Contents

Importance of Security to Mail Center Operations 1
Purpose of this Guide 1
Weapons of Mass Destruction 2
Anthrax 2
Definition 2
Assessment 4
Prevention 5
Response 9
Checklist 11
Resources 12
Mail Bombs and Bomb Threats 14
Definition 14
Assessment 14
Prevention 16
Response 17
Checklist 28
Resources 29
Mail Center Theft 30
Definition 30
Assessment and Prevention 32
Response 35
Mail Center Security Checklist 37
Resources 41

Mail Center Security Guide

Prevention is critical for keeping your mail center secure.

Importance of Security to Mail Center Operations

Although the mail center operates as the focal point for businesses, security policies and procedures for the mail center are often overlooked. Security is critical to mail center operations — large and small.

Lack of security can result in theft of supplies, postage, mail, and valuable information about your business contained in sensitive mail. An effective mail center security program includes policies and procedures to reduce risks and losses.

Purpose of this Guide

This *Mail Center Security Guide* was prepared by the U.S. Postal Inspection Service 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:

- Weapons of mass destruction.
- Mail bombs and bomb threats.
- Mail center theft.

Each of the three sections briefly states the definition of and the assessment, prevention, and response for a specific type of threat. Checklists and a resource list for additional information are also provided. Although the suggestions provided in this guide are applicable for many situations involving security threats, the suggestions are intended only as guidance.

Additional resources used to develop this guide include the Centers for Disease Control and Prevention, the General Services Administration, and the Bureau of Alcohol, Tobacco, and Firearms.

Weapons of Mass Destruction

The Federal Criminal Code defines weapons of mass destruction as:

- **Chemical** — Any weapon that is 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 weapon involving a disease organism, such as smallpox, botulinum toxin, and anthrax.
- **Radiological** — Any weapon that is designed to release radiation.

This guide specifies procedural responses for a biological threat (anthrax) delivered by the mail. The protective measures and responses for a chemical or a radiological threat delivered by the mail would be similar to those included in this guide for a biological threat.

What are the chances of receiving a biological, chemical, or radiological weapon in the mail?

The United States Postal Service delivers approximately 208 billion pieces of mail per year. To date, a small number of incidents of anthrax bacteria, a biological agent, have been sent through the mail.

Anthrax

Definition

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

Types of Anthrax Infections

Type	Exposure	Transmittal and Characteristics	Symptoms
Cutaneous	Skin	Cutaneous anthrax is the most common naturally occurring type of infection. Cutaneous anthrax usually occurs after skin contact with contaminated meat, wool, hides, or leather from infected animals. The incubation period ranges from 1 to 12 days. Infection is introduced through scratches or abrasions of the skin.	Skin infection begins as a raised bump that resembles a spider bite. Within 1 to 2 days, the infection develops into a blister and then a painless ulcer, with a characteristic black necrotic (dying) area in the center. The lesion is usually painless, but patients also may have fever, malaise, and headache. Lymph glands in the adjacent area may swell.
Inhalation	Inhalation	Anthrax spores must be aerosolized to cause inhalational anthrax. Inhalation anthrax is contracted by inhalation of the spores. It occurs mainly among workers handling infected animal hides, wool, and fur. The number of spores that cause human infection is unknown. The incubation period of inhalational anthrax among humans is unclear, but it is reported to range from 1 to 7 days, possibly ranging 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 an incubation period of 1 to 7 days, the onset of inhalation anthrax is gradual.
Gastrointestinal	Ingestion	Gastrointestinal anthrax usually follows the consumption of raw or undercooked contaminated meat and has an incubation period of 1 to 7 days.	Gastrointestinal anthrax is characterized by 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.

What is the treatment for anthrax?

Penicillin, doxycycline, and ciproflaxin are effective against most strains of anthrax. Penicillin is the drug of choice for naturally occurring anthrax. A vaccine is available and consists of a series of 6 doses over 18 months with yearly boosters. This vaccine, while known to protect against cutaneous anthrax, is also believed to be effective against the inhalation type.

Assessment

If you work in a mail center, should you be concerned about biological weapons?

Even a threat that is a hoax can disrupt the operations of your company. A delivery system for a biological agent can consist of just about anything that can produce an aerosol, including a wide variety of commercially available objects.

The most likely form for dissemination of anthrax as a biological terrorist agent is aerosolization of spores. Unlike nuclear and chemical agents, biological agents are not detectable to the human senses. You would never realize your exposure to a biological agent until you became sick with certain symptoms.

Are you at risk for getting anthrax from handling mail on the job?

There is a risk for anthrax associated with exposure to cross-contaminated mail, but the risk is very low — even for postal employees and persons who work in company mailrooms.

Prevention

How can you limit physical exposure of the mail center to suspect anthrax mailings?

Ways to Limit Physical Exposure to Suspect Anthrax Mailings

Step	Action
1.	Develop an emergency plan for steps in response to a known or a suspected exposure to anthrax.
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.	Have appropriate gloves available for mail handlers' use.

What worker safety guidelines are being issued?

The Centers for Disease Control and Prevention (CDC) and the Postal Service are collaborating to ensure that all mail handlers and postal workers are instructed on how to protect themselves from exposure to anthrax. Detailed guidelines may be found on CDC's Web site at *www.cdc.gov.*

In addition, the Postal Service's Web site features a General Services Administration (GSA) training module with information on how to respond to an anthrax threat in a mail center. The module is available at *www.usps.com.* The module describes actions that can be taken if there is a potential anthrax threat in a mail center, including countermeasures for staff to defend and protect against these threats.

