WHO PROTECTS YOUR MAIL?

UNITED STATES POSTAL INSPECTION SERVICE

GUIDE TO MAIL CENTER SECURITY

WHO PROTECTS **YOUR MAIL?**

GUIDE TO MAIL CENTER SECURITY

YOUR RISK LEVEL 3
PHYSICAL SECURITY OF YOUR WORKPLACE

YOUR MAIL CENTER 8
EMPLOYEE ROLES AND RESPONSIBILITIES

MAIL THEFT 11
SECURING YOUR MAIL CENTER FROM THEFT

LETTER OR PACKAGE BOMBS AND BOMB THREATS 13
ESTABLISH A SECURITY AND BOMB-SCREENING PLAN

CHEMICAL, BIOLOGICAL, OR RADIOLOGICAL THREATS 21
SECURING YOUR MAIL CENTER FROM HAZARDOUS SUBSTANCES

REFERENCES 25
CHECKLISTS AND ADDITIONAL RESOURCES

WHO PROTECTS **YOUR MAIL?**

We Do! We're the U.S. Postal Inspection Service

The U.S. Postal Inspection Service is one of the Postal Service™'s best-kept secrets. Many customers aren't even aware of what we do. So we want to take you behind the scenes and tell you how we can help you protect your business by securing your mail center.

What we do is truly unique. As a federal law enforcement agency with more than 200 years of experience, our U.S. Postal Inspectors investigate every aspect of mail-related crime—including mail theft, mail fraud, and mail containing dangerous items or substances. The work we do, every day, assures millions of postal customers they can depend on the security, privacy, and reliability of U.S. Mail. The U.S. Postal Inspection Service adds a value no other mail service can provide.

Call a Postal Inspector near you!
877-876-2455 (press 5)
postalinspectors.uspis.gov

Working Globally

Postal Inspectors travel the world to train foreign postal administrations in the latest safety protocols, educating them in emergency responses to ensure readiness for all hazards. Long-known as experts in all matters related to mail security, our Chief Postal Inspector was made chairman of the Universal Postal Union's Postal Security Group, directing Postal Inspectors to extend their reach beyond U.S. borders to secure the international mail network—and ensure the safety of American citizens.

Working for You

Every business has different needs. This guide provides general recommendations from Postal Inspectors to cover a broad range of businesses. Invite a Postal Inspector to visit your business and review your mail center operations. Their security reviews can pinpoint problems that could lead to mail theft or open the door to other security issues. You can ask an Inspector to schedule a workshop for your mail center employees to educate them on how to handle suspicious mail and deliver tips to improve security for your business and your employees.

Thanks to us, the U.S. Postal Service® delivers the nation's mail more safely and more securely than any other country in the world. And it's all included in the price of postage.

SECURITY: IT COMES WITH THE STAMP®

YOUR RISK LEVEL

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

Mailrooms may have 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; other measures will require some planning, action, and financing.

Start your risk assessment by evaluating these areas:

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

Consider the nature of your business. If your organization could attract political or 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's also important to be aware of your customers and the types of business they conduct. International businesses or controversial professions or services can significantly heighten risks. 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. Postal Inspectors advise you to develop screening procedures for all incoming deliveries, including those from private delivery firms, such as FedEx and UPS. All employees must be trained in safe mail handling procedures and should understand the importance of following protocols.

In any case, it's important that you're familiar with your local and state emergency response capabilities.

When Mail is Federally Protected

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's received at the organization. For this reason, the Postal Inspection Service discourages staff 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 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.

Centralizing Your Mail Handling Operations

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. It also reduces costs by eliminating redundancies in locations, staff, and equipment. Establishing a trained staff to work at a single location increases the efficiency of your operations.

Enhancing the Physical Layout of Your Mail Center

Properly designing a physical layout for your mail center is in itself a preventive security measure.

TIPS FOR THE LAYOUT OF YOUR MAILROOM

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

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

This is a general guide to help you establish sound security protocols for your business.

CHECKLIST FOR MAIL CENTER SECURITY

- ☐ 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 mailed items.
- ☐ 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 supervisors 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 letters and packages.
- ☐ Periodically test mail for loss and for quality control.
- ☐ Verify Postal Service receipts for meter settings against authorized amounts
- ☐ Regularly check postage meters.

Enhancing the Physical Security of Your Workplace

These guidelines will help ensure you offer a safe work environment for your employees.

