U.S. General Services Administration

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

Mail Center Security Guide

Fourth Edition - 2014

Acknowledgement

General Services Administration wishes to thank the following team members who helped make this guide possible. They include Mr. Romerio Moreno, United States Department of Agriculture, Mr. Alvan T. Majors, United States Department of Energy, Mr. Derrick Miliner, United States General Services Administration, Ms. Linda Willoughby, United States General Services Administration, Mr. Trent Keffer, United States Department of Defense, Mr. Ronald G. Boatwright, United States Department Homeland Security, and Ms. Karen Sage, Peace Corps.

Table of Contents

Abbreviations Used

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
DMM	Domestic Mail Manual, U.S. Postal Service
EAP	Employee Assistance Program
EMS	Emergency Medical Service
FEMA	Federal Emergency Management Agency
FMEC	Federal Mail Executive Council
FMR	Federal Management Regulations
FPS	Federal Protective Service
FSC	Facility Security Committee
GSA	General Services Administration
HEPA	High Efficiency Particulate Air (filter)
IMPC	Interagency Mail Policy Council
LEPC	Local Emergency Planning Committee
LESO	Law Enforcement Security Officer
NTAS	National Terrorism Advisory System
OCA	Office of the Chief Architect
OEP	Occupant Emergency Plan
OGP	Office of Government-wide Policy
OPM	U.S. Office of Personnel Management
OSHA	Occupational Safety and Health Administration
PMEF	Primary Mission Essential Function
PPE	Personal Protective Equipment
SERC	State Emergency Response Commission
SIP	Shelter in Place
USC	United States Code
USPIS	United States Postal Inspection Service
USPS	United States Postal Service

Throughtout this Guide, "you" refers to the mail center manager and "we" refers to GSA.

1 Introduction

The First Edition of this Mail Center Security Guide was published in December 2001, the Second Edition in October 2002, and the Third Edition in February 2004. This Fourth Edition of the Mail Center Security Guide incorporates new information that has become available, as this nation's understanding of homeland security has evolved. Additions to this edition include updated initial alert procedures, securing mail at an alternative work location, acronyms, and editorial changes.

General Services Administration (GSA) established the Office of Government-wide Policy (OGP) in 1995 with Mail Management as one of its federal policy areas. Mail Management Policy is governed by 44 U.S.C. Chapter 29 – Records Management by the Archivist of the United States and by the Administrator of General Services. Processing of mail by a federal agency is defined under records maintenance and use in 44 U.S.C. 2901. This section defines the term "records management", "records creation", "records maintenance and use", and "records disposition". 44 U.S.C. 2904 identifies the responsibilities of the Administrator of General Services to include promulgating standards, procedures, and guidelines with respect to records management and the conduct of records management studies.

The OGP Mail Policy established quarterly Interagency Mail Policy Council (IMPC) meetings, the Federal Mail Executive Council (FMEC) meetings, and a website (www.GSA.gov/mailpolicy) with training resources and other information, including mail center security, which is a significant part of the on-going training.

Mail center security became much more important after the anthrax attacks of October 2001 and the continuing threat of such attacks. Mail center managers provide security and training to meet a wide range of potential threats that can be introduced into an organization by way of the mail center. Threats that may involve chemical, biological, radiological, nuclear, or explosive substances (CBRNE) are both dangerous and disruptive.

This guide also addresses preventing theft in the mail center, emergency planning, and comprehensive security management.

In addition to this guide we have published several documents on specific security topics. In December 2003, we published the "National Guidelines for Assessing and Managing Biological Threats in Federal Mail Facilities."

1.1. Purpose of the Guide

There is no single set of "orders" or "best practices" that is applicable to all mail centers. There are several factors that help determine both the type of mail screening facility that is required and the range of screening procedures that should be implemented by the mail center manager.

This guide's purpose is to assist federal mail center managers in keeping mail centers safe and secure. It provides an outline of the planning and preparation that is appropriate for a federal mail center. It encourages you to communicate with others in the planning process by making you more familiar with their process. In particular, this guide offers:

- Elements of a mail center security plan;
- Descriptions and discussion of those elements;
- Tips for operations, training, and communications;
- A list of on-line resources; and
- A security checklist.

The mail center security plan has many objectives, including:

- Protecting staff and all other employees and building occupants;
- Avoiding unwarranted, costly and disruptive evacuations;
- Providing a visible mail screening operation that demonstrates to all employees that management is committed to their safety;
- Supporting employee morale and reducing stress by providing reassurance to all employees about the safety of mail; and
- Minimizing the likelihood of litigation.

A strong plan for mail center security, supplemented with regular training, rehearsals, and reviews, helps instill 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, and union representatives – during development and throughout is critical to the security plan's success.

1.2. A Note for Smaller Federal Facilities

Many federal agencies have satellite facilities where mail operations are performed in a small room, one corner of a room, or one corner of a desk. In these facilities, responsibility for processing mail is divided among professional and support staff. Security plans for small facilities are, of course, limited by both the size of the facility and the resources available to develop and implement plans. Small facilities will, therefore, adopt those recommendations from this guide that are appropriate to them. Nonetheless, every federal facility should have a security plan that considers each of the elements listed in Figure 1. For the most part, security policy should be developed at a headquarters level, with procedures tailored to the smaller location developed and implemented on site. Your threats and vulnerabilities will determine the measures to protect your facility.

1.3. What Should a Mail Center Security Plan Include?

A complete mail center security plan includes the elements listed in Figure 1, and every federal mail center manager should make sure that all of these are included. Refer to the FMR §102-192.80, and Appendix D in this guide.

The mail center manager will not be required to prepare all of these plans. They should participate actively in the development and implementation of each of these elements, but other parts of the agency or outside security experts should have the lead on most of them. The mail center manager must ensure that they have addressed each of these elements.

Figure 1. **Critical Elements of a Mail Center Security Plan**

1. Risk Assessment
2. Staff Protection Plan
3. Operating Procedures
4. Visible Mail Screening Plan
5. Mail Center Personnel Training
6. Training, Testing, and Rehearsal Plan
7. Managing Threats
8. Communications Plan
9. Occupant Emergency Plan (OEP)
10. Continuity of Operations Plan (COOP)
11. Annual Reviews

2 Risk Assessment

Organizations receive mail and packages from a wide variety of sources every day. Some of these sources (USPS, major express couriers), have extensive security, screening, and control processes embedded in their day-to-day operations. Many others deliver items that are from "trusted vendors" or other sources that limit the potential risk they pose to the intended recipient or other individuals within an organization.

Unfortunately, even the best procedures and control measures do not completely eliminate risk. Therefore, it is important to implement mail center procedures that provide a second line of screening and the ability to track mail and packages from receipt to delivery.

The first step in developing a security program is a site-specific risk assessment for your mail center and its operation, in coordination with your agency and bureau or department.

The objective of a risk assessment is to determine the likelihood that identifiable threats will harm a federal agency or its mission.

Each site has different threats and risk levels, and this will lead to different security measures for each site.

A thorough understanding of the risk assessment process will allow you to be better prepared to meet potential threats and eliminate or mitigate consequences. A risk assessment incorporates the entire process of asset and mission identification, threat assessment, vulnerability assessment, impact assessment, and risk analysis.

All decisions about mail center security must be supported by the risk assessment.

Make sure the risk assessment is documented!

2.1. Components of a Risk Assessment with Definitions of Terms

Asset and Mission Identification: Identification of the agency assets and missions that might be damaged by threats that could come through the mail center.

Threat Assessment: Identification of potential threats to the mail center, including natural events, criminal acts, accidents, and acts of terrorism. Each threat should be evaluated for the likelihood or probability that it may occur.

Vulnerability Assessment: Analysis of the extent to which the mail center is vulnerable to each of the potential threats identified in the threat assessment.

Impact Assessment: Determination of the impact on the mail center, the facility, and/or the agency if a specific asset were damaged or destroyed, or if a specific mission were impaired or temporarily halted (commonly referred to as "Consequence").

