuing mail operations has been developed if the mail center or building is closed.
		Important mail has been identified and mechanisms established for its delivery in case of a shutdown.
		Regular safety drills are conducted for mail center staff.
		A written emergency evacuation plan has been developed and employees have been trained on the applicable protocols.
		Precautions have been taken to ensure the safety and well-being of mail center staff.
		Safety/security training for mail center staff is provided on a regular basis.
		Mail/facility managers participate regularly in facility security committee meetings.
		Written procedures are in place to handle suspicious mail.
		Only authorized individuals have access to the mail center.
		Mechanisms are in place to ensure against theft, misuse, or destruction of equipment within the mail center.

Physical Security		
YES	NO	
		The mail center is an enclosed room with defined points of entry or a defined space that is used only for processing mail.
		Access to the mail center is limited to those employees who work in the mail center, or who have immediate need for access.
		Employees always wear photo identification.
		Visitors to the mail center sign a log and are escorted.

Security Training		
YES	NO	
		Basic security procedures have been developed and training has been provided.
		Employees have been trained on how to recognize and handle suspicious parcels/letters.
		Procedures are posted on how to recognize suspicious parcels/letters and staff is trained.
		Employees have been trained on the proper use of personal protection equipment (where applicable).
		Employees are trained on the OEP and regularly tested. Training is regularly provided by the facility mail managers through seminars, conference calls, and/or web-based training.
		Facility mail managers are aware of training available through other sources such as the GSA and the USPS.
		Mail centers rehearse various evacuation plans and/or scenarios.

Occupant Emergency Plan (OEP)		
YES	NO	
		Mail center personnel are familiar with the OEP, and their roles associated with it.
		Procedures are established for handling serious illness, injury, or mechanical entrapment.
		All occupants have been told how to get first aid/CPR quickly.
		Floor plans and occupant information are readily available for use by police, fire, bomb search squads, and other emergency personnel.
		Occupants know what to do if an emergency is announced.
		Evacuation procedures are established, and employees are familiar with the procedures.
		Special procedures have been established for evacuation of the disabled.
		Drills and training have been adequate to ensure a workable emergency plan.
		Emergency telephone numbers are displayed and/or published where they are readily available.
		Emergency numbers are reviewed and updated frequently.
		An advisory committee of appropriate officials (building manager, FPS, security force or security protection official, etc.) assisted in developing the plan for your mail center.

Continuity of Operations Plan (COOP)		
YES	NO	
		An alternate facility has been planned for incoming and/or outgoing mail.
		Employees are aware of a line of succession and delegation of authorities in the event of an emergency.
		Personnel accountability procedures are established for the duration of an emergency.
		Reliable processes and procedures are established to acquire resources necessary to continue essential functions and sustain operations for up to 30 days.
		Documents have been identified and prioritized as critical, important, or routine.
		Standards have been developed and procedures identified that enable your organization to process all critical documents during an emergency. First, plan the steps needed to begin processing the documents and mail designated as important, and then those designated as standard.
		A plan has been developed to work with the USPS and all other carriers as to what to do with the mail for alternate operations.
		A "fly-away kit" has been created for the center, and a key official and one or more alternates designated to pick up the kit in an emergency.

Communications		
YES	NO	
		A communications plan has been developed for use during an emergency.
		The mail manager keeps in contact with facility management through regularly scheduled meetings.
		Regular meetings are held with appropriate agency personnel concerning mail safety and all personnel are advised of outcomes/new procedures.
		Mail center management is involved in developing and implementing security plans.
		A call tree has been established and is continually updated for mail center managers and employees including names, addresses, email, work/home/mobile phone numbers.
		All available information is communicated in a timely manner.
		Everyone is sending the same message.
		All facts have been confirmed with competent authorities.
		Designated officials also have designated backups.
		Local union officials are involved.
		Messages are crafted so that all personnel can easily understand the information.
		Every effort is made to communicate the existing level of risk, and what actions are being taken.