- If your workplace has access control, don't allow employees to gain entrance by "piggy backing" their way in behind others.
- Have security guards greet all visitors and examine personal belongings brought into the building or office area.
- Restrict access to your workplace through locked or guarded entryways.
- Keep storage rooms, boiler rooms, telephone and utility closets, and similar potential hiding places locked or off-limits to visitors.
- Use distinct and separate ID badges for staff and visitors.
- Require visitors to be accompanied by staff employees to and from the office or facility entrance.
- Request visitors to display IDs to security personnel when they sign in.
- Keep logs on the arrival and departure times of all visitors.
- Consider hiring a certified protection professional to evaluate your company's personnel and physical security safeguards.

YOUR MAIL CENTER

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 ROLES & RESPONSIBILITIES

ROLE	RESPONSIBILITY
OVERSIGHT AND TRAINING	• Oversees screening process and ensures all deliveries are channeled through the mail center. • Trains employees in detecting suspicious letters and packages, verifications, safe handling, and communications with security and management in any crisis.
COMMAND	• Assumes command of the situation when a suspicious letter or package is identified by mail center employees during the screening process.
SAFETY ENFORCEMENT	• Ensures that personnel who detect suspicious mail place a safe distance between themselves and the item and that employees don't cluster around the item. • Ensures that only mail center employees have access to the mail.

YOU SHOULD CONSIDER THESE AREAS OF CONCERN:

HOW EXTENSIVE IS YOUR PRE-EMPLOYMENT SCREENING?

When you conduct pre-employment screening, check the job candidate's criminal records, have him/her undergo a drug-screening test, perform a credit inquiry on him/her, and verify his/her 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?

Employees' personal situations 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. Mail center supervisors must be alert for personality changes that could signal problems. Take precautions to protect your company from theft: Reducing the 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 your local Post Office™ a list of authorized employees to keep on file. If staff changes, update the list immediately and inform the Post Office to avoid unauthorized staff from receiving mail. It's 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 leaving mail unattended in unlocked delivery vehicles.

Train Your Mail Center Staff

Education in and knowledge of security protocols are essential to preparedness. Mailroom employees must be aware of their surroundings and the mail they handle. Carefully design and vigorously monitor your security program to reduce risks for your organization.

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

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

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

All employees in your organization should understand your mail security procedures. This helps instill employee confidence in the safety of the letters or packages delivered to their desks.

MAIL THEFT

While you should properly address 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 any valuable information about your company contained in sensitive mail.

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.

REPORT MAIL THEFT, TAMPERING, OR VANDALISM OF THIS MAILBOX

1-877-876-2455
select option 3

UNITED STATES POSTAL INSPECTION SERVICE

postalinspectors.uspis.gov

WARNING: WILLFUL DAMAGE TO MAILBOXES OR THEFT OF MAIL ARE FEDERAL CRIMES (FELONIES) PUNISHABLE BY FINE OR IMPRISONMENT OR BOTH. (18 USC 1705 & 1708)

Label 33, May 2009 PSN 7690-01-000-9043

Losses are charted by the Postal Inspection Service to identify problem areas and assist Inspectors in tracking down thieves. Report suspected mail losses to Postal Inspectors by calling 877-876-2455 (press 3) or at *postalinspectors.uspis.gov.*

PREVENTING THEFT IN YOUR MAIL CENTER

REGISTERED MAIL	Keep Registered Mail separate from other mail. Require employees to sign for Registered Mail™ to establish accountability. Use a log to track Certified Mail® and Registered Mail to record the date it's received, the type of mail, and the Postal Service's control number. The person receiving the mail must sign and date the log. This 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 detect unauthorized, after-hours use of the meter and helps you obtain a refund if your meter malfunctions.
ADVANCE DEPOSITS	Avoid paying for business reply, postage due, or other postal costs from petty cash. A petty cash drawer can provide a theft opportunity for dishonest mail center employees. Set up an advance-deposit account with your 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 it balances with receipts.
USE OF AUTHORIZED DEPOSITORIES	Don't leave trays or sacks of mail on a curb next to a full collection box. If this is a problem, contact your postmaster to resolve. This could prevent your mail from being lost or stolen.
OUTGOING MAIL	Periodically compare outgoing mail against customer order lists. This can detect dishonest employees using their name and address for orders shipped to legitimate customers. This is a difficult crime to detect unless someone reviews outgoing mail. When checking outgoing mail, see if employees are using metered postage for personal mail.
OUTSIDE MAIL PREPARATION SERVICES	Postal Inspectors have found some mail preparation service staff pocket fees without entering the material into the mail or have grossly overcharged advertisers for postage. Your local Post Office's Business Mail Entry Unit uses the PS Form 3600 series to maintain a record of bulk mailings. Any questions related to quantity, costs, and the date of a mailing can be verified by contacting this unit.
INCOMING MAIL	Clearly label depositories used to receive incoming mail and outgoing mail. Use PS Label 33, *Report Mail Theft, Tampering, or Vandalism of this Mailbox* (see a sample on page 11), available from your local Post Office or the Postal Inspection Service, to alert employees that material in such receptacles is protected by federal law.
MISSENT MAIL	Have a system to handle misdelivered or missent mail. Immediately return all such mail to the Post Office.