Risk Analysis: Quantification of the likelihood and extent of possible damage from each identified threat to the mail center, other agency assets, and agency missions. Analysis is based on the risk, impact, threat and vulnerability assessments. Figure 4 may help you to identify and rate your risk.

Risk Assessment: The entire process, consisting of asset and mission identification, threat assessment, vulnerability assessment, impact assessment, and risk analysis.

The resources we consulted in developing this section use terms in different ways. Even the term for the overall process differs – we have chosen to call it "risk assessment." Others might call it a security assessment or security scan. We are using a generally accepted model to make the subject of risk assessment for a mail center as simple as possible to understand and implement. It will help guide mail managers to review risk assessments for thoroughness.

2.2. Conducting a Risk Assessment

As mail center manager, you should be an active participant in the risk assessment. However, appropriately trained and experienced security personnel should have the lead in conducting your risk assessment. Depending on the situation, your risk assessment should be led by:

- Your building security office
- Base security
- Individual agency security service
- Professional security consultants
- United States Postal Inspection Service (USPIS)

Four primary resources were used to develop the Risk Assessment section of this guide. The second and third items on this list are copyrighted and are used here by permission.

They are:

- ***Risk Management: An Essential Guide to Protecting Critical Assets***, National Infrastructure Protection Center, Washington DC, November 2002.
- ***Threat/Vulnerability Assessments and Risk Analysis***, Nancy A. Renfroe and Joseph L. Smith, Applied Research Associates, Inc., March 2002.
- ***Anti Terrorism: Criteria, Tools & Technology***, Applied Research Associates, Inc., Updated February 19, 2003.

- ***Best Practices for Mail Screening and Handling***, U.S. Department of Homeland Security, September 1, 2012.

Additional resources that you may wish to consult include:

- Federal Emergency Management Agency (FEMA is the lead federal agency for consequence management) http://www.fema.gov

  Workplace Risk Pyramid, OSHA https://www.osha.gov/dep/anthrax/matrix/index.html
- Vulnerability Assessment of Federal Facilities, published by the US Department of Justice, June 28, 1995. www.usaid.gov/policy/ads/500/565A1
- Mail Center Security, USPIS. http://about.usps.com/publications/pub166.pdf
- Federal Protective Service website: http://www.dhs.gov/federal-protective-service

2.3. Asset and Mission Identification – What are you trying to protect?

The first step in a risk assessment is identifying the assets and missions that must be protected. During the asset identification step, the security specialist, with the assistance of the asset owner, identifies and focuses on those assets important to the mission or operation. By identifying and prioritizing these assets, you take the first step toward focusing resources on what is most important. Assets can be tangible (e.g., people, facilities, equipment) or intangible (e.g., information, processes, and reputations). Obvious mail center assets include personnel, postage meters and other equipment, computers, accountable mail, high-value shipments, the safe or vault and its contents, stamps, and the mail delivery roster. Your mail center probably has most of these, and others.

Since the mail center is a vulnerable point of entry for threats, your risk assessment must also identify the assets and missions of your customers, that is, the people to whom you deliver mail. Any deliberate attack may not be directed at your mail center. Rather, it may be directed at your customers and their missions.

Figure 2. **Questions Addressed by Risk Assessment**

1. What assets and missions are we trying to protect?
2. What credible threats and other dangers could arrive in the mail center? (natural, criminal, accidental, and terrorist)?
3. What is the relative likelihood of occurrence for each of those threats?
4. How vulnerable is the mail center to each of those threats?
5. How much damage might each of those threats cause, given what is known about missions, assets, threats, and vulnerability?
6. What should be done to protect the mail center, its employees, other agency personnel, and the agency's missions?
7. How much security is enough?
8. What assumptions must I make?

2.4. Threat Assessment – What bad things could happen?

The second step in the risk assessment is determination of potential threats. The threat assessment looks at the full spectrum of threats – natural, criminal, accidental, or terrorist – for a given location. The assessment should examine supporting information to evaluate the likelihood of occurrence for each threat.

The security analyst should identify the specific threats that might be faced in your mail center or your facility. It should be determined how threats might enter the mail center, and the likelihood of each threat. In making these estimates, the analyst must rely on data and information obtained from research and interviews, not intuition.

- For natural threats, you should look at historical data that shows the frequency of occurrence for tornadoes, hurricanes, floods, fires, and earthquakes in your area.
- For criminal threats, look at local crime rates and consider whether your customers' assets and missions make you or them more attractive to criminals.
- For accidents, look at the layout and machinery in your mail center, and also consider your building's mechanical equipment, especially plumbing. Also look at your historical accident rate (you should keep accessible, long-term records of accidents).
- For terrorist threats, look at the missions performed by your customers and the visibility of federal executives located in the facilities that you serve. Although routinely associated with foreign terrorism, in today's environment it could be domestic or a lone-wolf adversary.

Significant threats to a federal mail center include:

- Foreign terrorism – Agencies with high public visibility or international missions have a greater risk of being targeted by foreign terrorists. Also, agencies located in proximity to significant targets may be victims of collateral damage.
- Domestic hate groups – Some citizens are actively involved with anti-government and hate groups, and have adopted tactics similar to foreign terrorists.
- Disgruntled employees/workplace violence – Reorganizations, layoffs, and terminations may lead to theft, sabotage, or violence. Additional steps should be taken to protect individual employees who are being harassed, stalked, or threatened inside or outside the workplace.
- Accidents – Prepare for workplace accidents, vehicle accidents, floods from major plumbing leaks, and building fires.
- Acts of nature – Wildfires, floods, severe weather, or earthquakes

One very important part of this step is simply looking at your mail stream. Certain agencies, such as the Federal Bureau of Investigation (FBI), receive threatening mail almost daily. Other agencies seldom see a threatening mail piece despite careful, routine inspection.

A threat may be introduced by anyone who sends anything through the mail with the intent to frighten, disrupt, injure, etc. It could be an animal rights activist or environmental radical, pro-rights or pro-life extremist, disgruntled employee, angry spouse, or simply a disappointed citizen.

Remember: you don't have to be a target in order to become a victim.

Key questions that must be answered in a threat assessment are:

- How visible is your agency, your facility, and any executives who work in your facility?
- What extent does their visibility make it more or less likely that a criminal or terrorist might select your facility for an attack?

Some federal agencies are, of course, highly visible, but many federal agencies and facilities are relatively unknown to the general public and are, therefore, at much less risk.

2.5. Vulnerability Assessment – What are your strengths/weaknesses?

Vulnerability is the organization's assessment of the strengths and weaknesses of their operations and the physical characteristics of their mail center with respect to the known and projected threats. In this step, the security analyst looks for exploitable situations created by inappropriate design, inadequate equipment, or deficient security procedures. Examples of typical vulnerabilities (which you might also call points of weakness) in a mail center may include:

- Poor access controls
- Lack of X-ray equipment
- Inadequate security training or rehearsal
- Lack of stringent service contract management
- Unscreened visitors in secure areas

2.6. Impact Assessment – What would happen if your security measures failed?

Once you have identified each significant asset and mission, the fourth step in the risk assessment is to determine what the impact or consequence would be if that asset were lost, damaged, or destroyed. Consider what would happen if your agency were temporarily prevented from performing that mission, or if its ability to perform it were significantly impaired. The overall value of the asset or mission is based upon the severity of this effect.

For example, what would be the impact on your agency's mission if your mail center were closed for several days due to flooding?

What if an improvised explosive (that is, a bomb) passed through the mail center without being identified, reached its intended target in your facility, and detonated? What would be the consequences for the facility and the people who work there – the intended victim and everyone else?

2.7. Risk Analysis – What does it all add up to?

The final step in the risk assessment process is to combine the four previous steps, that is, to evaluate, for each asset and each mission, how the impact, threat, and vulnerability assessments interact. The product is a statement of the level of risk for each asset and each mission.

A worksheet such as the example in Appendix D makes it much easier to make this evaluation, by aligning all of the information into a readable and easily understood format.