Incoming Mail Procedures		
YES	NO	
		There are written policies and procedures on how incoming mail is processed.
		All mail is X-rayed before it comes into the mail center.
		Incoming mail is isolated in an area where it can be inspected.
		Delivery personnel have limited access to the mail center and are received at a controlled area outside the mail center where possible.
		Letters/parcels for senior agency officials are inspected closely.
		A system is in place for accountable letters and parcels (certified mail, expedited carriers, FedEx, etc.). Delivery is verified and only complete shipments are accepted.
		Accountable mail is signed for whenever possession changes and is never left at an unoccupied desk or mailbox.
		Incoming personal mail is not handled by the mail center unless an exemption for your agency applies.

Mail Center Opening Procedures		
YES	NO	
		A check of all locks/entrances.
		Start visitor log.
		Verify safe/vault contents.
		Take meter readings for manual backup records
		Deactivate all relevant electronic security systems

Mail Center Closing Procedures		
YES	NO	
		Close meter readings.
		Secure meters.
		File the visitor log.
		Secure all mail.
		Secure all safes/vaults.
		Check all locks/entrances.
		Execute daily cleaning procedures.
		Activate all relevant electronic security systems

Mail Transportation		
YES	NO	
		Authorized receptacles for mail are clearly labeled.
		High-value items are secured overnight.
		Labels are securely fastened to mail items.
		Labels and cartons do not identify valuable contents.
		Containers and sacks are used when possible.
		Outgoing mail is sealed shortly after the most valuable item is placed inside.
		Sender or addressee can identify the value of the contents.
		Lost and rifled mail is reported to the USPS.
		Parcels are prepared to withstand transit.
		Contract delivery services are screened.
		Outgoing mail is delivered to postal custody inside the facility.
		Unnecessary stops by delivery vehicles are eliminated.
		X-raying of mail occurs where appropriate.
		Employee parking is separated from the loading dock area (where possible).
		Contract delivery services are screened and/or X-rayed (when available)
		Unnecessary stops by delivery vehicles are eliminated.
		Procedures are established for handling unexplained parcels.

Employee Safety		
YES	NO	
		Personal protection equipment is available for all mail center personnel and employees who have been trained on the proper use of equipment and safety gear; training is documented.
		Signs are posted in the mail center listing whom to call in the event of emergencies such as fire, theft, suspicious parcels, etc.
		Daily procedures have been established for cleaning the area and equipment used to process inbound mail.
		Staff is instructed to wash hands frequently, especially before eating.
		Employees are instructed to make supervisors aware of unknown persons in the mail center.
		Evacuation procedures are established, and staff routinely trained in the event of a potential threat. Practice, train, and rehearse!
		Provide a separate and secure area for personal items (coats, and purses).

Loss Prevention & Cost Avoidance		
YES	NO	
		A check-and-balance system is in place to validate procedures for all forms of postage – meters, stamps, and permits.
		Regular checks are conducted to ensure employees are not using agency meters for personal mail.
		Controls are in place to ensure proper access and accountability for permit envelopes and labels.
		Regular inventory counts are logged properly.
		Regular audits are performed for inventory.
		Bills from other carriers (FedEx, UPS) are reviewed regularly to guard against unauthorized use and to ensure that appropriate refunds are collected.
		Personnel are screened before employment (if appropriate, background checks could be performed).
		Only authorized employees are assigned to accept mail.
		The designed physical layout of your mail center serves as a tool in helping to prevent loss.
		Call the USPIS to report mail losses. Refer to their website for more information: http://www.usps.com/postalinspectors .