Portions of the following information are excerpted from CDC's Web site.

Should all mail handling operations adopt anthrax worker safety guidelines immediately?

Every facility is different and should be evaluated based on the recommendations in the CDC guidelines. You should select the recommendations based on an evaluation of your worksite. This evaluation should focus on determining which processes, operations, jobs, or tasks would most likely result in an exposure if a contaminated envelope or package were found at the worksite. Many measures can be implemented immediately. Others require additional time and effort.

What kinds of engineering controls should mail-handling and processing operations consider implementing for detecting anthrax spores?

Anthrax spores can be aerosolized during the operation and maintenance of high-speed, mail-sorting machines. Mail processing could expose workers to spores and spores could enter heating, ventilating, or air-conditioning (HVAC) systems. Engineering controls can provide the best means of preventing worker exposure to potential aerosolized particles.

In settings where such machinery is in use, consider the following engineering controls:

- An industrial vacuum cleaner equipped with a high-efficiency particulate air (HEPA) filter for cleaning high-speed, mail-sorting machinery.
- Local exhaust ventilation at pinch roller areas.
- HEPA-filtered exhaust hoods installed in areas where dust is generated (e.g., areas with high-speed, mail-sorting machinery).
- Air curtains (using laminar air flow) installed in areas where large amounts of mail are processed. HEPA filters installed in the building's HVAC systems (if feasible) to capture aerosolized spores.

  Note: Machinery should not be cleaned using compressed air (i.e., blowdown/blowoff).

What administrative controls should your mail-handling and processing sites consider implementing to protect workers from exposure to anthrax spores?

You should limit the number of people working at or near sites where aerosolized particles may be generated, such as mail-sorting machinery and places where mailbags are unloaded or emptied. In addition, restrict the number of people including support staff and nonemployees entering areas where aerosolized particles may be generated. This recommendation applies to contractors, business visitors, and support staff.

What housekeeping controls in mail-handling and processing sites are recommended to protect workers from exposure to anthrax spores?

In the mail-handling worksite, dry sweeping and dusting should be avoided. Instead, the area should be jet-cleaned and vacuumed with HEPA-equipped vacuum cleaners.

What personal protective equipment for workers in mail-handling and processing sites is recommended to protect workers from exposure to anthrax spores?

Personal protective equipment for workers in mail-handling and processing worksites must be selected on the basis of the potential for cutaneous or inhalational exposure to anthrax spores. Handling packages or envelopes may result in skin exposure. In addition, because certain machinery such as electronic mail sorters can generate aerosolized particles, people who operate, maintain, or work near such machinery may be exposed through inhalation. People who hand sort mail or work at other sites where airborne particles may be generated (such as where mailbags are unloaded or emptied) may also be exposed through inhalation.

What are some examples of personal protective equipment and clothing that could be used to protect workers who handle mail from exposure to anthrax spores?

Protective, impermeable gloves should be worn by all workers who handle mail. In some cases, workers may need to wear cotton gloves under their protective gloves for comfort and to prevent dermatitis.

Gloves should be provided in a range of sizes to ensure proper fit. The choice of glove material such as nitrile or vinyl should be based

on safety, fit, durability, and comfort. Different gloves or layers of gloves may be needed depending on the task, the dexterity required, and the type of protection needed. Protective gloves can be worn under heavier gloves such as leather, heavy cotton for operations where gloves can easily be torn or if more protection against hand injury is needed.

Those workers for whom a gloved hand presents a hazard, such as those who work close to moving machine parts, the risk for potential injury resulting from glove use should be measured against the risk for potential exposure to anthrax.

Workers should avoid touching their skin, eyes, or other mucous membranes since contaminated gloves may transfer anthrax spores to other body sites. Workers should consider wearing long-sleeved clothing and long pants to protect exposed skin.

Gloves and other personal protective clothing and equipment can be discarded in regular trash once they are removed or if they are visibly torn, unless a suspicious piece of mail is recognized and handled. If a suspicious piece of mail is recognized and handled for anthrax, the worker's protective gear should be handled as potentially contaminated material. Workers should wash their hands thoroughly with soap and water when gloves are removed, before eating, and when replacing torn or worn gloves. Soap and water will wash away most spores that may have contacted the skin; disinfectant solutions are not needed.

Are there some areas in the postal setting that present a greater risk to some workers than others for anthrax exposure?

People working with or near machinery, such as electronic mail sorters, that can generate aerosolized particles should be fitted with NIOSH-approved respirators that are at least as protective as an N95 respirator. People working in areas where oil mist from machinery is present should be fitted with respirators equipped with P-type filters.

Because facial hair interferes with the fit of protective respirators, workers with facial hair like beards and or large moustaches may require alternative respirators such as powered air-purifying respirators (PAPRs) with loose-fitting hoods. Workers who cannot be fitted properly with a half-mask respirator based on a fit test may require the use of alternative respirators, such as full facepiece, negative-pressure respirators, PAPRs equipped with HEPA filters, or supplied-air respirators.

If a worker is medically unable to wear a respirator, the employer should consider reassigning that worker to a job that does not require respiratory protection. In addition, the use of disposable aprons or goggles by persons working with or near machinery capable of generating aerosolized particles may provide an extra margin of protection.