The terms used in the sample worksheet (high, medium, low) are subjective and difficult to combine. Depending on the audience for the risk assessment, the security analyst may choose terms such as these, or may choose a 1 to 10 numerical scale.

A simple equation provides the underpinnings for rating risks:

Risk = Threat + Vulnerability + Consequence

Figure 3. **Sample Questions to Ask as Part of Your Risk Assessment**

1. What is your agency protecting?
2. How much would this loss cost your agency in time, lost productivity or business? What is the key function your mail center needs to restore/preserve under a disaster recover scenario?
3. Does your agency deal internationally, have foreign affairs officers or suppliers? Has it been the primary focus of a recent crisis or other public interest?
4. Who are your adversaries?
5. Is your agency doing business where there is political/religious unrest?
6. Has your agency undergone recent downsizing, reduction in force, or hiring freezes?
7. Has anyone in your agency received an threat recently?
8. Is your agency involved in research, products, or services of public controversy?
9. What can you do to ensure that your vulnerabilities are limited and counter-measures are applied?

Figure 3 above offers a few questions that fit many federal mail centers.

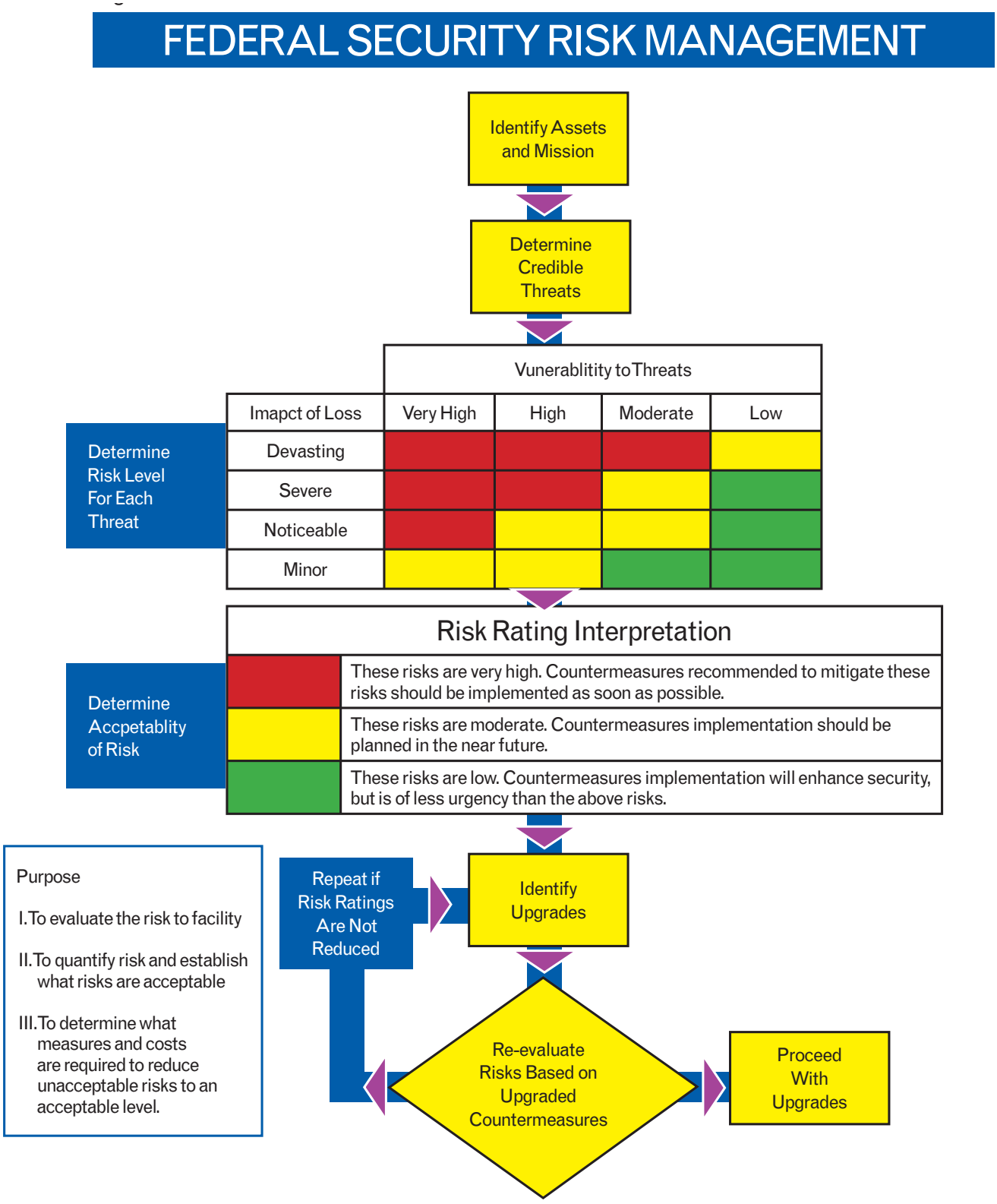
The remainder of this Mail Center Security Guide provides guidance on counter-measures, that is, on the things that the mail center manager, security professional, and agency executives can do to protect the assets identified in the risk assessment.

You need to recognize that most risks cannot be eliminated.

You also need to recognize that you can reduce risk dramatically by preparation, planning, training, rehearsal, and continuous review. A risk assessment is a snapshot in time and needs to be updated whenever there are significant changes in operations, the organization, or external conditions.

2.8. Federal Security Risk Management Chart

Figure 4 is provided with the permission of the authors at Applied Research Associates, Inc.



3 Mail Center Operating Procedures – Creating a Safe and Secure Environment

Most of the effort in developing a risk assessment should be accomplished by security professionals. However, mail center operating procedures must be developed locally. Though higher levels in the federal agency will develop the policy, these procedures are based on work processes at the local level. Please remember that all decisions about mail center operating procedures, as well as every other aspect of mail center security, must be based on the risk assessment.

3.1. Incoming Mail Procedures

To identify and catch problems before they occur, it is advisable to acquire an X-ray machine to scan mail. If mail volume is too low to justify acquiring an X-ray machine, consider partnering with another organization. All mail, regardless of carrier, should be X-rayed – be sure to include couriers and small package carriers.

Once the mail has been X-rayed, inspect the mail for suspicious characteristics. If possible, do this in an area isolated from the rest of the mail center. Refer to "Training,Testing, and Rehearsal" in Section 4 of this guide for information on inspecting incoming mail, and "Physical Security in a Mail Center/Facility," Section 3.6, for information on isolating the incoming mail processing area. Mark all packages with a stamp that says "X-rayed" to acknowledge that it has been screened if at all possible. Depending on the agency function, you may consider canine dogs to sniff mail centers.

Limit access for anyone who delivers mail to your center. Conduct mail transactions at a counter.

Place incoming mail in clearly labeled, authorized receptacles for U.S. Mail.

Make employees aware of established procedures for handling unexplained or suspicious packages, and reinforce training with posted instructions.

Make Personal Protection Equipment (PPE), including gloves and masks, available for all employees.

Require employees to wear photo identification at all times.

Instruct employees to challenge any unknown person in the facility.

3.2. Deliveries for Senior Executives

Give extra care and attention to letters and packages addressed to any senior officials whose names and/or positions give them higher public visibility. Meet with representatives from senior management (senior executives, executive secretariat, administrators, etc.) to establish procedures for mail and packages addressed to senior officials. A best practice is to mark all packages and envelopes addressed to senior officials with "Inspected by Mail Services" after you have screened them. No letters or packages should be accepted at the executive area unless clearly stamped. This procedure should be used for both internal and external deliveries.

3.3. Handling Accountable Mail

Establish a closed-loop manifest system for all accountable letters and packages (e.g., Certified Mail, UPS, and FedEx). A closed-loop system means that someone signs for each piece of accountable mail whenever possession changes. For example, the receiving clerk should require internal couriers to sign for all packages that they deliver. Always require a signature for accountable mail at the final point of delivery. Don't leave any accountable mail at an unoccupied desk or mailbox. Have someone else in the department sign for the piece, or leave a note with directions to pick up the piece at the mail center. Retain copies of all accountable mail manifests for at least two (2) years.