LETTER OR PACKAGE BOMBS AND BOMB THREATS

How vulnerable is your workplace to a bomb threat?

The chance that your workplace will receive a letter or package bomb is 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.

What motivates people to send letter or 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.

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

Bombs can be designed for mailing in many shapes and sizes—not just packages. Even letter-size mail or flats can contain dangerous substances.

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

Identifying the Right Security Plan

Your vulnerability and that of your workplace depends on many factors, both internal and external. No individual or company is completely immune from attack. Your security officer and top managers should meet to evaluate the probability that your company or its personnel become targets for mailed 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 guide you in establishing a secure mail center and detecting letter and package bombs. Call a Postal Inspector near your workplace. The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) has additional information on bomb threats and physical security planning at *atf.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. These controls can reduce your company's risk.

Ask the questions shown on the next page during your assessment to develop information that will 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? Check *splcenter.org* for the Southern Poverty Law Center, which 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 stalked? Has any employee made threats to harm any other employee or the company itself?

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

Handling and Processing Mail Safely

Screen all mail and packages for suspicious items when they first arrive at your mailroom for sorting. Staff who sort 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 letter or package is often not the intended recipient.

Prominently display a list of suspicious letter and package indicators in your mailroom and provide a copy of the list to all staff to ensure they're familiar with it. The Postal Inspection Service's Poster 84, *Suspicious Mail or Packages*, illustrates key characteristics of a suspicious or potentially dangerous mail item.

ESTABLISH A LETTER AND PACKAGE BOMB-SCREENING PROGRAM

- Evaluate your organization to determine if your business or an employee is a potential target.
- Appoint a mail center security coordinator and an alternate to be responsible for your screening plan and to ensure compliance.
- Establish lines of communication between the mail center security coordinator, management, and the security office.
- Develop screening procedures for all incoming letter and package deliveries. Train employees in the procedures.
- Develop handling procedures for items identified as suspicious and dangerous.
- Develop procedures for confirming the contents of suspicious letters and packages identified through screening.
- Establish procedures for isolating suspicious letters and packages.
- Train mail center, security, and management staff to validate all phases of your letter and package bomb-screening program.
- Conduct unannounced tests of mail center personnel.

WHAT ARE THE ROLES AND RESPONSIBILITIES OF THE MAIL CENTER SECURITY COORDINATOR RELATIVE TO LETTER AND PACKAGE BOMB SAFETY?

Postal Inspectors recommend including the mail center manager, or a designee, as a member of the group that develops your Bomb Threat Response Plan. Corporate management should ensure the mail center security coordinator and alternate are mature, responsible, and emotionally stable. They 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 covers. All circumstances of their receipt should be recorded.

WHAT ABOUT BOMB THREATS RECEIVED BY PHONE?

Phone threats offer an opportunity to obtain more detailed information, perhaps even the caller's identity. For that reason, your 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.

- Keep the caller on the line, ask him or her to repeat the message several times, and gather more information, such as caller ID.
- Write down the threat verbatim, using the caller's own words, and record any other information.
- Don't hang up under any circumstances!
- Ask corporate and security management to decide on the proper response, such as evacuation.
- Notify police and the fire department immediately.

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 EMPLOYEES DO IF THEY RECEIVE AN UNEXPECTED MAILPIECE?

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

If you receive an unexpected mailpiece:

- First check the return address.
- If you don't recognize the return address, contact the security office.
- The security office should attempt to contact the sender.
- Don't open the mailpiece until verification proves it's harmless.

