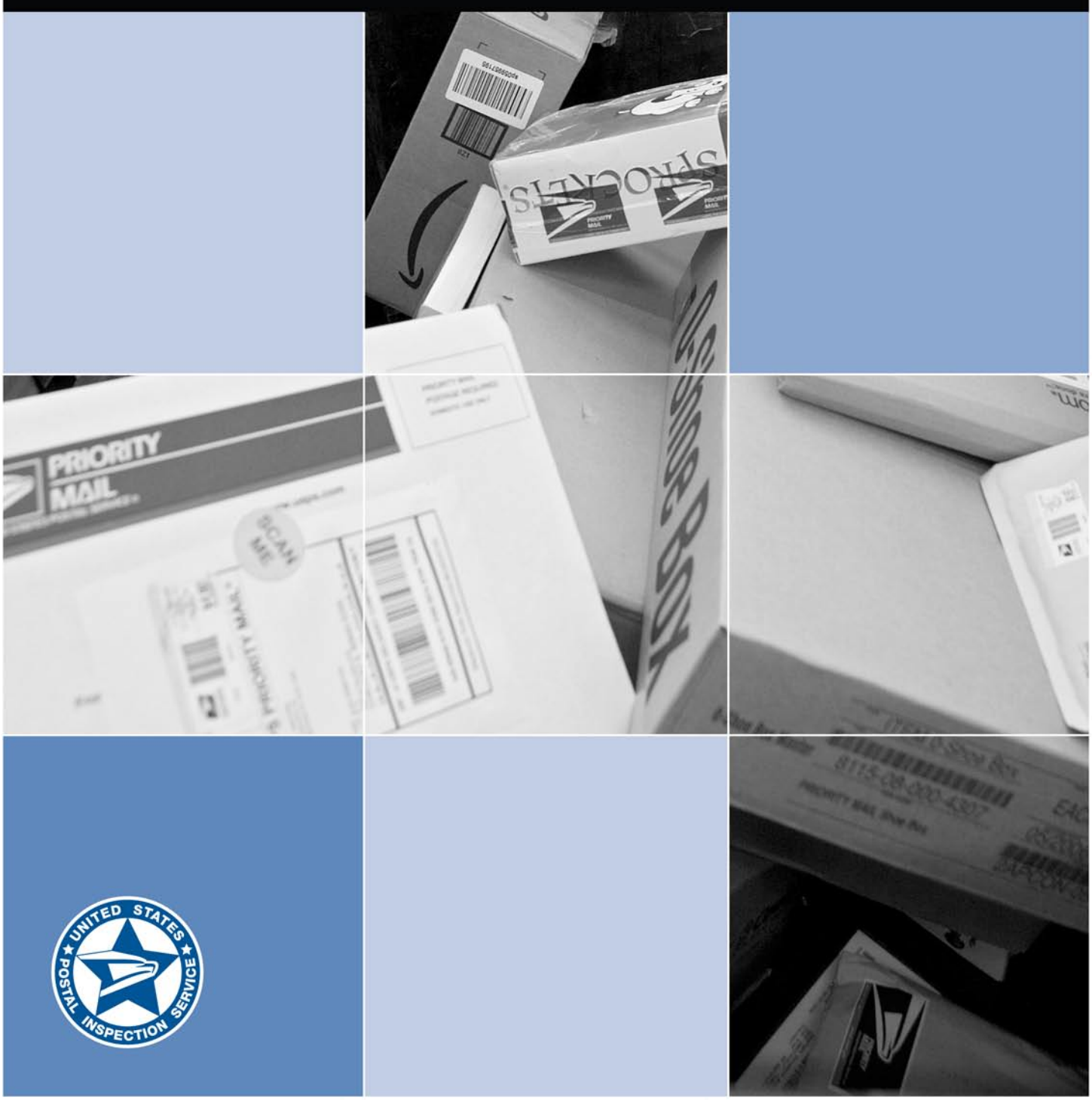
U.S. Postal Inspection Service

Guide to Mail Center Security



Contents

Introduction

The U.S. Postal Inspection Service offers this guide to help you, as a mail center supervisor, and your coworkers keep your mail center safe and secure. The guide provides general advice and recommends protective measures to help you assess, prevent, and respond to three types of threats:

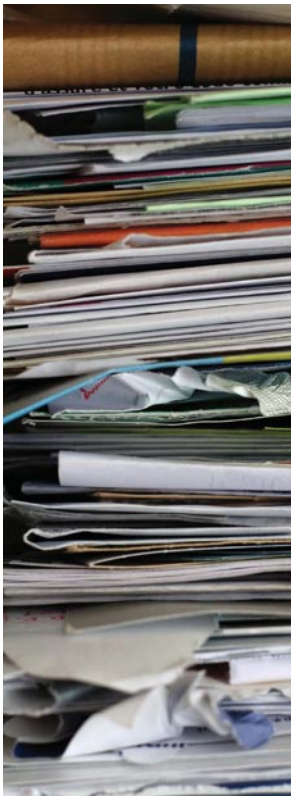
- Mail theft.
- Package bomb or bomb threat.
- Chemical, biological, or radiological threats.

The U.S. Postal Inspection Service is one of the oldest federal law enforcement agencies in the country. For more than 200 years, U.S. Postal Inspectors have protected the U.S. Postal Service, secured the nation's mail system, and ensured public trust in the mail.

Each year, the U.S. Postal Inspection Service commits significant resources to its security and prevention campaigns, emphasizing the value of preventing crime through education. Postal Inspectors across the country regularly conduct seminars for government agencies, major mailers, large and small businesses, and other postal customers to teach them about fraud schemes related to the mail, mail security practices, and principles for maintaining a safe workplace.