Response

What are the indicators of a suspicious letter or parcel?

A parcel or letter is considered suspicious when it has more than one of the following characteristics:

- No return address or one that can't be verified as legitimate.
- Excessive postage.
- Handwritten or poorly typed address, incorrect titles or titles with no name, or misspellings of common words.
- Addressed to someone no longer with your organization or not addressed to a specific person.
- Strange return address or no return address.
- Marked with restrictions, such as "Personal," "Confidential," or "Do not X-ray."
- Powdery substance on the outside.
- Unusual weight given its size, lopsided, or oddly shaped.
- Unusual amount of tape on it.
- Odors, discolorations, or oily stains.

What should you do if you receive a suspect anthrax threat by mail?

Step	Action
1.	Notify your supervisor, who will immediately contact the U.S. Postal Inspection Service, local law enforcement authorities, safety office, or designated person.
2.	Isolate the damaged or suspicious packages. 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 letter and/or envelope. 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.	Notify the Centers for Disease Control and Prevention's Emergency Response line at: 770-488-7100 for answers to any questions.
8.	Call a Postal Inspector (see list on the inside back cover of this guide) to report that you've received a letter or parcel in the mail that may contain biological or chemical substances.

How should you decontaminate the contaminated articles?

Decontamination can be done by boiling contaminated articles in water for 30 minutes or longer and using some of the common disinfectants. Chlorine is effective in destroying spores and vegetative cells.

Checklist

Suspicious Mail Guidelines

If you receive a suspicious letter or package:

1 Handle with care.
Don't shake or bump.

2 Don't open, smell, touch, or taste.

3 Isolate it immediately

4 Treat it as suspect. Call local law enforcement authorities.

If a letter/parcel is open and/or a threat is identified...

For a Bomb

Evacuate Immediately
Call Police
Contact Postal Inspectors
Call Local Fire Department/HAZMAT Unit

For Radiological

Limit Exposure – Don't Handle
Distance (Evacuate Area)
Shield Yourself From Object
Call Police
Contact Postal Inspectors
Call Local Fire Department/HAZMAT Unit

For Biological or Chemical

Isolate – Don't Handle
Wash Your Hands With Soap and Warm Water
Call Police
Contact Postal Inspectors
Call Local Fire Department/HAZMAT Unit

Resources

Centers for Disease Control and Prevention

Web site: *www.cdc.gov*

The Centers for Disease Control and Prevention (CDC), the lead federal agency for protecting the health and safety of people, coordinates public health response to bioterrorism threats. For up-to-date information on health threats from exposure to biological, chemical, or radiological agents, visit CDC's bioterrorism Web page at: *www.bt.cdc.gov.*

To report an incident, contact CDC's Emergency Preparedness and Response Branch, National Center for Environmental Health at: 770-488-7100.

U.S. Postal Service

Web site: *www.usps.com*

The U.S. Postal Service Web site features a General Services Administration (GSA) training module with information on how to respond to an anthrax threat in a mailroom, which is available at *www.usps.com.* The module lays out actions that can be taken if there is a potential anthrax threat in a mailroom, including countermeasures for staff to defend and protect against these threats.

This section of the web site also features clips and a full version of the Postal Service video, *Biological Threat: Protecting Your Mailroom,* which features information on keeping mail centers safe. Business customers can order a free copy of the complete video at *www.usps.com* or call toll-free at: 800-275-8777.

U.S. Postal Inspection Service

Web site: *www.usps.com*

The Postal Inspection Service provides information about establishing a secure mail center, detecting mail bombs, and protecting your business against mail fraud schemes or any other postal crimes. Contact your nearest Postal Inspection Service location for details. Inspectors can perform on-site security surveys for larger firms and assist your firm in giving security training presentations.

Federal Bureau of Investigation

Web site: *www.fbi.gov*

The Federal Bureau of Investigation (FBI) is the lead federal agency for crisis management for all acts of terrorism and in all threats or incidents of weapons of mass destruction (WMD). The FBI's Awareness of National Security Issues and Response (ANSIR) Program is the *public voice* of the FBI for espionage, counterintelligence, counter terrorism, economic espionage, cyber and physical infrastructure protection, and all national security issues. To report suspected illegal intelligence or terrorism activity against the interest of the United States, telephone the ANSIR coordinator at the FBI Field Office nearest you.

General Services Administration

Web site: *www.gsa.gov*

The General Services Administration has posted a reference version of the material from its course, "How to Respond to an Anthrax Threat in a Mail Center," on its Web site. Anyone can access the content of this course at no cost.

Occupational Safety & Health Administration

Web site: *www.osha.gov*

The mission of the Occupational Safety & Health Administration (OSHA) is to ensure safe and healthful workplaces in America. OSHA provides training and reference materials on safety and health for outreach initiatives to the public. To report incidents of workplace safety violations to OSHA call their toll-free number at: 800-321-6742, and TTY at: 877-889-5627.

Mail Bombs and Bomb Threats

Definition

What motivates people to send mail 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.

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

Mail 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.

Assessment

How vulnerable is your workplace to a bomb threat?

The chances of your workplace receiving a mail 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 mail bombs and bomb threats.

The following are typical questions asked during this 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.

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.

- **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 two 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? (See Resources section for the Web site of the U.S. Department of State that offers information on terrorist organizations.)
- **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 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?