Contractors		
YES	NO	
		The contractor should provide copies of all written procedures on how mail is handled.
		Develop a performance work statement that defines the federal mail center requirements in terms of the objective and measurable outputs.
		Identify security steps the contractor will take to provide the best possible security, including hiring practices and employee screening checks.
		Evaluate what technology the contractor will use to process your mail. Request presentations on electronic systems that may be used.
		Conduct on-site audits to ensure that you are being charged correctly and receiving the appropriate discounts if you are using a contract service to prepare and presort your mail.
		Conduct periodic reviews separate from the contract process.
		Do an impromptu tour to see that the procedures are being followed. Confirm that the mail is being processed, and that performance standards are being met.

Appendix E: Mail Center Screening Requirements and Best Practices

Determining the proper mail screening approach requires a combined evaluation that includes the overall level of risk, the mail center classification, the current mail processes assessment, and any additional factors that security and management personnel deem significant.

Table F1 below provides a way to integrate and evaluate all these factors. The mail screening requirements rating provides an indication of the minimum recommended mail screening facility and technology approaches for a particular organization and mail center location.

Facility Type	Visual Screening	Dangerous Contraband	Hoax Screening	Explosive Screening	Chemical Screening	Biological Screening	Rad/Nuc Screening	Content Screening
S	X	X	X					
M	X	X	X	X				
L	X	X	X	X	X	X	X	X

Table F1 Mail Screening Requirements by Facility Type

The following checklists provide a starting point for mail center managers and organization security personnel to begin to build out their own mail screening operation. It is a baseline set of screening processes founded on best practices currently in use in government and commercial facilities around the world. Specific or unique situations may require significant upgrades to the recommended processes, or they may permit reductions in the level of screening recommended for a site, based on its risk rating and its mail center classification.

Facility Design	Best Practices	Minimum Recommendations
Location	<p>Mail center located in an offsite facility outside the main, primary office or campus location.</p> <p>Offsite facility is not located in a high-traffic or high-visibility area.</p>	<p>Mail center located in a facility or specific area controlled by the organization.</p> <p>Mail center is in a designated room away from the primary office activities.</p>

Facility Design	Best Practices	Minimum Recommendations
Security	<p>Mail center has a separate CCTV security system that is monitored 24/7.</p> <p>Facility is enclosed by security fence.</p> <p>Access to secure area is monitored by a guard.</p> <p>The visitor control system issues temporary badges that include a picture.</p>	<p>Mail center itself has a separate access control system.</p> <p>Only mail center personnel are allowed access to the mail screening and handling areas.</p>
Loading Dock	<p>Access to loading dock is restricted to mail center personnel and approved delivery vehicles.</p> <p>Loading dock has inbound and outbound doors separated by a sufficient distance to avoid cross contamination.</p>	<p>Access to loading dock is restricted to individuals and vehicles inside the campus or building security perimeter.</p> <p>Access to loading dock can be closed or restricted when not in use.</p>
Biological Contamination	<p>Mail center has a negative pressure system that begins at the loading dock and includes dedicated screening and temporary quarantine areas.</p> <p>The negative pressure mail center has a separate HVAC system.</p>	<p>Mail center personnel can shut off flow to the HVAC system supporting the mail center.</p> <p>Access to mail center does not require personnel to carry unscreened items through core office areas.</p>

Tracking and Accountability	Best Practices	Minimum Recommendations
USPS Mail	<p>Inbound mail is tracked throughout the initial screening process at the tub or tray level using internally-generated barcodes.</p>	<p>Inbound mail is tracked, processed, segregated, and delivered daily.</p>