Verify the delivery manifest sheet to ensure that you have received all packages listed. Accept complete shipments only.

If possible, install an electronic manifest system to speed up the process and increase accuracy. An electronic system also makes it easier to conduct research on past deliveries.

3.4. Personal Mail

In most circumstances, agency- and/or facility-level policy should prohibit handling incoming or outgoing personal mail in a federal mail center. The federal regulation on mail management, 41 CFR, 102-192.125(i), authorizes agencies to adopt this policy, but it also authorizes federal mail managers, at the facility level, to make exceptions where 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 therefore may be opened by the agency mail center if warranted. However, personal mail remains personal and 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.

3.5. Loss Prevention and Cost Avoidance

- Be aware of circumstances that may prompt an employee to steal.
- Integrate accounting procedures for all forms of postage – meters, stamps and permits.
- Establish procedures to control access of employees, known visitors, and escorted visitors. This should include requiring visitors to sign a log, and if possible, installing access control equipment such as key control, card readers, or buzz entry options.

- Permit only authorized employees to accept mail.
- Conduct regular checks of your postage meters to ensure employees are not using agency meters for personal mail. Maintain meter logs (Postal Service Form 3602-A or electronic logs) diligently and lock meters when not in use. Where feasible, remove the meter from the equipment and store it in a locked cabinet during off-hours.
- Carefully package shipments of valuable materials; send them via accountable mail, and make sure their outside labeling does not identify the contents.
- Implement inventory controls to ensure proper access and accountability for stamps, permit envelopes and labels. Perform regular audits of the inventory.
- No personal mail should be sent using the meter or permit imprints. If the agency allows staff to drop personal mail at the mail center, separate it from official outgoing mail, and insist that staff provide their own stamps for personal mail.
- Review bills from carriers (e.g., FedEx, UPS) regularly to guard against unauthorized use.
- Check periodically to determine if the mail messengers are making unauthorized stops or leaving the mail unattended in unlocked delivery vehicles.
- Obtain delivery time listings from express carriers and make sure that all appropriate refunds for late or incomplete deliveries are collected.

3.6. Physical Security in a Mail Center/Facility

- If possible, make the mail center an enclosed room with defined points of entry. If you can't put the mail center in its own room, then set aside a defined space that is used only for processing mail. Do not have employee lockers within the mail center. If possible, locate the mail center near the loading dock. This will minimize the impact that any potentially contaminated mail will have on the rest of the building.
- Where the risk assessment, the volume of mail, and a cost-benefit analysis make it appropriate, the mail center should have its own air handling and ventilation system. You may also consider establishing negative air pressure for the area where you process incoming mail or for the entire mail center. Down-draft tables with HEPA filters are a good way to limit employee exposure to routine dust as well as possible airborne hazards. You may also want to consider an isolated room with its own ventilation system and HEPA filters.
- If you regularly see suspicious letters or packages in your mail stream, you may want to obtain a glove box or biochemical hood to open mail (a biochemical hood operates with negative air pressure).
- Install alarms at each access point, and monitor them for after-hours activity.
- Install secure areas, such as safes or locked cabinets, for meters, express shipments and valuables. Reset combinations and re-key locks after significant employee transitions.
- Provide a separate and secure area for personal items (e.g., coats and purses). Consider prohibiting employees from taking personal items into the workplace.
- Where appropriate, use surveillance cameras to monitor the service counter and all entrances. Assure your employees that the cameras aren't for tracking their movements, but for protecting them from potential threats.

- Make sure that supervisors and team leaders are clearly visible from the floor. Proper supervision is a prerequisite for keeping personnel and your mail center safe. Leaders must be easily accessible to respond to emergency situations.
- Post signs around the mail center listing whom to call in the event of various emergencies such as fire, theft, suspicious package, etc. This is probably the most important step you can take in preparing to deal with emergencies or suspicious letters and packages. Make sure these signs are updated.

3.7. Daily Opening and Closing Procedures

Prepare detailed procedures for opening and closing the mail center. Make sure that logs and checklists are filled out and signed daily.

The checklist for opening the mail center should include:

- Check all locks/entrances
- Start visitor log
- Verify contents of safe/vault
- Take meter readings

The checklist for closing the mail center should include:

- Take meter readings
- Secure meters
- File visitor log
- Secure all mail
- Create safe/vault contents log
- Ensure that all locks/entrances are closed
- Clean areas and equipment

Establish daily procedures for cleaning the area and equipment used to process inbound mail. All flat work areas should be wiped down daily with disinfectant. All machines should be cleaned with disinfectant wipes and vacuums equipped with HEPA filters. Do not use pressurized air to clean equipment and machinery.

3.8. Facility Security Committees

The 1995 Department of Justice Vulnerability Assessment of Federal Facilities recommended that all federal buildings should have Building Security Committees, now referred to as Facility Security Committees (FSC). FSC membership consists of at least one representative from each of the federal agencies occupying the building. The FSC serves as the principal forum for discussion of the building's security and emergency planning requirements.

The mail center manager should serve as part of the FSC membership to ensure that the overall building security plan includes specific consideration of the mail center and its particular vulnerabilities and needs.

3.9. Offsite Processing of Incoming Mail

Offsite processing is an option that you should consider if the security assessment identifies a high level of risk or if mail volumes are large enough to justify the cost. There are also advantages, primarily in terms of timely processing and readily available customer service, to placing the mail center on site.

Consideration of offsite processing may raise additional questions, such as:

- Which specific aspects of mail processing can be accomplished with a higher level of security offsite?
- What is the difference in cost to build, maintain, and operate the offsite facility versus a comparable facility onsite?
- Will you also maintain a customer service counter onsite?
- How much longer will it take to deliver mail if it is processed offsite, and would the additional time be critical to part of your agency's operations?
- Will a contractor operate the offsite facility and, if so, what security and performance standards will you establish in the contract?
- Would it be cost-effective to scan, store, and deliver some portion of the incoming mail electronically?

3.10. Sending and Receiving Mail at an Alternative Worksite

FMR102-192.70 (c) requires agencies to have a security policy for employees receiving incoming and sending outgoing mail at an alternative worksite such as a telework center.

GSA recommends all incoming mail be screened at a federal facility before sending to employees at alternative worksites. It is the agency's responsibility to develop the plan on receiving mail, packages, and accountable mail.

Agencies should consider the following when developing alternate worksite policy:

- How employees will receive official mail, (i.e., USPS, FedEx, UPS, other service provider(s)
- Accountable tracking for sending mail from alternative worksites
- Mail security steps employees must implement for receiving, sending and storing official mail
- Resending mail from the agency to employees, including whether the agency is willing to spend the additional funds

3.11. Personal Protective Equipment

GSA does not recommend mandatory use of Personal Protective Equipment (PPE) if the risk analysis does not support it. This includes gloves, aprons, and respirators. On the other hand, GSA does recommend making PPE available for any mail center personnel who choose to use them.

The mail center manager should provide training on the use of PPE. This equipment can cause problems, so any employee who chooses to use them must be trained. For example, removing gloves the wrong way can spread contamination, and respirators can induce respiratory problems in some people. Respirators must be

fitted by a trained expert to provide a useful level of protection. Managers must ensure that all equipment is kept clean and properly serviced.

If some employees choose to use PPE, the manager should establish a log to monitor employees' initial equipment training and periodic retraining.

The Centers for Disease Control (CDC) provides guidance on selecting PPE to protect against bioterrorism. For the most current information, refer to the Centers for Disease Control website: http://www.cdc.gov/niosh/topics/emres/ppe.html and https://www.osha.gov/Publications/osha3151.html

3.12. Psychological Effects

Many Americans have been profoundly affected by the attacks on the United States and the specter of a prolonged war against terrorism. We need to support and listen to each other, and understand that on-going hoaxes may keep our emotions high in anticipation of another attack.