Postal Inspectors recommend consultations with security experts in terrorist tactics and vulnerability assessment. The Postal Inspection Service can provide information about establishing a secure mail center and detecting mail bombs. Contact a Postal Inspector near your workplace. In addition, the Bureau of Alcohol, Tobacco, and Firearms (ATF) provides information about bomb threats and physical security planning on its Web site.

Prevention

The key to prevention is having a bomb threat response plan.

When properly planned and implemented, a bomb threat response plan will help to prevent incidents of mail bombs, bomb threats, and suspiciously placed devices from creating panic among employees and from inflicting physical harm to employees or facilities.

A bomb threat response plan should be part of your company's overall corporate security program that addresses all personnel and physical security issues. Individuals from corporate management and from security should share responsibilities for developing the plan.

Because needs and resources of companies differ, every recommendation below may not apply to all companies. Determine which are appropriate for your company and conduct periodic security reviews of your operation to identify needed improvements.

What are some controls for the physical security of your workplace?

Most explosive devices are placed, not mailed, therefore, 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.

Controls to Enhance 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 identification badges for staff and for visitors.
5.	Require visitors to be accompanied by staff employees to and from the office or facility entrance.
6.	Request visitors to display identification to security personnel when they sign in.
7.	Keep detailed logs on the arrival and departure times of all visitors.
8.	Consider using the services of a certified protection professional to evaluate in detail your company's personnel and physical security safeguards.

Response

Each bomb threat presents three basic options:

- Evacuate everyone immediately and search.
- Evacuate some employees while a search is undertaken.
- Evacuate no one and search.

A fourth option, to ignore the threat, is not generally considered viable. If the company policy is to evacuate all employees and shut down operations when any threat is received, this policy will likely result in false alarms placed by employees anxious to exploit the policy. It is best to judge the credibility of each threat individually.

What are the components of a Bomb Threat Response Plan?

A Bomb Threat Response Plan should encompass all facilities at your company's site, including outbuildings, parking lots, and garages immediately adjacent to buildings occupied by employees. If your company maintains offices at multiple sites, security officers at each site must be included in the communications loop.

The Bomb Threat Response Plan should, at a minimum, include procedures, provisions, and policies for the following:

- Ensuring that nonpostal deliveries (except commercial shipments) are channeled through the mail center.
- Operating a Command Center.
- Channeling all mail and parcels through a mail bomb-screening program.
- Defining and maintaining communication channels among the mail center security coordinator, management, and security.
- Responding to written bomb threats and phoned in bomb threats.

What, who, and where is a Command Center?

What — While all threats should be taken seriously, your company's response may depend on the circumstances present at any given time. The decision to evacuate all or part of the facility should be made by a Command Center working group. Do not publicize your policy on evacuations.

Who — Representatives from your company's management, security, and mail center should be the core of your Command Center working group. These representatives, specified by name and title, should have the authority to decide how your company will respond to any bomb threat situation.

Where — Locate the Command Center at or near the communications center of your company. Equip the Command Center with telephone numbers for the police, Postal Inspectors, ATF, fire department, and emergency medical services. An employee roster with all current telephone numbers, including home, office, pagers, and cellular telephones should also be maintained. Current copies of your company's floor plans or building blueprints are also critical.

What are the components of a mail bomb-screening program?

Postal Inspectors can help develop a mail bomb-screening program that can be adapted to most company's mail center operations regardless of the size of the company. A successful mail bomb-screening program depends on:

- A well-trained mail center staff.
- Good communication within the firm's management, security, and mail center.
- Cooperation among employees at every level.

Steps to Establish a Mail Bomb-Screening Program

Step	Action
1.	Perform a vulnerability assessment to determine if your company or a particular employee is a potential target.
2.	Appoint a mail center security coordinator and an alternate to be responsible for the developed plan and to ensure compliance with it.
3.	Establish direct lines of notification and communication among the mail center security coordinator, management, and the security office.
4.	Develop specific screening and inspection procedures for all incoming mail or package deliveries. Train employees in those procedures.
5.	Develop specific mail center handling techniques and procedures for items screened and identified as suspicious and dangerous.
6.	Develop verification procedures for confirming the contents of suspicious packages encountered through the screening process.
7.	Establish procedures for isolating the suspicious package.
8.	Conduct training sessions for mail center, security, and management personnel to validate the practicality of all phases of the Mail Bomb Screening Program.
9.	Conduct unannounced tests for mail center personnel.

What are the role and responsibilities of the mail center security coordinator?

Postal Inspectors recommend including the mail center manager, or a designee, as a member of the planning group that develops the

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.

Mail Center Security Coordinator

Role	Responsibilities
Oversight and Training	Oversees the mail bomb-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 the suspect postal item place sufficient safety distance between themselves and the item and that those employees do not cluster around the item.

How vital are direct lines of communication?

Having direct lines of communication between the mail center security coordinator, management, and corporate security is vital. The mail center security coordinator must be able to communicate directly with managers in the Command Center.

Corporate security must receive prompt notification when a suspicious package is identified or a threat is received in the mail center. Additional verification may be required of corporate security, or notification may be given to the supporting police, Postal Inspector, and bomb squad disposal units.

These channels of communication will also be crucial when a package clears the screening process, is delivered, and is declared suspicious by the recipient. Information concerning that parcel should be relayed back to the mail center in the event that other similar parcels are being processed.