Tracking and Accountability	Best Practices	Minimum Recommendations
USPS Parcels	<p>All parcels are barcoded and tracked from receipt, throughout the screening process, and until delivered to the recipient or a designated representative.</p> <p>Undeliverable parcels are secured in the mail center in a separate area until delivery can be made.</p>	<p>All parcels are barcoded and tracked from receipt, throughout the screening process, and until delivered to the recipient or a designated representative.</p> <p>Undeliverable parcels are secured in the mail center in a separate area until delivery can be made.</p>
Express Couriers	<p>All parcels are tracked using the dedicated courier tracking number/barcode from receipt, throughout the screening process, and until delivered to the recipient or a designated representative.</p> <p>Undeliverable parcels are secured in the mail center in a separate area until delivery can be made.</p> <p>All items are screened using an X-ray scanner at an offsite facility.</p>	<p>All parcels are tracked using the dedicated courier tracking number/barcode from receipt, throughout the screening process, and until delivered to the recipient or a designated representative.</p> <p>Undeliverable parcels are secured in the mail center in a separate area until delivery can be made.</p>
Supplies and other items	<p>Mail center personnel must confirm all items against the delivery manifest.</p> <p>Items must be entered into the tracking and/or procurement system.</p> <p>All items must be screened and stored in a secure facility until delivered or consumed.</p>	<p>Mail center personnel must confirm all items against the delivery manifest.</p> <p>Items must be entered into the tracking and/or procurement system.</p> <p>All items must be screened and stored in a secure facility until delivered or consumed.</p>

Screening Equipment and Processes	Best Practices	Minimum Recommendations
<p align="center">Chemical</p>	<p>Mail center has an air sampling system with automatic alert capability.</p> <p>Sensors are located at the loading dock and inside mail screening facilities.</p> <p>Chemical sensor system is monitored by the mail center security operations.</p>	<p>Mail center personnel visibly inspect mail and parcels for the presence of liquids.</p> <p>Mail and parcels with obvious contaminants are set aside for further inspection by security or HAZMAT personnel.</p>
<p align="center">Biological</p>	<p>Mail and parcels are screened inside a negative pressure environment.</p> <p>Items are visually inspected for signs they may contain a biological hazard.</p> <p>Air samples are collected from the outside and inside of all mail and parcels.</p> <p>Samples are collected from mail tubs and trays.</p> <p>Collection device filters are tested for biological hazards by a CDC-approved laboratory.</p> <p>Mail and parcels are quarantined until negative test results are obtained.</p>	<p>Items are visually inspected for signs they may contain a biological hazard.</p> <p>Suspicious items are segregated until released by mail center supervisors, security personnel, or first responders.</p> <p>No mail is released for delivery until suspicious mail has been cleared.</p>

Screening Equipment and Processes	Best Practices	Minimum Recommendations
Radiological/Nuclear	<p>Inbound delivery vehicles are screened for radiation using pedestal or wall mounted sensors.</p> <p>Radiation sensors are integrated into the central security system and monitored 24/7.</p> <p>Mail center personnel wear radiation pagers while screening and processing mail.</p> <p>If radiation is detected in an item, mail center personnel leave the immediate area.</p>	<p>Mail center personnel visually screen items for signs that a radiation producing device is enclosed.</p> <p>Mail center personnel wear radiation pagers while screening and processing mail.</p>
Explosives	<p>Vehicles and mail/parcels are screened by explosive detection canine teams before being allowed inside the screening facility.</p> <p>Items are visually inspected for signs they may contain an explosive device.</p> <p>Mail is screened at the batch level (tubs or trays) using an X-ray scanner.</p> <p>Parcels are screened individually with an X-ray scanner.</p> <p>Mail center personnel conducting scanning operations are networked with remote security personnel for technical support as necessary.</p> <p>Suspicious items are segregated until released by mail center supervisors, security personnel, or first responders.</p>	<p>Mail center personnel visually screen items for signs that an explosive device is enclosed.</p> <p>Suspicious items are segregated until released by mail center supervisors, security personnel, or first responders.</p>

Screening Equipment and Processes	Best Practices	Minimum Recommendations
<p>Contraband and Dangerous Items</p>	<p>Items are visually inspected for signs they may contain dangerous or contraband items.</p> <p>Mail is screened at the batch level (tubs or trays) using an X-ray scanner.</p> <p>Parcels are screened individually with an X-ray scanner.</p> <p>Mail center personnel conducting scanning operations are networked with remote security personnel for technical support as necessary.</p> <p>Suspicious items are segregated until released by mail center supervisors, security personnel, or first responders.</p>	<p>Mail center personnel visually screen items for signs that they may contain dangerous or contraband items.</p> <p>Suspicious items are segregated until released by mail center supervisors, security personnel, or first responders.</p>