WHAT SHOULD THE MAIL CENTER SECURITY COORDINATOR DO AFTER ENCOUNTERING A SUSPICIOUS LETTER OR PACKAGE DURING SCREENING?

RESPONSE	ACTION
FIRST	Follow your local established protocols.
INQUIRE	Ask the employee who found the suspicious letter or package to write down the specific recognition point in the screening process that caused the alert (excessive postage, no return address, rigid or bulky, lopsided or uneven appearance, strange odor, protruding wires, oily stains, discolorations, excessive tape, etc.).
ISOLATE	Isolate the area where the mailpiece was found—do not touch it.
ALERT	Alert employees that a suspicious letter or package has been found, what the points of recognition are, and to remain clear of the isolation area.
NOTIFY	Inform management and security that a suspicious item has been detected by the screening process.
DOCUMENT	Without touching the mailpiece, 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.
INFORM	Inform police (and Postal Inspectors if sent through the U.S. Mail) of all information recorded from the suspect item.

WHAT ARE SOME QUESTIONS TO ASK THE ADDRESSEE OR SENDER DURING THE VERIFICATION PROCESS?

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

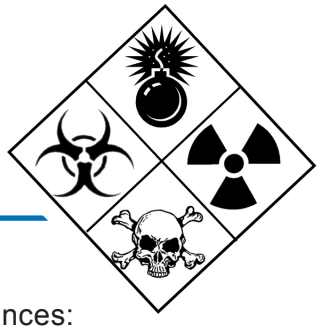
If you determine the sender is unknown at that return address or the return address is fictitious, consider this scenario as an indication the letter or package may be dangerous.

WHAT IS THE IMPORTANCE OF TESTING CONTINGENCY PLANS?

The Postal Inspection Service can't 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.

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 recommendations from the Centers for Disease Control (CDC) on protective gear for your employees, contact your local CDC representative or visit *cdc.gov*.

ANTHRAX CHARACTERISTICS

TYPE	EXPOSURE	TRANSMITTAL & 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.
GASTRO-INTESTINAL	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.

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. To cause harm, ricin must be injected, inhaled, or ingested.

HOW TO LIMIT EXPOSURE TO A SUSPICIOUS SUBSTANCE IN THE MAIL?

- Develop an emergency plan in response to a known or possible exposure to a suspicious substance.
- Train workers how to recognize and handle a suspicious letter or package.
- Identify a single point of contact to open mail.
- Screen all mail for suspicious letters or packages.
- Do not open mail in an area where other personnel are present.
- If appropriate, have personal-protective equipment (gloves, masks, etc.) available for employees who handle mail.

WHAT SHOULD YOU DO IF YOU RECEIVE A SUSPICIOUS SUBSTANCE BY U.S. MAIL?

STEP	ACTION
1.	Above all else, follow your local established protocols. Notify your supervisor.
2.	If there is a known medical emergency or chemical reaction to the mailpiece, call 911 and then call Postal Inspectors at 877-876-2455 (press 2).
3.	If there is no known medical emergency or chemical reaction, call Postal Inspectors at 877-876-2455 (press 2).
4.	Isolate the damaged or suspicious letter or package. Cordon off the immediate area.
5.	Ensure that anyone who touched the mailpiece washes his or her hands with soap and water.
6.	List everyone who touched the mailpiece. Include contact information and have the information available for authorities. If asked, provide the information to first responders.
7.	Follow first responders' instructions on decontamination procedures.

You can find more guidance on suspected chemical, biological, or radiological contamination from the Centers for Disease Control at *cdc.gov*

REFERENCES

LOW- AND MODERATE-RISK FACILITIES SAFETY CHECKLIST

- ☐ Appoint a mail center security coordinator and ensure the position is supported by senior management.
- ☐ Meet with local first responders including the police department, fire department, Postal Inspectors, Centers for Disease Control (CDC), the Occupational Safety and Health Administration (OSHA), and others to establish familiarity with responsible groups and identify best local practices.
- ☐ 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 letters or packages.
- ☐ Provide training for mail handling staff on policies and procedures for mail security and emergency protocols.
- ☐ Perform in-depth background checks when hiring new staff and institute a probationary period for new hires.
- ☐ Limit mailroom access to employees wearing proper ID badges, uniquely identify and escort visitors, and encourage employees to challenge unknown people in a 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.
- ☐ Provide mailroom employees with CDC-approved, personal-protection equipment as appropriate.