Telephone threats received by company receptionists, or others, should be brought to the attention of the corporate security officer and then relayed to the mail center manager, who needs to be informed of any specific information that is valuable for the mail bomb-screening process.

Who should perform the mail screening function?

Incoming mail procedures in most companies follow a similar pattern. Bags or bundles of mail and items sent by courier are delivered to a centralized mail center for distribution. If your company does not have a centralized receiving procedure, then management should institute such a procedure immediately.

The initial sorting of the mail for delivery must be done by hand. This is the point where screening of incoming mail for suspect items should occur. Individuals who normally handle the mail sorting function should perform the screening function. As such, these individuals are most likely to notice packages that are out of the ordinary.

What are the indicators of a suspicious letter or package?

The basic screening procedures of incoming mail and packages are not foolproof. In many cases, the person who first detects anything suspicious about a package is the recipient. For this reason, you should distribute a list of suspicious package indicators to all employees to increase their awareness of suspicious packages.

Indicators of a suspicious package are:

- Excessive postage.
- Misspelled words.
- Addressed to title only.
- Rigid or bulky.
- Badly typed or written.
- Fictitious, unfamiliar, or no return address.
- Strange odor.
- Lopsided.
- Oily stains on wrapper.
- Wrong title with name.
- Protruding wires.

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 information. Write down the threat verbatim — in 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 procedures. 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 are the preparations for conducting a bomb search?

Preparations for a Bomb Search

Evacuate building	If your company is regulated by OSHA, follow procedures given in your company's emergency evacuation and fire prevention plan as required by OSHA.
	Furnish evacuation routes to all supervisors.
	Fire alarms should not be used to signal an emergency bomb response evacuation. The possibility exists that a bomber would target routes, such as stairwells and/or emergency exits, normally used during an evacuation due to a fire alarm.
Contact police and fire departments	Your local police and fire department should be contacted about their bomb search policies. Determine if in the event of a threat, if these departments will help conduct the search. If yes, find out what they will need from your Command Center.
	Police agencies often will not conduct searches of private facilities. If your local police and fire department will not assist in the search for an explosive device, company search teams will have to be deployed. You and your employees know your facility and are more likely to observe unusual items that police and fire department personnel could overlook.
Deploy bomb search team	Searches may be conducted by individuals from your company who have volunteered for bomb search deployment duty and who have been trained for this purpose.
	A bomb search team may consist of managers only or teams of managers and employees. For best results, the individuals conducting the search should be very familiar with all the sights, sounds, and smells of the area to be searched. The ideal search team usually consists of two volunteer employees and a supervisor.
	The employees conduct the search under the direction of the supervisor, who communicates the progress of the search to the Command Center. Volunteers should be trained in basic search and building clearance techniques by private security professionals.
Outfit search teams	Search teams should be outfitted beforehand with a few elementary tools, such as screwdrivers, crescent wrenches, pry bars, and flashlights. Remember to have the necessary keys or a custodian available to open storage rooms, boiler rooms, telephone, and utility closets.

How should a bomb search be conducted?

Search techniques should be kept confidential and training should be limited to security employees.

Conducting a Building Search

Who	A team of two employees.
Where	Start with the building's exterior.
How	The team should search the areas of the facility most accessible to the public. Then move indoors through the main entrance or lobby to waiting rooms, rest rooms, stairwells, and elevators. Each of the two employees begins his or her search at the same point in the room. Begin at floor level. Divide the room into four-foot increments from the floor to the ceiling, including the area above a false/suspended ceiling. Each employee works his or her way up in four-foot increments. Each person works in opposite directions around the room and back to the center of the room. The search patterns should overlap somewhat. This process is repeated methodically from office to office and from floor to floor throughout the entire facility.
What If	If a suspicious parcel or device item is found, evacuate and cordon off the immediate area to prevent inadvertent exposure to the danger. Vibration from movement near the suspect item may cause an explosion. Additionally, a timing mechanism may be set to activate the device within minutes of placement. Do not touch the suspicious device. Touching it may trigger a detonation. Under no circumstances should volunteers attempt to handle or remove suspicious placed devices. Report the situation to your security office who will call the police. Once the area is cleared, continue throughout the facility until the entire area is declared safe for re-entry. This precaution is necessary because a bomber may plant more than one device.

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 you are fully satisfied 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(s) in the screening process that caused the alert (excessive postage, no return address, rigid envelope, lopsided, strange odor).
2.	Alert	Alert the remaining employees that a suspicious package has been found and what the points of recognition are and to remain clear of the isolation area.
3.	Remove	Place suspect item in reinforced container and take it to the isolation area.
4.	Document	Record from each 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 in exact spelling and location given on item.
5.	Notify	Contact management and security and inform them a suspicious item has been detected through the screening process.
6.	Inform	Inform the police and Postal Inspectors (if a mailed item) giving 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 accurately all information pertaining to the suspicious package in an incident log. If possible, dispatch a security officer with a Polaroid camera to photograph all sides of the package without moving it, as it rests in the holding container. These exact details of the package's markings will be made available for study and use by the bomb scene officer.
2.	Contact and verify	Before calling the police, security personnel should attempt to find out if the addressee of the suspicious package has any knowledge of the item or its contents. If the addressee can positively identify the suspect item, the package may be opened by security with relative safety. Attempt to resolve the verification by contacting the sender as indicated on the suspicious package's return address. If the sender must be contacted to identify the item and contents, a management decision must be made as to the reliability of the information.
3.	Notify	If the return addressee proves to be fictitious, or if you cannot locate the sender within a reasonable period of time, notify the police and Postal Inspectors. Tell them that a suspicious package has been detected by the mail screening process and has been placed in the holding container in the isolation area awaiting their arrival. Be sure to give responding authorities the specific location of the holding area and the mail center coordinator's or security officer's name. Notify appropriate management personnel of the detection, through mail screening, of a suspicious package.
4.	Assist	Stand by to offer assistance to the police and Postal Inspectors upon their arrival.