Personal Protective Equipment (PPE)	Best Practices	Minimum Recommendations
<p>Clothing</p>	<p>PPE includes a Tyvek outer garment, hood, gloves, boots, and a minimum N95 respirator (FFP Mask).</p> <p>A smock may be substituted for a Tyvek suit for individuals not involved in biohazard screening.</p>	<p>PPE includes wear of smock, gloves, and N95 mask (FFP Mask).</p> <p>PPE is made available to all personnel.</p>
<p>Wear</p>	<p>Mail screeners dress in PPE prior to entering the screening facility and remove it before leaving the negative pressure environment.</p>	<p>Smocks are left in the mail center when not in use.</p> <p>If worn, gloves and masks are donned prior to screening and sorting mail.</p>
<p>Disposal</p>	<p>PPE is enclosed in sealed bags and remains in the negative pressure environment until the daily mail has tested clean.</p> <p>PPE is disposed of daily.</p>	<p>Smocks are left in the mail center when not in use.</p> <p>Other PPE items are disposed of daily.</p>

Suspicious Mail Incident Response	Best Practices	Minimum Recommendations
Incident Response Plan	<p>Mail center has a formal emergency response plan.</p> <p>Response plan is reviewed and updated at least quarterly.</p> <p>Copies of the response plan are maintained by the mail center, security personnel, local managers, and when appropriate, first responders and public health officials.</p>	<p>Mail center has a formal emergency response plan.</p> <p>Response plan is reviewed and updated at least quarterly.</p> <p>Copies of the response plan are maintained by the mail center, security personnel, local managers, and when appropriate, first responders and public health officials.</p>

Training	Best Practices	Minimum Recommendations
Suspicious Mail and Parcel Characteristics	<p>All mail center personnel have received initial training on identification and handling of suspicious mail and parcels prior to beginning work at the mail center.</p> <p>All mail center personnel have received annual training on identifying suspicious items.</p>	<p>All mail center personnel have received initial training on identification and handling of suspicious mail and parcels prior to beginning work at the mail center.</p> <p>All mail center personnel have received annual training on identifying suspicious mail and parcels.</p>
Screening Technology and Procedures	<p>Mail center personnel have received initial training on specialized mail screening equipment from the vendor.</p> <p>Mail center personnel have received annual training from the vendor or local supervisors.</p>	<p>Mail center personnel have received initial training on specialized mail screening equipment from the vendor.</p> <p>Mail center personnel have received annual training from the vendor or local supervisors.</p>

Training	Best Practices	Minimum Recommendations
<p>Incident Response</p>	<p>Mail center personnel have received, read, and been briefed on the emergency response plan.</p> <p>Mail center personnel and related organizations have conducted a tabletop exercise of the emergency response plan.</p> <p>Mail center personnel and related internal organizations have completed a live exercise of the emergency response plan.</p> <p>Local first responders and, as appropriate, public health officials have conducted a site visit of the mail center location and reviewed emergency response procedures.</p>	<p>Mail center personnel have received, read, and been briefed on the emergency response plan.</p> <p>Mail center personnel and related organizations to include public health officials have conducted a tabletop exercise of the emergency response plan.</p>

Acknowledgements

The following organizations participated in, contributed to, and/or were instrumental in the update of this document:

- General Services Administration
- Interagency Security Committee, Department of Homeland Security
- Department of Veterans Affairs
- Department of Homeland Security
- Department of Transportation
- Department of Treasury
- Department of Labor
- National Credit Union Administration
- Internal Revenue Service
- Federal Law Enforcement Training Center, Department of Homeland Security
- Central Intelligence Agency
- United States Postal Inspection Service