To contact a U.S. Postal Inspector near you, call 877-876-2455. To learn more about the U.S. Postal Inspection Service, visit *http://postalinspectors.uspis.gov.*

Note: This guide is intended for mail center supervisors and employees. The guide should not be distributed to the general public.



Assess Your Risk Level

You can determine safe mail handling standards for your organization by conducting a risk assessment of your mail operations. The assessment focuses on the room or area where mail is handled, its physical location, and its accessibility to employees and the public.

Mailrooms can be categorized as having a low, medium, or high risk level depending on their locations and their customers. If your organization employs security professionals, they can identify your mailroom risks and recommend how to address them. If not, you can immediately set in place some security measures, while others will require planning, action, and financing.

You begin a risk assessment by evaluating these areas:

- Location of mail operations.
- Jobs and tasks involved in processing mail.
- Personnel who handle the mail.
- Your customers.

You should also consider the nature of your company's business. If your organization could attract political or other potentially controversial attention, it could be a target for a mailed threat. Your mail center may be situated within a high-risk facility or in a high-risk area of your community. It is also important to be aware of your customers and the types of business they conduct. Customers involved with international businesses or a controversial profession or service can significantly heighten your risk. By assessing the people who use your mailroom, you can determine the appropriate security level you need to maintain for it.

Your assessment should identify the jobs, tasks, and personnel most likely to be jeopardized if a suspicious or dangerous letter or package entered the workplace. The Postal Inspection Service advises that you develop screening procedures for all incoming deliveries, including those from private delivery firms. All personnel must be properly trained to follow safe mail handling procedures and should understand the importance of following protocol.

In any case, it is important to evaluate the adequacy of local and state emergency response capabilities.

Review Mail Handling and Processing

One of the best ways to minimize risk to your employees and the public, reduce costs, and increase the efficiency and effectiveness of your mail center is to centralize mail handling at a separate location from the rest of your organization. Having a separate mail location reduces risk by limiting exposure to potentially dangerous mail to one location and fewer people. Having a central location reduces costs by eliminating redundancies in locations, personnel, and equipment. Establishing a trained staff to work at a single location increases the efficiency of your operations.

You should screen mail for suspicious items when it first arrives at your mailroom for sorting. Staff responsible for sorting mail by hand should perform the screening, as they are the ones most likely to notice a suspicious item. Unfortunately, screening procedures for incoming mail and packages are not foolproof. The person who first detects a suspicious package is often the intended recipient.

You should prominently display a list of suspicious package indicators in the mailroom and provide a copy of the list to all staff to ensure they become familiar with it. The Postal Inspection Service's Poster 84, *Suspicious Mail,*

illustrates key characteristics of a suspicious or dangerous mail item and is available for viewing and printing at *http://postalinspectors.uspis.gov* and on page 17 of this guide. You can order copies for a small fee by calling 800-332-0317 and selecting option 4. Enter your phone number, then select option 4 again, and wait an operator will take your call.

Appoint a Mail Center Security Coordinator

Postal Inspectors recommend you appoint a mail center security coordinator to oversee operations, ensure that security protocols are followed, and assure accountability for your mail.

Mail Center Security Coordinator

Role	Responsibilities
Oversight and Training	Oversees the screening process and sees that all deliveries are channeled through the mail center. Trains employees in detecting suspicious packages, verifications, safe handling, and communications with security and management in any crisis.
Command	Assumes command of the situation when a suspicious package is identified by mail center employees during the screening process.
Safety Enforcement	Ensures that personnel who have detected a suspicious postal item place a safe distance between themselves and the item, and that employees do not cluster around the item. Ensures that only mail center employees have access to the mail.

Train Your Mail Center Staff

Education and knowledge of security protocols are essential to preparedness. Employees must be aware of their surroundings and the packages they handle. You must carefully design and vigorously monitor your security program to reduce risks for your organization.

Training your employees encourages a culture of security awareness in your operation. A training program should address these concerns:

- Basic security procedures.
- Recognition and reporting of suspicious packages.
- Proper use of personal-protection equipment.
- Response protocols for a biological, radiological, or bomb threat.

Document the training provided for your employees and regularly follow it up with refresher training. Consider using simulation exercises followed by in-depth reviews of the response activity. Note areas where employees need improvement.

In addition to educating mail center employees, all employees in your organization should understand the mail security measures you have established. This helps instill employee confidence in the safety of the packages delivered to their desks.

Additional guidance for suspected chemical, biological, or radiological contamination is provided by the Centers for Disease Control at *www.cdc.gov.*

Secure Your Mail Center From Theft

While attention should be given to chemical, biological, and radiological threats, mail centers are much more likely to experience problems caused by common crimes such as theft. Security is vital to mail center operations large and small. Lack of security can result in theft of supplies, postage, mail, and valuable information about your company contained in sensitive mail.

When developing policies and procedures for your mailroom, the key word is prevention.

To make your mail center secure and to reduce risks and losses, your company should have policies and procedures for the following:

- Personnel security.
- Access control.
- Registered Mail™ and high-value shipments.
- Company funds.
- Postage meters.

Federal Protection of the Mail

Mail received into the hands of an addressee or addressee's agent is considered properly delivered mail. Mail addressed to employees or officials of an organization at the organization's address is considered properly delivered after it has been received at the organization. For this reason, the Postal Inspection Service discourages individuals from using their employer's address to receive personal mail.