HIGH-RISK FACILITIES SAFETY CHECKLIST

- ☐ Appoint a mail center security coordinator and an alternate and ensure the position is supported by senior management.
- ☐ Meet with local first responders including the police department, fire department, Postal Inspectors, Centers for Disease Control (CDC), the Occupational Safety and Health Administration (OSHA), and others to establish familiarity with responsible groups and identify best local practices.
- ☐ 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 letters or packages.
- ☐ Provide training for mail handling staff 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 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 ID 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.

HIGH-RISK FACILITIES SAFETY CHECKLIST (CONTINUED)

- ☐ Hire or designate security personnel for the mail center area.
- ☐ Ensure adequate lighting for areas 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 them to record and store surveillance of indoor and outdoor areas.
- ☐ Install an intrusion-detection system.
- ☐ 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 Postal Inspectors at 877-876-2455 (press 2).
- ☐ 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.

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

Additional Protective Measures for High-Risk Facilities

- Consider purchasing bomb-detection equipment or a K-9 unit.
- X-ray all incoming mail and store it in containment containers until testing is concluded.
- Use a “safe air” room for mail 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 these tactics:
  - Use an industrial vacuum cleaner equipped with a high-efficiency particulate air (HEPA) filter for cleaning. Don’t clean machinery with compressed air (blow-down/blow-off).
  - Install air curtains (using laminar air flow) in areas where large amounts of mail are processed.
  - Install filters in your building’s HVAC systems to capture aerosolized spores (if feasible).

PUBLICATIONS ABOUT MAIL CENTER SECURITY

These publications from the U.S. Postal Inspection Service may be viewed or printed at *usps.com* under Forms & Publications.

- Publication 52, *Hazardous, Restricted, and Perishable Mail*
- Publication 166, *Guide to Mail Center Security*
- Publication 167-B, *Response Checklist for Suspicious Mail and Unknown Powders or Substances*
- Publication 280, *Identity Theft*
- Notice 107, *Let’s Keep the Mail Safe*
- Notice 128, *The Safety of the Mail is Everybody’s Responsibility*
- Poster 84, *Suspicious Mail or Packages*

ADDITIONAL RESOURCES

postalinspectors.uspis.gov

U.S. POSTAL INSPECTION SERVICE

The U.S. Postal Inspection Service is the federal law enforcement agency responsible for all mail-related crime. Postal Inspectors can help businesses keep mail secure and protect against theft. They can perform on-site mail center security reviews for major mailers and assist with training in security protocols.

cdc.gov

CENTERS FOR DISEASE CONTROL AND PREVENTION

The Centers 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.

fbi.gov

FEDERAL BUREAU OF INVESTIGATION

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

ready.gov

FEDERAL EMERGENCY MANAGEMENT AGENCY

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

osha.gov

OCCUPATIONAL SAFETY AND HEALTH ADMINISTRATION

The Occupational Safety and Health Administration (OSHA) is an agency of the U.S. Department of Labor charged with the enforcement of safety and health legislation.

splcenter.org

SOUTHERN POVERTY LAW CENTER

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.

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's 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.

MAIL CENTER SECURITY
QUICK REFERENCE GUIDE

FOR SUSPICIOUS LETTERS AND PACKAGES

- First, if there is a known medical emergency or chemical reaction with the mailpiece, call 911. 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 Postal Inspectors at 877-876-2455 (press 2) if the item was received in the U.S. Mail.

FOR A BOMB

- Evacuate immediately.
- Call 911 for police, fire and hazmat unit.
- Call Postal Inspectors at 877-876-2455 (press 2) if the item was received in the U.S. Mail.

FOR CHEMICAL, BIOLOGICAL, OR RADIOLOGICAL CONTAMINATION

- Isolate it—don't handle.
- Wash your hands with soap and warm water.
- Call 911 for police, fire, and hazmat unit.
- Call Postal Inspectors at 877-876-2455 (press 2) if the item was received in the U.S. Mail.

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.

FOR A PLACED DEVICE

Do not disturb. If you're unable to verify the owner:

- Evacuate immediately.
- Call 911 for police, fire, and hazmat unit.

This guide is intended only for mail center supervisors and their employees.

877-876-2455 press 5
postalinspectors.uspis.gov

Publication 166 | January 2013 | PSN 7690-05-000-4890