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 origin?
- Has the addressee purchased or ordered any merchandise from any business concern whose parent organization might be located in area of origin?

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 parcel may be dangerous.

What is the importance of testing of 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. These tests should be conducted in a manner that does not alarm employees. The 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 your emergency contingency plan by conducting scheduled tests. Hold post-testing meetings to address problems and resolve them before the next test. Use the following Bomb Threat Response Plan checklist to periodically review your company's preparations.

Checklist

Bomb Threat Response Plan Checklist

- ☐ The Bomb Threat Response Plan complements overall physical security plan. Ensure that your company's premises are secured against unauthorized entry.
- ☐ Command Center staff include corporate management, security, and the mail center security coordinator. First step is to perform a vulnerability assessment.
- ☐ Command Center staff have authority to deal with any threat received and to order an evacuation.
- ☐ Equip Command Center with telephone numbers of police, fire department, Postal Inspection Service, medical emergency services, and all employees. Have facility floor plans or blueprints on file.
- ☐ Determine local police policy on conducting bomb threat searches.
- ☐ If needed, organize and train search teams of volunteer employees familiar with areas to be searched.
- ☐ Equip search teams with basic tools, such as flashlights, screwdrivers, pry bars, and keys to all offices and storage areas.
- ☐ Train telephone operators and receptionists to remain calm if receiving a threat and to gather additional information.
- ☐ Establish policy requiring all mailed and privately delivered parcels to undergo screening in the mail center.
- ☐ Train mail center employees to recognize suspicious parcel and mail bomb characteristics during screening.
- ☐ Advise employees to not open suspicious parcels.
- ☐ Advise all employees to contact mail center if they receive a parcel they are not expecting and which cannot be explained.

Resources

Southern Poverty Law Center

Web site: *www.splcenter.org*

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

Bureau of Alcohol, Tobacco, and Firearms

Web site: *www.atf.treas.gov*

The Bureau of Alcohol, Tobacco, and Firearms (ATF) is a law enforcement organization within the U.S. Department of the Treasury responsible for enforcing the federal laws and regulations relating to alcohol, tobacco, firearms, explosives, and arms. ATF's Web site provides information on bomb threats and physical security planning.

U.S. Department of State

Web site: *www.state.gov*

The U.S. Department of State's Web site provides a current list of terrorist organizations.

Mail Center Theft

When developing your mail center policies and procedures, the key word is prevention.

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. 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.

Definition

What is mail? Or, when does federal protection and the U.S. Postal Inspection Service jurisdiction extend into your mail center?

Letters or parcels are personal property. They are not considered mail protected by federal statutes until they are placed in an authorized depository for mail matter.

Authorized depositories include:

- Any Post Office.
- Collection box.
- Letter box.
- Other receptacle intended or used for the receipt or delivery of mail on any mail route.
- Mail handed to a carrier serving a route.

Items that are intended for mailing, but that are stolen by an agent or messenger of the sender prior to deposit in an authorized depository *are not protected under federal statute.*

When does federal protection of mail terminate?

Mail received into the hands of the addressee or the 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 for receipt of 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 item remains in the box. Mail adjacent to such a box is also protected.

Protection 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.

To learn about the federal laws applicable to postal crimes, see the Resources section on page 41 for a web site for the United States Code.

Representative Federal Laws on Selected Postal Crimes
18 USC 501, Counterfeiting Stamps, Meter Stamps, or Postal Cards
18 USC 876, Mailing Threats and Extortion Letters
18 USC 1341, Mail Fraud
18 USC 1342, Using Fictitious Name or Address in Mail Fraud Scheme
18 USC 1461, Mailing Obscene or Crime-Inciting Matter
18 USC 1463, Mailing Indecent Matter on Wrappers or Envelopes
18 USC 1707, Theft of Postal Service Property
18 USC 1708, Theft of Mail or Possession of Stolen Mail (by nonpostal person)
18 USC 1715, Firearms Nonmailable, in Certain Cases
18 USC 1716, Bombs and Other Injurious Articles Nonmailable
18 USC 1720, Reuse of Canceled Stamps or Envelopes
18 USC 1725, Postage Unpaid on Mail Put in Mailbox
21 USC 843b, Unlawful Mailing of a Controlled Substance

Assessment and Prevention

Personnel

When evaluating the security policies and procedures in a mail center, focus on the three "Ps" of mail center security — Personnel Place Procedures

Do you give the same personnel screening to your mail center employees as you do to others in your company? Review the personnel screening requirements for your mail center personnel. Remember, these mail center workers have access to almost everything that comes into or goes out of your company.

How extensive is your pre-employment screening?

When conducting 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. In addition, by interviewing a job candidate in-depth and at length, you may identify any potential 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 should remain 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 the mail and other valuables?