Mail delivered into a privately owned receptacle, designated by postal regulations as a depository for receipt or delivery of mail, is protected as long as the mail remains in the box. Mail adjacent to such a box is also protected.

Protection for your mail ends when the items are removed by the addressee or the addressee's agent. Mail addressed to a Post Office™ box is considered delivered once it is properly removed from the box.

How extensive is your pre-employment screening?

When you conduct pre-employment screening, you should check a job candidate's criminal records, have the candidate undergo a drug-screening test, perform a credit inquiry on the candidate, and verify the candidate's former employment. When you interview a job candidate in depth and at length, you may identify potentially derogatory information.

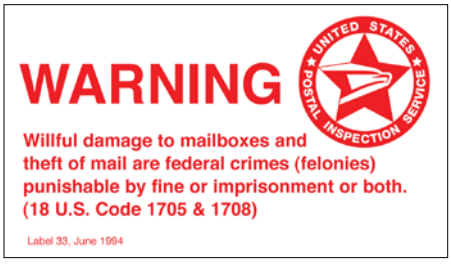
What may prompt an employee to steal?

An employee's personal situation can change quickly. An honest, trusted employee can become a thief because of need. Alcohol, drugs, gambling, and marital or health problems can cause an employee to become dishonest. If you are a supervisor of a mail center, you need to be alert for personality changes that might signal such a problem. Take precautions to protect your company from theft. Reducing an employee's opportunity to steal is an essential prevention technique.

Who should accept and drop off mail and other valuables?

Only authorized employees should be assigned to accept mail at the office. Give the Post Office a list of authorized employees for its file. When your mail center personnel change, update the employee list immediately and provide a copy to the Post Office to avoid having mail given to an unauthorized person. It is crucial to keep the list current, especially when you process accountable mail, such as registered and certified letters.

If your company sends out or receives valuables, vary the time of day and direction of travel between your office and the Post Office. Check periodically to determine if your mail couriers are making unauthorized stops or are leaving your mail unattended in unlocked delivery vehicles.



Label 33, *Warning! Penalty for Damage to Mailboxes and Theft*

Is the physical layout of your mail center vulnerable to theft?

A properly designed physical layout for your mail center is in itself a preventive security measure. The following table provides guidlines for the layout of your mailroom.

Measures to Deter Theft by Enhancing the Physical Layout of Your Mail Center

Step	Action
1.	Make all work areas visible to supervisors.
2.	Use one-way glass, closed-circuit video surveillance cameras, or elevated supervisor stations.
3.	Eliminate desk drawers and similar places of concealment.
4.	Ensure adequate supervision of mail center employees, who may have access to thousands of dollars worth of merchandise, remittances, and company credit cards.
5.	Control access to your mail center and handling areas. Use of sign-in/out sheets, card key access control systems, and photo identification badges are all effective security procedures. Extend this control to all employees including cleaning and maintenance personnel.
6.	Enforce limited access to the mail center. Only authorized employees should be allowed in the working areas of the mail center.
7.	Use a counter or a desk to separate the area where employees pick up mail from the rest of the mail center.

Theft Prevention Tips

Mail Center Activity and Equipment	Action
Registered Mail	Keep Registered Mail separate from other mail. Require employees to sign for Registered Mail to establish accountability. Set up a log to track Certified Mail™ and Registered Mail items to record the date a piece of mail is received, the type of mail, and the Postal Service's control number. Have the person receiving the mail sign and date the entry log. This step provides a reliable tracking system.
Petty Cash	Establish adequate controls to identify responsibility for losses that may occur. Never keep postage stamps in unlocked drawers.
Postage Meter Security	Restrict access to postage meters to authorized personnel. Do not allow employees to run personal mail through postage meters as it can result in theft of company funds. You can get an accurate account of postage and its purpose when only authorized employees operate postage meters. Keep your postage meter locked when not in use. Have a trusted employee maintain a record of meter register readings. This helps detects unauthorized, after-hours use of the meter and aids you in obtaining a refund if your postage meter malfunctions.

Mail Center Activity and Equipment	Action
Advance Deposits	Avoid paying for business reply, postage due, or other postal costs from petty cash. Using a petty cash drawer can provide a theft opportunity for a dishonest mail center employee. Establish an advance deposit account with the local Post Office. Companies that prefer using petty cash can protect themselves against theft by requiring receipts from the Post Office for postage paid and by checking mail to ensure that it balances with receipts.
Use of Authorized Depositories	Do not leave your tray or sack of mail on a curb next to a full collection box. If this is a problem for your company, contact your postmaster to resolve. This could prevent your mail from being lost or stolen.
Outgoing Mail	Conduct periodic checks of outgoing mail against customer order lists. This step can detect dishonest employees who are putting their name and address on orders being shipped out to legitimate customers. This is a very difficult crime to detect without someone reviewing outgoing mail. Also, while checking outgoing mail, you can see if your employees are using metered postage for personal mail.
Outside Mail Preparation Services	Postal Inspectors have found that some mail preparation service operators have either pocketed fees without entering the material into the mail or have grossly overcharged advertisers for postage on the mailings. Your local Post Office's Business Mail Entry Unit uses the PS Form 3600 series to maintain an independent record of bulk mailings. Any questions related to the quantity, costs, and date of a particular mailing can be verified by contacting this unit.
Incoming Mail	Clearly label depositories used to receive incoming mail and those designated for outgoing mail. Label 33, *Warning Penalty for Damage to Mailboxes and Theft*, available from your local Post Office or the Postal Inspection Service (see sample on page 5), can be used to highlight the fact that material in such receptacles is protected by federal law.
Missent Mail	Implement a system to handle misdelivered or missent mail. Immediately return all such mail to the Post Office.