Feel and observe what is going on around you. Listen to what is being said, and watch the attitudes, moods and body language of co-workers, friends and others with whom you interact. Do you sense that unspoken fears are troubling a co-worker? Does he/she seem unusually quiet, sad, troubled? Trust your instincts and intuitions. Don't hesitate to strike up a conversation. Create an atmosphere that welcomes sharing, while also being respectful of individuals who have little to say or prefer to remain silent.

The attitudes and feelings of employees are critical to the success of your mail center. It is important to recognize that some of your employees will have concerns about their personal safety. Managers need to be prepared to help employees carry out their jobs in these challenging times.

Every federal agency has an Employee Assistance Program (EAP) to help restore employees to full productivity. The EAP provides free, confidential, short-term counseling to identify the employee's problem and, when appropriate, make a referral to an outside organization, facility, or program to assist the employee in resolving their problem. Counselors are available to help manage fears. Mail managers should know how to avail themselves and employees of these services if they are needed. To locate the EAP serving your federal agency, call your human resource office and ask for the telephone number. For additional information about EAP, download ***Your Federal Employee Assistance Program: a Question and Answer Guide for Federal Employees*** at http://archive.opm.gov/employment_and_benefits/worklife/officialdocuments/handbooksguides/eap_qanda/index.asp

A traumatic event in the workplace may impact an organization's ability to perform. Guidance for agency managers can be found in ***Handling Traumatic Events: a Manager's Handbook***, which describes steps managers can take to provide effective leadership after a traumatic event. This is at: http://www.opm.gov/policy-data-oversight/worklife/reference-materials/traumaticevents.pdf

3.13. Workplace Violence

Employees who are being harassed, stalked, or threatened inside or outside the workplace should inform their managers and supervisors. Managers have a responsibility to be sensitive to the realities of workplace violence and the effects on employees from abuse outside the workplace. Some employees may be involved in domestic

disputes that have the potential to erupt and spill over into the workplace. Every effort must be made to protect these employees and anyone else who may become an innocent victim.

Building security should be notified, and additional steps should be taken to protect these employees. If there appears to be an immediate threat, notify the law enforcement resource that can most readily provide security in the situation. This resource may be a local police officer, an inspector, a special agent, or a Federal Protective Service officer. Everyone in the office should know who the responsible law enforcement resources are and how to contact them. Establishing these contacts prior to a crisis can help in the event they are needed in an emergency.

More information is available on workplace violence at the OPM website at: http://www.opm.gov/policy-data-oversight/worklife/reference-materials/workplaceviolence.pdf.

4 Training, Testing, and Rehearsal

All mail center personnel should receive training (at a minimum on an annual basis) on identifying and handling suspicious mail and packages. It is important to 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.

Education and awareness are the essential ingredients to preparedness. Employees need to remain aware of their surroundings and the packages they handle. You must carefully design and vigorously monitor your security program to reduce the risk for all.

Through training, you can develop a culture of security awareness in your operation. Through rehearsal, you can ensure that critical lessons have been learned and retained. A union representative or other employee representative will ensure employee confidence in their safety in developing and giving training. Managers should consider security training and rehearsal a critical element of their job.

In addition to educating the employees who work for you, you should educate the employees who work for your agency. Employee awareness of the measures you've taken leads to confidence in the safety of the packages that are delivered to their desktops.

The actions you take ***before*** a threat have a lasting impact on the safety of everyone in your agency. The actions you take ***during*** a threat have an immediate impact on the safety of everyone in your mail center. Preparing your mail center and your employees to handle a threat is an obligation you must meet every day.

4.1. The Importance of Testing the Plan

One key to performance during an emergency is testing of the plan in advance. Test contingency plans in a way that does not alarm employees and customers but follows the steps to take if there is an event. The dress rehearsals reinforce the training so the plans can be effectively implemented in the event of an actual emergency.

4.2. X-Ray Training

Training is necessary to qualify someone to inspect letters and packages by X-ray. You should ensure that all of your personnel and any contractors who staff the X-ray machine have sufficient training, and that they keep their training current.

4.3. Contents of a Complete Training Program

- Basic security procedures
- How to recognize and report suspicious packages
- Inspecting letters and packages by X-ray
- Proper use of Personal Protective Equipment (PPE)
- How to respond to a biological threat
- How to respond to a bomb threat
- Continuity of Operations Plan (COOP)
- Occupant Emergency Plan (OEP)

To be effective, any training must be ongoing. This is especially true with security issues. Schedule brief update sessions with your employees on a regular basis. Maintain a log of all mail center employees and training attended, including the date completed.

5 Managing Threats

5.1. Suspicious Letters and Packages

The mail center is a first line of defense for your agency. You should examine every piece of mail before you do anything else with it. You should inspect it with an X-ray machine, and look for suspicious characteristics. Figure 5 is a standard list of characteristics that you and your staff should look for.

Figure 5. **Characteristics of Suspicious Packages or Letters**

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

Mail Center employees should receive annual training to recognize and report suspicious packages. Characteristics of a suspicious package or letter vary, depending upon the types of mail that your operation routinely processes. What is suspicious in one mail center is not necessarily suspicious in another. However, anything from the preceding list that is unusual, in terms of your normal mail, or multiple items from this list, should draw the attention of your employees.

5.2. Post Examples

Copies of a "suspicious letter" poster should be displayed in every mail center. These posters are available from the Federal Bureau of Investigation (FBI) and the United States Postal Inspection Service (USPIS). We have worked with the FBI, USPIS, and other authorities to develop the standard list shown in Figure 5 "Characteristics of Suspicious Packages or Letters". You should post phone numbers of whom to call, and display USPS Poster 84, "Suspicious Mail and Packages." http://about.usps.com/posters/pos84.pdf.

5.3. Rehearse

Rehearse scenarios and test contingency plans at least annually with employees to ensure that, in the event of an emergency, they will know how to respond. Do this in a way that does not alarm employees or customers. One way is to conduct a tabletop exercise of the emergency response plan. These rehearsals will help ensure that the lines of communication function as planned and that everyone knows their role. Hold post-test meetings to address problems, and resolve them before the next test.

5.4. Initial Alert Procedures

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. There are, however, a number of common steps that should be taken.

- Remain calm. Alert others in the immediate area that you have identified a suspicious item. Ensure that the organization's security command center or local law enforcement and first responders are notified. If in a multi-tenant facility, building management should also be contacted.
- Do not attempt to move the suspicious item. Put the envelope or package 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 open the letter or package.
- Do not shake or empty the contents of a suspicious letter or package.
- Do not carry the letter or package or allow others to examine it.

Mail that contains an unidentified secondary container: If X-ray inspection shows a secondary container that may contain an unknown material, or if you open a letter or package and discover such a container, do not open or otherwise disturb the secondary container. Treat the secondary container as suspicious, unopened

mail. Call the addressee and see if they can identify the container. If the addressee cannot be located, then call in the first responder designated to open suspicious mail.

5.5. Chemical, Biological, Radiological, Nuclear, and Explosive Devices (CBRNE)

The procedures for examining letters and packages, identifying suspicious ones, and calling in an expert when necessary are part of managing threats. The first responder should assess for the presence of chemical, biological, radiological, nuclear, and explosive devices (CBRNE). Many different threats can be sent through the mail.

In the event that a trained first responder, after reviewing the situation, determines that a possible threat may be present, the first responder should take steps to determine the nature of the threat. A chemical, explosive, or radiological threat is immediate and requires swift, crisis-level responses. A biological agent is any biological material capable of causing:

- Death, disease, or other biological malfunction in a human, an animal, a plant, or another living organism;
- Deterioration of food, water, equipment, supplies or material of any kind;
- Harmful alteration of the environment.

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 not often immediately noticeable. When it is safe to do so, seek shelter inside a building, putting as much shelter between you and the potential contaminant as possible. Limit the amount of exposure by leaving the area when it is safe to do so, or wait for the directions of first responding organizations.