Only authorized employees should be assigned to accept mail at the office. Give the Post Office a list of these employees for its file. When any personnel change, update the mail personnel list immediately and provide a copy to the Post Office to avoid having mail given to unauthorized persons. 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 messengers are making unauthorized stops or are leaving your mail unattended in unlocked delivery vehicles.

Place

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

A properly designed physical layout of a mail center can serve as a preventive measure.

Measures to Enhance the Physical Layout of Your Mail Center for Deterring Theft

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.	Supervise employees. Often, dishonest mail center employees have stolen thousands of dollars worth of merchandise, remittances, and company credit cards simply because they were not adequately supervised.
5.	Control access to your mail center and mail 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 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.

Procedures

In reviewing the mail center internal controls, what questions should you ask?

- Is my outgoing mail sealed shortly after the most valuable item is placed inside?
- Can the contents and value of the mail item be identified from the exterior appearance?
- Is address correction requested routinely so my mailing lists can be updated? Is postage paid for this service accounted for periodically?

Theft Prevention Tips

Mail Center Activity and Equipment	Action
Registered Mail	Keep registered mail separate from other mail.
	Document each transfer of registered mail by requiring the receiving employee to sign for it. This procedure will establish accountability. Companies find they have difficulty tracking certified and registered mail if they do not set up a log 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 piece of mail sign and date the entry log. This step provides a reliable tracking system.
Petty Cash	Establish adequate controls to identify individual 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 because this practice is often theft. You can get an accurate account of postage and its purpose when only authorized employees operate the postage meters.
	Keep your postage meter locked when not in use.
	Have a trusted employee maintain Form 3602-A, *Record of Meter Register Readings* (see sample of form on page 36. This procedure detects unauthorized after-hours use of the meter and also aids you in obtaining a refund if your postage meter malfunctions.
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.

Theft Prevention Tips (continued)

Mail Center Activity and Equipment	Action
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	Contract with a commercial mail preparation service to compile, stuff, and presort your mailings. On occasion, Postal Inspectors have found that some 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 Bulk Business Mail Entry Unit uses the 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 next page), 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.

Response

Always call your Post Office to report mail losses. Losses are charted by the Postal Inspection Service. This process identifies problem areas and assists Postal Inspectors in identifying thieves.

Security recommendations developed by the U.S. Postal Inspection Service are given in the Mail Center Security Checklist on page 37. Use the checklist to evaluate security in your mail center operations.

Example of a Form for Recording Meter Readings

Month of _____ Year _____

Day	A. Ascending Register	B. Descending Register	C. Total of Columns A and B	D. Locking Seal Number

Sample Label For Incoming and Outgoing Mail Depositories

WARNING

Willful damage to mailboxes and theft of mail are federal crimes (felonies) punishable by fine or imprisonment or both. (18 U.S. Code 1705 & 1708)

Label 33, June 1994

Mail Center Security Checklist

- ☐ Mail center personnel screened.
- ☐ Authorized receptacles for U.S. Mail clearly labeled.
- ☐ Location, furniture, and mail flow provide maximum security.
- ☐ Alarms and surveillance equipment installed.
- ☐ Access limited to authorized personnel.
- ☐ Distribution delays eliminated.
- ☐ Postage and meter protected from theft or unauthorized use.
- ☐ High-value items locked overnight.
- ☐ Accountable items verified and secured.
- ☐ Control of address labels maintained.
- ☐ Labels securely fastened to mail items.
- ☐ Postage meter strips overlap labels.
- ☐ Labels and cartons do not identify valuable contents.
- ☐ Return address included and duplicate label in carton.
- ☐ Presort and ZIP+4® savings taken when applicable.
- ☐ Parcels prepared to withstand transit.
- ☐ Containers and sacks used when possible.
- ☐ Outgoing mail delivered to postal custody inside the facility.
- ☐ Employee parking separated from dock area.
- ☐ Lost and rifled mail reported to Postal Service.

Checklist (continued)

- ☐ Supervisor can see all employees and work areas.
- ☐ Contract delivery services screened.
- ☐ Unnecessary stops by delivery vehicle are eliminated.
- ☐ Procedures established for handling unexplained or suspicious packages.
- ☐ Periodic testing done for loss and or quality control.
- ☐ Postal Service receipts for meter settings verify authorized amounts.
- ☐ Meters checked regularly.

The Diligent Employee: He Stole a Little Every Day

Excerpted from the *Philadelphia Inquirer*, January 5, 1992, by Kimberly McLarin and Linda Lloyd

Mail room Supervisor Raymond Greene bilked Pennsylvania Hospital out of $373,000. It was a scam, pure and plain, a beautiful operation helped along by the simple fact that nobody asked any questions.

Nobody wondered why Raymond Greene, the mail room supervisor at Pennsylvania Hospital, went to the post office for stamps every day instead of buying in bulk. Nobody asked why Greene would turn in five, ten, or 20 receipts a day for reimbursement instead of one.

Nobody wondered why the hospital was spending tens of thousands of dollars a year for loose stamps when it had a postage meter...

By the time someone got around to asking, Greene had bilked Pennsylvania Hospital out of approximately $373,000 over nearly six years, according to Assistant District Attorney William Heiman. Greene was being reimbursed over $1,000 a week - for stamps he hadn't bought. And every dollar of the take was approved by someone in charge.

"This all went through the business accounting office," Heiman said. "Unfortunately, as soon as the clerks saw the postage stamp" - the post office seal stamped on the receipt, - "they didn't question it further." Something so simple got by them so long...