Always report suspected mail losses to the Postal Inspection Service by calling 877-876-2455 or online at *http://postalinspectors.uspis.gov.* Losses are charted by the Postal Inspection Service to identify problem areas and assist Postal Inspectors in identifying thieves.

Mail Center Security Checklist

- ☐ Screen mail center personnel.
- ☐ Clearly label authorized receptacles for U.S. Mail.
- ☐ Ensure that mailroom location, furniture, and mail flow provide maximum security.
- ☐ Install alarms and surveillance equipment.
- ☐ Limit mailroom access to authorized personnel.
- ☐ Eliminate mail distribution delays.
- ☐ Protect postage and meters from theft or unauthorized use.
- ☐ Lock high-value items overnight.
- ☐ Verify and secure accountable items.
- ☐ Maintain control of address labels.
- ☐ Securely fasten labels to mail items.
- ☐ Check that postage meter strips do not overlap labels.
- ☐ Ensure that labels and cartons do not identify valuable contents.
- ☐ Include a return address, and duplicate the return address label inside packages.
- ☐ Ensure presort and ZIP + 4® savings are taken when applicable.
- ☐ Prepare parcels to withstand transit.
- ☐ Use containers and sacks when possible.
- ☐ Do not leave mail in an unsecured area, and deliver outgoing mail directly to Postal Service custody.
- ☐ Separate employee parking from mail delivery area.
- ☐ Immediately report lost or rifled mail to Postal Inspectors.
- ☐ Ensure that supervisor can see all employees and work areas.
- ☐ Screen contractors who provide delivery services.
- ☐ Eliminate any unnecessary stops by your delivery vehicles.
- ☐ Establish procedures for handling unexplained or suspicious packages.
- ☐ Periodically test mail for loss and or quality control.
- ☐ Verify Postal Service receipts for meter settings against authorized amounts.
- ☐ Regularly check postage meters.

Protect Your Business from Package Bombs and Bomb Threats

Revenge is the motivation that most often triggers a package bomb or a bomb threat.

The chance that you will receive a bomb through the mail is about 1 in a billion. Nonetheless, you should be aware of the proper guidelines to handle such incidents.

What motivates people to send package bombs? People often think of a mail bomber as a person motivated by radical political beliefs. This stereotype is incorrect. If you adhere to this stereotype, you may improperly assess and respond to a bomb threat.

Jilted spouses or lovers may seek revenge at the end of their romantic involvement. Former business partners or employees may seek revenge when a business relationship goes sour or when business reversals cause layoffs or firings. Law enforcement officers and members of the judiciary have been targeted for bombs and bomb threats by individuals seeking revenge for having been investigated or prosecuted.

Package bombs usually target specific individuals. Placed bombs, however, are generally intended to disrupt workplaces and injure indiscriminately. Bomb threats may target either individuals or organizations.

How vulnerable is your workplace to a bomb threat?

The chances of your workplace receiving a package bomb are extremely remote. The chances are greater of receiving a telephoned bomb threat or finding a suspicious and potentially harmful bomb placed at your workplace or on your property.

The vulnerability of you and your workplace depends on a variety of factors, both internal and external. No individual or company is completely immune from attack. The security officer and top management should meet to evaluate the probability of your company or its personnel becoming targets for package bombs and bomb threats.

Postal Inspectors recommend you consult with security experts about terrorist tactics and to receive a vulnerability assessment. The Postal Inspection Service can provide information about establishing a secure mail center and detecting package bombs. Contact a Postal Inspector near your workplace. In addition, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) provides information about bomb threats and physical security planning on its Web site at *www.atf.treas.gov.*

Since most explosive devices are placed, not mailed, your security plan must include controls over individuals who can physically access and move about your workplace and its immediate surroundings. Having such controls can reduce your company's risk.

You should ask the following questions during your assessment. The questions can be used to develop information that would help identify company officers or employees who could be targeted or organizations that may attempt a bombing:

- **Foreign terrorism.** Does your company have foreign officers, suppliers, or outlets? If so, in what countries? Are you doing business in countries where there is political unrest and civil strife, or where terrorist organizations operate? Has your company refused to do business with, withdrawn from, or failed to successfully negotiate business contracts with companies, organizations, or governments within the last 2 years that are affiliated with current terrorists or that represent countries suffering domestic unrest? Does your company manufacture or produce weapons or military support items for the international arms trade that would normally bear markings identifying the organization as the manufacturer?
- **Domestic hate groups.** Is your company a high-profile organization whose services, research, or products are the subjects of public controversy? (See Resources section for the Web site address of an organization that tracks hate groups.)
- **Workplace violence.** Has your company experienced a recent downsizing, take-over, or reorganization requiring layoffs? Has any employee complained of being physically abused, harassed, or of being stalked? Has any employee made threats to harm any other employee or the company itself?

Note: Care must be given not to violate an individual employee's privacy. All information should be treated as extremely sensitive. This information should be shared with the mail center security coordinator in the event that a suspicious package is received. The information should not be disseminated to other employees.

U.S. Postal Inspectors regularly conduct biohazard drills at postal facilities nationwide.