In chemical attacks, a solid, liquid or toxic gas is used to contaminate people or the environment. The prevalent symptoms are tightness in the chest, difficulty breathing, blurred vision, stinging of the eyes, or loss of coordination. 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. If the release is inside the building and the situation permits, close ventilation, then leave as soon as possible and go outside, moving upwind and away from the area. Some significant differences exist between biological and other threats, as exemplified by the following Table 1.

Table 1: **Chem/Bio Attack Profile Matrix**

	BIOLOGICAL	CHEMICAL
Release Site of Weapon	Difficult to identify, possible time delay in defining area of attack unless overt	Quickly discovered, possible to cordon off contaminated attack area(s)
Manifestation of Symptoms	Delayed, usually days to weeks after an attack (except toxins)	Rapid onset, usually minutes to hours after an attack
Distribution of Affected Patients	Widely and rapidly spread; contagious versus non-contagious	Downwind area near point of release
Signatures	Typically no characteristic signatures immediately after an attack	Easily observed (colored residue, dead foliage, pungent odor, dead insects or animal life)
Medical Countermeasures	Antimicrobial treatments, vaccines or immunoglobulins for some agents	Chemical antidotes for some agents
Casualty Management & Contamination	Patient isolation and/ or quarantine crucial if communicable disease is involved	After decontamination, no further need of protective measures or risk of further contamination

As opposed to chemical and radiological agents, biological agents are not as immediately recognizable, and consequences may be delayed, for example, by therapy or vaccination, not traditionally performed by first responders. However, effective countermeasures are available against many of the bacteria, viruses, and toxins that might be used. If we develop a solid understanding of the biological threats we face and how to respond to them, many effects can be prevented or minimized.

The most important thing to remember when dealing with a letter bomb, biological or chemical agent threat is: don't panic. Rash actions can lead to even more harmful consequences. Biological agents, for example, can spread more rapidly when improperly handled.

The United States Postal Inspection Service uses the acronym "SAFE":

- Safety comes first.
- Assess the situation before taking action.
- Focus your efforts on the hazard, avoiding contact and access.
- Evaluate the situation and notify authorities.

5.6. Mail Bombs

Motives for mail bombs are often revenge, extortion, terrorism, or business disputes. The likelihood of receiving a mail bomb is very remote. However, mail bombs must be taken seriously, as they can kill and seriously injure.

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. Mail bombs may or may not have one or more of the characteristics listed in in Figure 5, Characteristics of Suspicious Packages or Letters.

The critical lesson about mail bombs is that virtually all of them can be detected by skilled X-ray inspection of letters and packages. To ensure that X-ray inspectors are paying close attention, consider using software that randomly inserts a test image of a suspicious package among the images of actual letters and packages being scanned.

For more information on mail bombs, check with your local Postal Inspector or visit the USPIS web site at: https://postalinspectors.uspis.gov

6 Communications Plan

The mail center should develop a communications plan to be executed when responding to a threat. This plan should cover how to acquire and distribute information. Prepare a list of trusted resources to acquire timely and accurate information (e.g., GSA, USPS, CDC, National Terrorism Advisory System (NTAS), etc.). Organize protocols for the approval and distribution of information on the status of the mail operation. For more information, also see the section on the Occupant Emergency Plan (OEP) and GSA's National Guidelines for Assessing and Managing Biological Threats in Federal Mail Facilities. Good communications are part of any successful mail operation and are critical for security issues. You have at least three audiences: management, customers, and mail center personnel. All these audiences rely on relationships.

6.1. Management

Schedule regular meetings with representatives from the senior management of your agency (executive secretariat, administrators, etc.), regional offices, and facility. Review the steps you've taken to secure the mail, employees, and facility, and address any outstanding issues.

When first establishing your own security guide, begin with more frequent meetings, perhaps monthly. As events dictate, you may be able to change the frequency to quarterly or semi-annually. However, do not let six months pass without a meeting.

6.2. Customers

The aspects of your security plans that will affect customers directly should be developed with cooperation and assistance from mailers. Highlights of your plans should be communicated regularly to all customers. These two steps will assure customer cooperation and understanding in the event of an emergency. Consider marketing your plan during annual or semi-events.

6.3. Mail Center Personnel

Mail center personnel should be thoroughly involved in developing and implementing your security plans. Once the plan is developed, the most important part of communicating those plans is training. We also suggest that you set aside time in every meeting with mail center personnel to discuss security. Enhanced security procedures and vigilance must become a way of life for those involved.

As part of your security procedures, you should establish a call tree for employees and managers. The call tree list should include, as a minimum:

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

This call tree should be tested and updated regularly.

6.4. Communications during an Emergency

Clear, consistent, and factual communications are critical in any emergency. Past biological attacks (ricin, anthrax, etc.) demonstrated that the morale and performance of everyone involved in an emergency could be very seriously affected by inconsistent, vague, and opinionated information. Everyone in authority must be very careful to check facts, to know who the designated official spokesperson is for every aspect of the emergency, and to coordinate any messages thoroughly.

Occupational Safety and Health Administration (OSHA) standards require employers to make health and safety information available to any employee who requests it. All information relevant to apparent and credible biological threats should be provided to employees as quickly as possible, preferably without waiting for a request. Health and Safety Plans, also required by OSHA regulations, must include provisions for sharing health and safety information.

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 at www.nod.org.

6.5. Relationships with Partner Organizations (First Responders, Public Health Authorities, FBI, FPS, Regional USPIS, Fire, Hazmat and Law Enforcement Officials)

Many other aspects of security also require that you develop and maintain relationships with key partners. Your first task in this regard 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 Federal Bureau of Investigation Weapons of Mass Destruction (WMD) coordinators at: www.fbi.gov/about-us/investigate/terrorism/wmd; and
- Regional US Postal Inspection Service inspectors.

A "first responder" is an emergency worker who responds to an incident within a set amount of time. They also provide trained people to respond to emergency situations. Usually this first responder label is specific to Fire, Law Enforcement, and Emergency Medical Service (EMS) immediately arriving assets. You may need to establish relationships with several different first responder organizations, depending on the personnel and capabilities that they can provide. First responders to federal mail facilities may be federal, state, and/or local organizations, depending on your specific circumstances.

Once you have identified your first responder(s), then

1. Determine who will be responsible for opening suspicious letters and packages, and establish a relationship with them (this may be specially trained federal personnel or other first responders).
2. Establish relationships and protocols with internal emergency management office.
3. Ensure that the first responder organization(s) are ready, willing, and able to follow the established protocols.

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 at http://www.epa.gov/osweroe1/content/epcra/serc_contacts.htm.

7 Occupant Emergency Plan (OEP)

The Occupant Emergency Plan is 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 its development of the OEP.

An occupant emergency is an event that may require you to evacuate from your occupied space or relocate to a safer area. The emergency may include a fire, 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. In the event of an emergency, the mail center manager must protect the people who work there and ensure their exit from the situation to a safe place.

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 spells out all the details of an Occupant Emergency Program.

The GSA Occupancy Emergency Plans Guide defines an OEP as "the actions that occupants should take to ensure their safety if a fire or other emergency situation occurs." These plans reduce the threat to personnel, property, and other assets within the facility in the event of an incident inside or immediately surrounding a facility by providing facility-specific response procedures for occupants to follow.

7.1. Occupant Emergency Program

The Occupant Emergency Program establishes a process for safeguarding lives and property in and around the facility during emergencies. The first component of an Occupant Emergency Program is the development of a plan, which is the OEP, to protect life and property under certain specified emergency conditions. The second component is the formation of an Occupant Emergency Organization.

7.2. Occupant Emergency Organization

The Occupant Emergency Organization is a group of employees from the agency who carry out the emergency program. It is comprised of a designated official and other employees assigned to undertake certain responsibilities and perform the specific tasks outlined in their OEP.

7.3. Designated Official

The designated official establishes, develops, applies, and maintains the plan. The designated official is the highest-ranking official in a federal facility, or may be another person chosen by all tenant agencies. In the absence of a designated official, an alternate may be selected to carry out additional responsibilities.