...as Supervisor, Greene soon developed a routine. Every morning, he would walk the six blocks to the U.S. Post Office at Ninth and Market Streets to buy stamps. He went so often that clerks there knew him by name. At the start, Greene would buy one book of stamps for $5, postal workers testified. He always asked for a receipt. But instead of asking for only one receipt for $5, Greene would ask for four receipts for $1.25 each. He told the clerks he needed four receipts to submit to four different accounting divisions. So after clearing it with their supervisor, the clerks did as he asked...

"Using a pen, Greene would then alter the handwritten receipts so that $1.25 became $49.25, or $39.25, or $34.25, or $69.25, Heiman said...

Then Greene would submit the receipts, often totaling several hundred dollars a day, to one of several supervisors with the authority to approve his reimbursement requests...

...after awhile, Greene, realizing his scam was so successful, began increasing the number of stamp books he bought - and the number of receipts he received. Instead of buying $4 worth of stamps, he would buy $20 worth. And instead of altering four receipts, he altered 16 and turned them all in for reimbursement. In his best year, 1989, Greene was reimbursed $138,000, Heiman said. Early the next year, hospital officials got suspicious.

They conducted an internal audit and began watching Greene's actions. They called in the District Attorney's Office...

Greene was fired in March,1990, but the district attorney's investigation continued. Officer Jeffrey Judge of the Philadelphia Police Department spent nearly three months analyzing the 9,936 receipts Greene had submitted to the hospital for reimbursement.

Under infrared light, ink can appear either opaque or transparent depending on the type used, Judge testified. So using such light, he was able to determine that the numbers on at least some of the receipts had been written with two different pens, and that one figure was written over another...

Greene's co-workers testified that he was always beautifully dressed, often draped in gold jewelry, and drove a large, fancy car. But he and his wife lived in a modest row home. Mack, the block captain,... described Greene as a good neighbor and loyal member of the block club. "We trusted him with money to buy things and we haven't had any problems," she said. "We knew he was honest." "He really believes in working," she said after learning Greene was going to prison. "I hope this doesn't hurt him on his new job."

Resources

U.S. Postal Inspection Service

Web site: *www.usps.com*

The Postal Inspection Service can provide more information about establishing a secure mail center and protecting your business against mail theft. Contact the Postal Inspection Service Division nearest you for details. Inspectors can perform on-site security surveys for larger firms and assist your firm in giving security training presentations.

General Services Administration

Web site: *www.legal.gsa.gov*

FedLaw, a page on the Web site of the General Services Administration, has references and links to federal regulations and the United States Code.

To order a printed copy of this *Mail Center Security Guide,* call the Material Distribution Center at: 1-800-332-0317, press option 4, and ask for Publication 166. Additional resources related to security of the mail and an online version of this guide are available on *www.usps.com.*

Publication 166
September 2002

Divisions of the Postal Inspection Service

For the telephone number of your local Postal Inspector, contact the nearest Postal Inspection Service division from the list below.

Florida Division
3400 Lakeside Dr 6th Fl
Miramar FL 33027-3242
(954) 436-7200
Fax: (954) 436-7282

Gulf Coast Division
PO Box 1276
Houston TX 77251-1276
(713) 238-4400
Fax: (713) 238-4460

Michiana Division
PO Box 330119
Detroit MI 48232-6119
(313) 226-8184
Fax: (313) 226-8220

Mid-Atlantic Division
PO Box 3000
Charlotte NC 28228-3000
(704) 329-9120
Fax: (704) 357-0039

Midwest Division
1106 Walnut St
St Louis MO 63199-2201
(314) 539-9300
Fax: (314) 539-9306

New York Metro Division
PO Box 555
New York NY 10116-0555
(212) 330-3844
Fax: (212) 330-2720

North Jersey/Caribbean Division
PO Box 509
Newark NJ 07101-0509
(973) 693-5400
Fax: (973) 645-0600

Northeast Division
495 Summer St Ste 600
Boston MA 02210-2114
(617) 556-4400
Fax: (617) 556-0400

Northern California Division
PO Box 882528
San Francisco CA 94188-2528
(415) 778-5800
Fax: (415) 778-5822

Northern Illinois Division
433 W Harrison St Rm 50190
Chicago IL 60669-2201
(312) 983-7900
Fax: (312) 983-6300

Northwest Divison
PO Box 400
Seattle WA 98111-4000
(206) 442-6300
Fax: (206) 442-6304

Philadelphia Metro Division
PO Box 7500
Philadelphia PA 19101-9000
(215) 895-8450
Fax: (215) 895-8470

Rocky Mountain Division
1745 Stout St Ste 900
Denver CO 80202-3034
(303) 313-5320
Fax: (303) 313-5351

Southeast Division
PO Box 16489
Atlanta GA 30321-0489
(404) 608-4500
Fax: (404) 608-4505

Southern California Division
PO Box 2000
Pasadena CA 91102-2000
(626) 405-1200
Fax: (626) 405-1207

Southwest Division
PO Box 162929
Ft. Worth TX 76161-2929
(817) 317-3400
Fax: (817) 317-3430

Washington Metro Division
PO Box 96096
Washington DC 20066-6096
(202) 636-2300 or
(301) 499-7585
Fax: (202) 636-2287

Western Allegheny Division
1001 California Ave Rm 2101
Pittsburgh PA 15290-9000
(412) 359-7900
Fax: (412) 359-7682