Enhance the Physical Security of Your Workplace

Step	Action
1.	Have security guards greet all visitors and examine personal belongings being brought into the building or office area.
2.	Restrict access to the facility or office through locked or guarded entryways.
3.	Keep storage rooms, boiler rooms, telephone and utility closets, and similar potential hiding places locked or off-limits to visitors.
4.	Use easily distinguishable ID badges for staff and visitors.
5.	Require visitors to be accompanied by staff employees to and from the office or facility entrance.
6.	Request visitors to display IDs to security personnel when they sign in.
7.	Keep logs on the arrival and departure times of all visitors.
8.	Consider hiring a certified protection professional to evaluate your company's personnel and physical security safeguards.

Establish a Package Bomb-Screening Program*

Step	Action
1.	Evaluate your organization to determine if your business or an employee is a potential target.
2.	Appoint a mail center security coordinator and an alternate to be responsible for your screening plan and to ensure compliance with it.
3.	Establish lines of communication between the mail center security coordinator, management, and the security office.
4.	Develop screening procedures for all incoming mail or package deliveries. Train employees in those procedures.
5.	Develop handling procedures for items identified as suspicious and dangerous.
6.	Develop procedures for confirming the contents of suspicious packages identified through screening.
7.	Establish procedures for isolating suspicious packages.
8.	Train mail center, security, and management personnel to validate all phases of your package bomb-screening program.
9.	Conduct unannounced tests of mail center personnel.

*You may order a copy of the Postal Inspection Service's Poster 84, *Suspicious Mail,* by calling 800-332-0317 and selecting option 4. Enter your phone number, then select option 4 again, and wait for an operator to take your call.

What are the roles and responsibilities of the mail center security coordinator in relation to package bomb safety?

Postal Inspectors recommend including the mail center manager, or a designee, as a member of the planning group that develops your Bomb Threat Response Plan. Corporate management should ensure that the mail center security coordinator or an alternate are mature, responsible, and emotionally stable. These individuals should be trained in the Bomb Threat Response Plan.

What about bomb threats received in writing?

Written threats provide physical evidence that must be protected from contamination. Written threats and any envelopes in which they are received should be placed under clear plastic or glassine covers. All the circumstances of their receipt should be recorded.

What about bomb threats received by telephone?

Telephone threats offer an opportunity to obtain more detailed information, perhaps even the caller's identity. For that reason, the telephone receptionist or others who take calls from the public should be trained to remain calm and to solicit as much information as possible. The bomber's intentions may be to damage property, not to injure or kill anyone. If so, the person receiving the call may be able to obtain useful information before the caller ends the conversation.

Response to Bomb Threats Received By Telephone

Persons	Action
Receptionist	Keep the caller on the line, ask him or her to repeat the message several times, and gather additional information, such as caller ID. Write down the threat verbatim, using the caller's own words, and record any additional information. Do not hang up on the caller under any circumstances.
Corporate security and management	Decide on the proper response, such as evacuation. Notify the police and fire department immediately.

Sample questions that a trained telephone receptionist should ask during a telephoned bomb threat are:

- What kind of bomb is it?
- What does it look like? Please describe it.
- Where is it located? Can you give us the office and floor number and building location?
- What will cause it to detonate?
- Many innocent people may be hurt. Why are you doing this?
- What is your name and address?

What should employees do if they receive an unexpected package?

Because of the increased sophistication of mail and placed bombs, fewer of the devices can be readily identified by examining the exterior of the package. Remind employees: If you're not expecting a package, be suspicious.

If you receive an unexpected package:

- First, check the return address.
- If you do not recognize the return address, contact the security office.
- The security office should attempt to contact the sender.
- Do not open the package until verification proves that it is harmless.

What should the mail center coordinator do after encountering a suspicious package during screening?

Step	Response	Action
1.	**Inquire**	Ask the employee who found the suspicious package to write down the specific recognition point in the screening process that caused the alert (e.g., excessive postage, no return address, rigid envelope, lopsided appearance, or strange odor).
2.	**Isolate**	Isolate the area where the package was found—do not touch it.
3.	**Alert**	Alert employees that a suspicious package has been found, what the points of recognition are, and to remain clear of the isolation area.
4.	**Notify**	Inform management and security that a suspicious item has been detected by the screening process.
5.	**Document**	Without touching the package, record from each visible side of the item all available information (name and address of addressee and of sender, postmark, cancellation date, types of stamps, and any other markings or labels found on the item). Copy information with exact spelling and location given on item.
6.	**Inform**	Inform the police and Postal Inspectors (if a mailed item) of all information recorded from the suspect item.

What should management or security staff do after they are told of a suspicious package by the mail center coordinator?

Step	Response	Action
1.	**Document**	Record all information about the suspicious package in an incident log. If possible, photograph all sides of the package without moving it, as it rests in the holding container. The exact details of the package markings will be made available for study and use by the bomb scene officer.
2.	**Contact and verify**	Before calling police, try to find out if the package addressee knows about the item. If someone can identify it, you may open the package with relative safety. Try to contact the sender as indicated on the return address. If the sender must be contacted to identify the item, a management decision must be made as to the reliability of the information.
3.	**Notify**	If the return addressee is fictitious or if you cannot locate the sender within a reasonable period of time, notify police and Postal Inspectors (if a mailed item). Tell them you detected a suspicious package, and it is in an isolated area. Provide authorities with the location of the package and the name of the mail center coordinator or security officer. Notify appropriate management of the incident.
4.	**Assist**	Stand by to offer assistance to police and Postal Inspectors.

What are some questions to ask the addressee or sender during the verification process?