7.4. Critical Elements of the OEP

Evacuation Plans
Be sure to specify where the mail center's employees should gather immediately after an evacuation, so that the supervisor on duty can account for every mail center employee and visitor. In some circumstances employees may be instructed to Shelter-In-Place (SIP). 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, staying put and creating a barrier between yourself and potentially contaminated air outside, a process known as shelter-in-place is a matter of survival. Make sure employees know how to listen for instructions on where to go and when to evacuate. They must know the exact route that authorities specify. It is important to follow instructions and not take any shortcuts, as lives are dependent on following instructions. For more information on SIP visit http://emergency.cdc.gov/preparedness/shelter/.

Whom to Contact in the Event of an Emergency
All personnel should know whom 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. This list should be included in the disaster supply kit.

Building/Occupant Information
The OEP should contain specific information about the building's construction and its occupants in narrative form or on a Building Information Sheet and Occupant Information Sheet. Floor plans should be included with evacuation routes clearly marked.

The Command Center
Emergency operations are directed from a command center. The command center should be centrally located and easily accessible. The command center should have good communications capability, including at least two telephones and, if possible, portable radios and batteries along with chargers.

More information on OEPs is available on the web by searching for 'OEP' at http://www.gsa.gov or at:

For more information contact your local FPS Law Enforcement Security Officer (LESO).

8 Continuity of Operations Planning (COOP)

The intent of the Continuity of Operations Plan (COOP) is to ensure continuance of essential federal functions across a wide range of potential emergencies. Essential functions are those that 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. The COOP deals with maintaining essential work once the safety of your personnel has been assured.

The anthrax attacks demonstrated that hard-copy mail is not essential for every federal office, but mail remains a critical function for many federal programs. The mail manager should be thoroughly involved in the COOP process in any case. The actual steps that are 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.

8.1. Key Elements of a COOP

- Outline Primary Mission Essential Functions (PMEFs)
- Plan decision process for implementation
- Establish a roster of authorized personnel
- Provide advisories, alerts and COOP activation, and associate 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 on an emergency basis

8.2. Responsibilities of the Mail Manager in a COOP

The following are key suggested questions that the COOP should address for mail:

- 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?

8.3. Objectives of a COOP for a Mail Facility

- 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 during an emergency
- Reduce or mitigate disruptions to operations
- Protect essential facilities, equipment, records, and other assets
- Facilitate decision-making during an emergency
- Achieve orderly recovery from a wide range of potential emergencies or threats, including acts of nature, accidents, technological and attack-related emergencies
- Mitigate risks

8.4. COOP Background Documents

Since 1988, a number of documents have built the foundation for COOP in federal agencies:

- Executive Order 12656 assigned responsibility for national security emergency preparedness to federal departments and agencies.
- Presidential Decision Directives 39, 62, and 63 addressed counter-terrorism, terrorism, and critical infrastructure.
- Presidential Decision Directive 67 specifically addressed COOP in 1998

These documents are available for download at: the Homeland Security Digital Library at http://www.hsdl.org

8.5. 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, this 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. You should designate a key official and one or more alternates to pick up the kit in an emergency. You should also keep a duplicate fly-away kit at your backup facility.

9 Review of the Security Plan

9.1. Initial Review

Agency mail managers must coordinate with their agency security service and/or the FPS or the U.S. Postal Inspection Service to develop agency mail security policies and plans.

At a minimum, the plan should provide a written report that covers

- Location(s) surveyed
- A critique of the formal plan
- Training audit
- Analysis to determine if employees are following established procedures
- Background of the organization conducting the review

If you desire, the GSA Mail Management Policy office will coordinate a peer review of your operation, employing senior members of the Interagency Mail Policy Council. These reviews will only be conducted if requested by the agency or mail center manager. All results from the review will be held confidential, with all copies being handed over to the requesting official.

If you would like GSA to coordinate a review, please send an e-mail request to the Director, GSA Mail Management Policy. In your request, please include the desired dates of the survey, an alternate start date, name of the organization to be surveyed, and the point-of-contact name and phone number.

E-mail requests to: federal.mail@gsa.gov

9.2. Annual Review

Once a year or if there are any changes, you should review all aspects of your security plan. Circumstances change, and the guidance on protecting your mail center and your agency continues to evolve. Re-evaluate your last rehearsal to determine any training needs that might have emerged as a result. Train your personnel and rehearse your plan.

10 Contractors

Many agencies use contractors to process their mail, either as outsource providers that manage mail centers or as letter shops that consolidate and/or presort outgoing mail. It is important to remember that mail center security remains the responsibility of the agency, even when a contractor takes over 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 –These will reduce opportunities for mishandling.
- Security –The contract should specify the steps the vendor will take to provide the best possible security, including hiring practices and employee screening checks.
- Technology – Evaluate the technology that the vendor will deploy to process your mail. GSA suggests you request presentations on electronic manifests for inbound mail, Coding Accuracy Support System (CASS) certification, Intelligent Mail barcode (IMb), National Change of Address (NCOA), etc.
- Discount sharing –When you use a presort agency/company to prepare and presort your mail, conduct on-site audits to ensure that you are being charged correctly and receiving the appropriate discounts.
- Scanning/electronic imaging – Ask for vendor briefings on preparing and storing digital images. Ask your agency information technology department for assistance with this review. The briefing should cover the strategy for the long-term storage of electronic documents, retrieval from long-term storage, and how original documents will be prepared and indexed for storage.

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

1. **A performance work statement**: The performance work statement 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. It is important to answer these questions completely, to allow the vendor the opportunity to accurately assess resources required and risks involved.

2. **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.

3. **Appropriate incentives**: Incentives should be used when they will encourage better quality performance, and may be either positive or 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.

Conduct periodic reviews separately from the acquisition process. Also, tour the shop to see that the procedures are being followed. Confirm that all mail is being processed in a timely manner and that all other performance standards are being met.

More information on Performance-Based Contracting can be found at http://www.gsa.gov by typing ARNET, using the search tool. This will provide the latest information.

11 Conclusion

The federal mail center is a gateway into the infrastructure of the agency. Safety and security is critical to a mail center's operations regardless of whether it is large or small. Although the mail center operates as an entry point for federal agencies, security policies and procedures for the mail center are often overlooked. Mail center personnel must understand their roles as gatekeepers who are charged with protecting not only their personal safety, health, and welfare, but that of the facilities and customers they serve.

Avoid underestimating the importance of mail center security:

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

This Mail Center Security Guide was prepared by GSA with a team of experts to help you, the mail center manager, and your coworkers to keep your mail center safe and secure.

Prevention is the key for keeping your mail center secure.

12 Appendices

Appendix A – Glossary of Terms

1. **Accountable Mail** – Items that require tracking, signature, or proof of delivery (e.g., Registered Mail, Certified Mail, FedEx, etc.).

2. **Asset and Mission Identification** –The first step in a risk assessment is identifying the assets and missions that must be protected. In the asset identification step, the security specialist, with the assistance of the asset owner, identifies and focuses only on those assets important to the mission or operation.

3. **Biological Agent** – Any biological material capable of causing the following:
   a. Death, disease, or other biological malfunction in a human, an animal, a plant, or another living organism;
   b. Deterioration of food, water, equipment, supplies or material of any kind;
   c. Harmful alteration of the environment.

4. **Facility Security Committee** – The FSC consists of at least one representative from each of the federal agencies occupying the building. The FSC serves as the principal forum for discussion of the building's security and emergency planning requirements.

5. **Closed-Loop Manifest System** – A system in which someone signs for each piece of accountable mail whenever possession changes. For example, the receiving clerk should require internal couriers to sign for all packages that they deliver.

6. **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.

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

8. **Designated Official (DO)**– A staff member, who establishes, develops, applies, and maintains the plan. The designated official is the highest-ranking official in a federal facility or may be another person agreed upon by all tenant agencies.

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

10. **Down-Draft Tables** – Mail processing tables with High Efficiency Particulate Air (HEPA) filters are a good way to limit employee exposure to routine dust as well as possible airborne hazards.