Some sample questions to ask are the following:

- Is the addressee familiar with the name and address of the sender?
- Is the addressee expecting a package from the sender? If so, what is the approximate size of the item?
- Ask the sender to fully explain the circumstances surrounding the sending of the parcel and to describe the contents. At this point, management and security must make a decision whether to proceed to open the parcel or not.
- If the sender is unknown, is the addressee expecting any business correspondence from the city, state, or country of origin of the package?

- Is the addressee aware of any friends, relatives, or business acquaintances currently on vacation or on business trips in the area of the return address?
- Has the addressee purchased or ordered any merchandise from a business whose parent organization might be located in the area of the return address?

If the verification process determines that the sender is unknown at the return address or that the return address is fictitious, consider this scenario as an indication that the package may be dangerous.

What is the importance of testing contingency plans?

The Postal Inspection Service cannot overemphasize the need to test contingency plans with mock suspicious parcels placed in the mail center or elsewhere in the facility. The tests should be conducted in a manner that does not alarm employees. Dress rehearsals help ensure that your lines of communication function as planned and that each person who has a role to play knows his or her part.

Test the efficiency of your emergency contingency plan by conducting scheduled tests. Hold post-test meetings to address problems and resolve them before the next test.

Protect Your Mail Center from Chemical, Biological, or Radiological Threats

Biological threats may include the following substances:

- **Chemical.** Any substance designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors, such as mustard gas, nerve agents, and sarin gas.
- **Biological.** Any substance involving a disease organism, such as smallpox, botulinum toxin, anthrax, and ricin.
- **Radiological.** Any substance designed to release radiation.

Anthrax

Anthrax is a bacterial disease caused by Bacillus (B.) anthracis. In humans, three types of anthrax infections can occur based on the route of exposure.

For detailed information on Centers for Disease Control (CDC) recommendations on protective gear for your employees, contact your local CDC representative or visit their Web site at *www.cdc.gov.*

Type	Exposure	Transmittal and Characteristics	Symptoms
Cutaneous	Skin	The most common, naturally occurring anthrax infection. May be transmitted via skin contact with contaminated meat, wool, hides, or leather from infected animals. Incubation is from 1 to 12 days. Infection occurs through scratches or skin abrasions.	Infection appears as a raised bump resembling a spider bite. Within 1 to 2 days, it develops into a blister and then a painless ulcer, with a black necrotic (dying) area in the center. The lesion may cause fever, malaise, and headache. Lymph glands in the area may swell.
Inhalation	Inhalation	Anthrax spores must be aerosolized to cause inhalational anthrax. It is contracted by inhaling spores and occurs in workers handling infected animal hides, wool, and fur. The number of spores that cause infection is unknown. Incubation period is unclear, but may range from 1 to 7 days or up to 60 days.	Inhalation anthrax resembles a viral respiratory illness. Initial symptoms include sore throat, mild fever, muscle aches, and malaise. Symptoms may progress to respiratory failure and shock with meningitis. After incubation of 1 to 7 days, the onset of inhalation anthrax is gradual.
Gastrointestinal	Ingestion	Gastrointestinal anthrax usually follows consumption of raw or undercooked contaminated meat and has an incubation period of 1 to 7 days.	Causes acute inflammation of the intestinal tract. Initial signs are nausea, loss of appetite, vomiting, fever followed by abdominal pain, vomiting of blood, and severe diarrhea.

How to Limit Exposure to a Suspicious Substance in the Mail

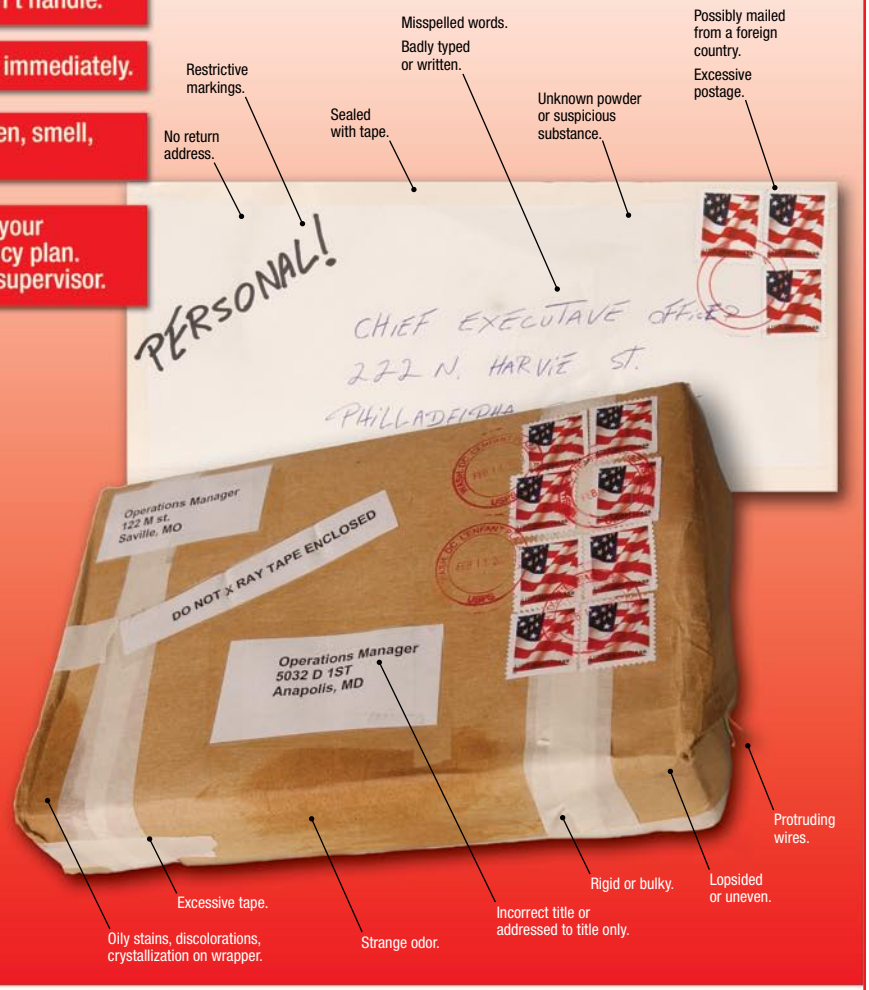
Step	Action
1.	Develop an emergency plan for steps in response to a known or a possible exposure to a suspicious substance.
2.	Train workers in how to recognize and handle a suspicious piece of mail.
3.	Identify a single point of contact to open mail.
4.	Screen all mail for suspicious packages.
5.	Do not open mail in an area where other personnel are present.
6.	If appropriate, have gloves available for employees who handle mail.

SUSPICIOUS MAIL OR PACKAGES

Protect yourself, your business, and your mailroom.

If you receive a suspicious letter or package:

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



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

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

UNITED STATES POSTAL SERVICE.

To order this poster, call 1-800-332-0317.

Poster 84
September 2006
PSN 7690-07-000-7097

What should you do if you receive a suspicious substance by mail?

Step	Action
1.	Notify your supervisor or immediately contact Postal Inspectors, local police, the safety office, or a designated person.
2.	Isolate the damaged or suspicious mailpiece or package. Cordon off the immediate area.
3.	Ensure that all persons who have touched the mailpiece wash their hands with soap and water.
4.	List all persons who have touched the mailpiece. Include contact information and have this information available for the authorities. Provide the list to the U.S. Postal Inspection Service.
5.	Place all items worn when in contact with the suspected mailpiece in plastic bags and have them available for law enforcement agents.
6.	Shower with soap and water as soon as practical.
7.	Call your local police department at 911.
8.	Call a Postal Inspector at 877-876-2455 or at the number provided by a Postal Inspector contact to report that you've received a letter or parcel in the mail that may contain harmful chemical, biological, or radiological substances.

Ricin

There have been a few incidents of mail purporting to contain the chemical poison ricin. Ricin is made from castor beans, a plant that is plentiful in many areas of the world, including the United States. Castor beans are used to make castor oil and other beneficial products used for many purposes. In fact, castor oil is often used in the manufacture of paper, including paper used as envelopes. Trace amounts of castor are present in many common items. The process for making ricin from castor beans is rather difficult and quite dangerous. Common first responder field kits have been known to show positive test results for the poison ricin in substances containing harmless amounts of castor bean pulp or derivatives. A positive field test for ricin may result from castor bean products, even if there is no refined ricin. To be dangerous, ricin must be injected, inhaled, or ingested.

Safety Checklist for Low- and Moderate-Risk Facilities

- ☐ Appoint a mail security coordinator and ensure the position is supported by senior management.
- ☐ Establish standard operating procedures for the mailroom that include security procedures, and implement a regular review of the procedures.
- ☐ Identify proper protocols for emergencies such as a fire, the presence of hazardous materials, or other environmental or safety issues; develop and maintain action plans to address each hazard; and provide current emergency contact information.
- ☐ Display procedures for handling suspicious mail or packages.
- ☐ Provide training for mail handling personnel on policies and procedures for mail security and emergency protocols.
- ☐ Perform in-depth background checks when hiring new personnel and institute a probationary period for new hires.
- ☐ Limit mailroom access to employees wearing proper identification badges; uniquely identify and escort visitors; and encourage personnel to challenge unknown people in the work area or facility.
- ☐ Ensure strict accountability for all mailroom locks and keys.
- ☐ Ensure adequate lighting for the area where mail is handled and the exterior of your building.
- ☐ Use closed circuit television (CCTV) cameras to record and store surveillance of operation areas and exterior of your building.
- ☐ Install an intrusion-detection system at your facility.
- ☐ Meet with local first responders including police, fire department staff, Centers for Disease Control (CDC) staff, the Occupational Safety and Health Administration (OSHA), and the General Services Administration (GSA) to establish familiarity with responsible groups and identify best local practices.
- ☐ Provide mailroom employees with CDC-approved personal-protection equipment as appropriate.

Safety Checklist for High-Risk Facilities

- ☐ Appoint a mail security coordinator and an alternate coordinator, and ensure the position is supported by senior management.
- ☐ Form a mail security response team, depending on the size of mail center staff.
- ☐ Maintain updated contact information for response-team personnel and identify each person's responsibilities.
- ☐ Keep detailed logs of visitor arrivals and departures, and restrict drivers and deliveries to a specific area.
- ☐ Establish standard operating procedures for the mailroom that include security procedures, and implement a regular review of the procedures. Consider storing backup copies of the procedures at an off-site location.
- ☐ Identify proper protocols for emergencies such as a fire, the presence of hazardous materials, or other environmental or safety issues; develop and maintain action plans to address each hazard; and provide current emergency contact information.
- ☐ Develop a business continuity plan in the event of an emergency, including an alternate location for mail operations.
- ☐ Prepare incident reports after every incident, and include a review for corrective action or process improvement.
- ☐ Display procedures for handling suspicious mail or packages.
- ☐ Provide training for mail handling personnel on policies and procedures for mail security and emergency protocols.
- ☐ Perform in-depth background checks when hiring new personnel and institute a probationary period for new hires.
- ☐ Ensure that employment agencies provide your organization with pre-screened individuals.
- ☐ Provide a separate secure area for employees' personal items, such as coats and purses. Prohibit personnel from taking personal items into the main work area.
- ☐ Limit mailroom access to employees wearing proper identification badges; uniquely identify and escort visitors; and encourage personnel to challenge unknown people in the work area or facility.
- ☐ Ensure strict accountability for all mailroom locks and keys.
- ☐ Hire or designate security personnel for the mail center area.
- ☐ Ensure adequate lighting for the area where mail is handled and the exterior of your building.
- ☐ Install closed circuit television (CCTV) cameras at entrances and around the exterior of your building. Use CCTV to record and store surveillance of indoor and outdoor areas.
- ☐ Install an intrusion-detection system.