11. **Executive Order 12656** – An executive order assigning responsibility for national security emergency preparedness to federal departments and agencies.

12. **First Responder** –The first person (e.g., 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.

13. **Fly-Away Kit** – An emergency supply kit that consists of those items considered 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.

14. **FMR 102-192** – Federal Mail Management Regulation. This document prescribes policy and requirements for the effective, economical, and secure management of incoming, internal, and outgoing mail in federal agencies.

15. **Impact Assessment** – A determination of the impact or consequences if an asset were lost, damaged, or destroyed; if an agency were temporarily prevented from performing its mission; or if its ability to perform its mission were significantly impaired.

16. **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.

17. **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.

18. **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.

19. **Offsite Processing** – Offsite processing is an option to consider if a security assessment identifies a high level of risk, or if mail volumes are large enough to justify the cost.

20. **Performance-Based Contract/Service** – A contract designed to describe the requirements in terms of results required rather than the methods of performing the work. It uses measurable performance standards (i.e., terms of quality, timeliness, quantity, etc.) and quality assurance surveillance plans. It may also include performance incentives where appropriate.

21. **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.

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

23. **Presidential Decision Directives 39, 62, 63, & 67** – Directives 39, 62, and 63 addressed counter-terrorism, terrorism, and critical infrastructure. Presidential Decision Directive 67 specifically addressed COOP in 1998.

24. **Risk Assessment** – Process to determine the likelihood that identifiable threats will harm a federal agency or its mission. Each site or mail center has different threats and risk levels, and this will lead to different security measures for each site.

25. **Satellite Facilities** – Refers to mail operations that are performed in a small room, one corner of a room, or one corner of a desk. In these facilities, responsibility for processing mail is divided among professional and support staff.

26. **Security Analyst** – Individual who identifies the specific threats that might occur in your mail center or your facility.

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

28. **Threat Assessment** – An evaluation of the full spectrum of threats – natural, criminal, accidental, or terrorist – for a given location. The assessment should examine supporting information to evaluate the likelihood of occurrence for each threat.

29. **Vulnerability Assessment** – Considers the potential impact of loss from a successful event or occurrence.

Appendix B – Risk Analysis Worksheet

Assets and Missions	Undesirable Events	Loss Effect	Threats	Vulnerability	Counter-measure Options	Overall Risk Evaluation
Postage meters	Fraudulent use	Medium	Mail center personnel	Medium	Automated postage tracking	Medium
Mail center personnel	Injury	High	Workplace injuries	High	Improved mail center layout	Medium
Mail delivery roster	Loss	High	Fire	Low	Effective OEP	Low
Agency missions	Temporarily disabled	Critical	Flood	Low	Plumbing maintenance	Low
Agency executives	Injury or death	Critical	Improvised explosive	Low	X-ray inspection of packages	Low

Appendix C – Online Resources for Keeping Your Mail Center Safe

Bureau of Alcohol, Tobacco and Firearms (ATF) – http://www.atf.gov/

Centers for Disease Control (CDC) – http://www.cdc.gov

Department of the Army Pamphlet 25-52, Mail Facility Security and Handling Suspicious Mail – http://www.apd.army.mil/pdffiles/p25_52.pdf

Department of Homeland Security, Biological Attack: The Danger - http://www.dhs.gov/biological-attack-danger

DHS Security Assessment – https://www.dhs.gov/critical-infrastructure-vulnerability-assessments

Federal Bureau of Investigation (FBI) – http://www.fbi.gov

Federal Emergency Management Agency (FEMA) – http://www.fema.gov

Federal Protective Service (FPS) – http://www.dhs.gov/federal-protective-service

General Services Administration (GSA) – http://www.gsa.gov

GSA Mail Communications Policy – http://www.gsa.gov/mailpolicy

Office of Personnel Management – publishes questions and answers on federal employees, personnel issues, etc. – http://www.opm.gov

U.S. Department of Labor (DOL), Occupational Safety and Health Administration (OSHA) – http://www.osha.gov

US Postal Service (USPS) – www.usps.com

USPS Suspicious Mail Alert Poster – http://about.usps.com/posters/pos84.pdf

USPS Postal Inspection Service – www.usps.com/postalinspectors

Workplace Risk Pyramid, OSHA – http://www.osha.gov/dep/anthrax/matrix/index.html

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

Best Practices for Mail Center Security – http://about.usps.com/securing-the-mail/best-practices.htm

Bombs by Mail (Notice 71) – http://uspsnotices.lettercarriernetwork.info/not71.pdf

Consumer & Business Guide to Preventing Mail Fraud Publication 300A – http://about.usps.com/publications/pub300a.pdf

Identify Theft Brochure – (Publication 280) – http://about.usps.com/publications/pub280.pdf

Notice of Reward (Poster 296) – http://about.usps.com/posters/pos296/welcome.htm

Warning! Reusing Postage (Poster 5) – http://about.usps.com/posters/pos5.pdf

Appendix D – Mail Center Security Checklist

This checklist was first developed in 2002 to help federal agencies develop and determine the requirements for their security plans. This tool is provided to assist mail center managers with the preparation of their security plans, and to aid in determining the security requirements for their mail centers/facilities.

I. Inbound Mail Procedures – See USPS Pub 166: pp 8, 19, 20, 21

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/packages for senior agency officials are inspected closely.
☐	☐	A system is in place for accountable letters and packages (i.e., 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).

II. 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 packages/letters.
☐	☐	Procedures are posted on how to recognize suspicious packages/letters and staff is trained.
☐	☐	Employees have been trained on the proper use of personal protection equipment, if it is being used.
☐	☐	Employees are trained on the Occupant Emergency Plan and are 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 General Services Administration and the U. S. Postal Service.

☐ ☐ Mail centers rehearse various evacuation plans and/or scenarios.

III. 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 wear photo identification at all times.

☐ ☐ Visitors to the mail center sign a log and are escorted at all times.

The checklist for opening the mail center includes:

YES NO

☐ ☐ A check of all locks/entrances

☐ ☐ Visitors' log

☐ ☐ Verification of contents of safes/vaults

☐ ☐ Open meter readings

The checklist for closing the mail center includes:

YES NO

☐ ☐ Close meter readings

☐ ☐ Secure meters

☐ ☐ File the visitors' log

☐ ☐ Secure all mail

☐ ☐ Log out of all safes/vaults

☐ ☐ Check all locks/entrances

YES NO

☐ ☐ Employee parking is separated from the loading dock area (where possible).

☐ ☐ Contract delivery services are screened and/or X-rayed (where possible).

☐ ☐ Unnecessary stops by delivery vehicles are eliminated.

☐ ☐ Procedures are established for handling unexplained packages.

☐ ☐ The mail manager keeps in regular contact with the Building Security Committee.

IV. Mail Is Transported In A Safe Manner

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.

V. 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 in the event that 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 building security committees.
☐	☐	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.

VI. Communication

YES	NO	
☐	☐	The mail manager keeps in contact with facility center 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

employ¬ees to include: names, addresses, work phone numbers, home phone numbers, beeper numbers, and cellular phone numbers.

A communications plan has been developed for use during an emergency.

YES	NO	
☐	☐	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.

VII. 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; a log entry is made when each employee has completed training.
☐	☐	Signs are posted in the mail center listing whom to call in the event of emergencies such as fire, theft, suspicious packages, 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 (e.g., coats, and purses).

VII. Loss Prevention and 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 (e.g., 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 U.S. Postal Inspection Service to report mail losses. Refer to their website for more information: http://www.usps.com/postalinspectors.

IX. Contractors

Consider addressing the following in the contract; the specifics will depend on the scope of the contract:

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.

X. Occupant Emergency Plan (OEP)

YES NO

☐ ☐ 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 handicapped.

☐ ☐ 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, Federal Protective Service, security force or security protection official, etc.) assisted in developing the plan for your mail center.

XI. 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 are accounted for throughout the duration of the 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.