Safety Checklist for High-Risk Facilities

- ☐ Meet with local first responders including police, fire department staff, Centers for Disease Control (CDC) staff, the Occupational Safety and Health Administration (OSHA), and the General Services Administration (GSA) to establish familiarity with responsible groups and identify best local practices.
- ☐ Establish hazmat-response plans and a relationship with hazmat emergency-response personnel for 24/7 coverage and contact, as appropriate.
- ☐ Maintain and display local first responder phone numbers to call in an emergency such as for the police, fire department, and U.S. Postal Inspection Service at 877-876-2455.
- ☐ Provide mailroom employees with CDC-approved personal-protection equipment as appropriate.
- ☐ As your level of risk assessment dictates and your budget allows, you should augment your mail security programs with additional countermeasures.

Additional Protective Measures for High-Risk Facilities

- Consider purchasing bomb-detection equipment or a K-9 unit.
- X-ray all incoming mail and store mail in containment containers until testing is concluded.
- Use a “safe air” room for processing and conduct monthly swab testing of the mail handling area.

Engineering controls provide the best means of preventing workers from exposure to potential hazardous aerosolized particles and potential explosive devices. To provide protection from chemical, biological, and radiological hazards consider:

- Using an industrial vacuum cleaner equipped with a high-efficiency particulate air (i.e., HEPA) filter for cleaning. Do not clean machinery with compressed air (i.e., blow-down/blow-off).
- Installing air curtains (using laminar air flow) in areas where large amounts of mail are processed.
- Installing filters in the building’s HVAC systems (if feasible) to capture aerosolized spores.

Quick Reference

For suspicious packages and letters:

If you are unable to verify mail contents with the addressee or sender:

Do not open it.

Treat it as suspect.

Isolate it—don't handle.

Contact building security, if available.

Call the police by dialing 911.

Call Postal Inspectors at 877-876-2455 if the item was received in the mail.

For a bomb:

Evacuate immediately.

Call police by dialing 911.

Call Postal Inspectors at 877-876-2455 if the item was received in the mail.

Call fire department and hazmat unit.

For chemical, biological, or radiological contamination:

Isolate it—don't handle.

Wash your hands with soap and warm water.

Call police by dialing 911.

Call Postal Inspectors at 877-876-2455 if the item was received in the mail.

Call fire department and hazmat unit.

For air contamination:

Turn off fans or ventilation units and shut down the air handling system in the building, if possible. Leave area immediately and close the door, or section off the area to prevent others from entering it.

Notify your building security official or a supervisor and call 911.

If possible, list all people who were in the room or area. Give the list to public health authorities for any needed medical advice and to law enforcement authorities for follow-up.

Publications for Mail Center Security

U.S. Postal Inspection Service publications are available for viewing or printing at its Web site, or you may order them by calling the Postal Service's Material Distribution Center toll-free at 800-332-0317 and selecting option 4. Enter your phone number, then select option 4 again and wait for an operator to take your call. There is a minimal charge for printed material.

Poster 84, *Suspicious Mail*

Notice 71, *Bombs by Mail*

Publication 54, *Notice of Bomb Threat*

Publication 280, *Identity Theft*

Additional Resources

The U.S. Postal Inspection Service can provide more information about establishing a secure mail center and protecting your business against theft. Postal Inspectors can perform on-site security surveys for larger firms and assist with training in security protocols.

http://postalinspectors.uspis.gov/

The Center for Disease Control and Prevention (CDC) is a U.S. Public Health Service agency that monitors and works to prevent disease outbreaks. CDC also establishes protocols related to biological, chemical, and radiological threats.

http://www.cdc.gov

The Federal Bureau of Investigation (FBI) investigates cases related to weapons of mass destruction and terrorist attacks.

http://www.fbi.gov

The Federal Emergency Management Agency (FEMA) is the federal agency responsible for disaster mitigation, preparedness, response, and recovery training.

http://www.fema.gov/hazard/hazmat/index.shtm

The Occupational Safety and Health Administration (OSHA) is the federal agency charged with the enforcement of safety and health legislation.

http://www.osha.gov

The Southern Poverty Law Center provides a list of active hate groups based on information gathered from publications, citizens' reports, law enforcement agencies, field sources, and news reports.

http://www.splcenter.org/

Conclusion

Regardless of the size or potential risks of a mail center, basic mail center security can protect your employees, the public, and your organization's assets and operations. By demonstrating a strong interest in security, you may deter potential criminal activity by employees or outsiders.

Some of the recommendations in this guide may not apply to your mail center, so it is important that you assess your organization's needs — whether it is a large dedicated mail processing facility or a desk at a small business — and apply the practices that are reasonable and prudent.

In the event a suspicious substance is found in or around mail, Postal Inspectors who are certified specialists conduct field screening to identify the substance.

Publication 166
March 2008
PSN 7690-05-000-4890