MAIL ROOM SECURITY

ADDRESSING

BIOLOGICAL & CHEMICAL THREATS

AND

MAIL BOMBS

PRESENTED BY

UNITED STATES POSTAL INSPECTION SERVICE

OCTOBER 2001

MAIL ROOM SECURITY AWARENESS

The mail room is the focal point for businesses and government agencies and is often the most overlooked when applying security policies and procedures. A comprehensive and effective mail room security program should include policies and procedures to reduce risks and losses. This handbook highlights recommended security awareness related to ***Biological and Chemical Threats (including Anthrax)*** *and* ***Mail Bombs***.

Security is extremely important to mail room operations both large and small. Lack of security can result in theft of supplies, postage, mail, and valuable information about your business contained in sensitive mail. When reviewing your mail center policies and procedures, the word is ***Prevention***.

BIOLOGICAL AND CHEMICAL THREATS:

Federal Criminal Code defines weapons of mass destruction as:

- 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.
- any weapon involving a disease organism; such as small pox botulinum toxin, and anthrax.
- any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

ANTHRAX

I. HOW LIKELY IS IT THAT SOMEONE WOULD RECEIVE A HARMFUL BIOLOGICAL OR CHEMICAL AGENT IN THE MAIL?

The Postal Service delivers approximately 208 billion pieces of mail per year. Presently, there have been a relatively small number of suspected incidents of anthrax bacteria being sent through the mail.

II. HOW OFTEN DO THESE THREATS AND HOAXES OCCUR?

During FY 1999 and FY 2000, there were approximately 178 anthrax threats received at courthouses, reproductive health service providers (clinics offering abortion services or counseling), churches, schools, and post offices. During FY 2001 we have had only approximately 60 threats or hoaxes, which included anthrax, hoof and mouth disease, the Klingerman virus hoax, and others.

Chemical and biological weapons are sometimes referred to as the “poor man’s nuclear weapons” and pose a significant threat in the post-Cold War environment. The relative low cost and simplicity of design and technology make them weapons of choice for a variety of rogue states and terrorist and non-state organizations. Although acts of chemical and biological terrorism have not been prevalent in the U.S. up to now, use of these weapons or the threat of their use are disruptive forces.

The Federal Bureau of Investigation (FBI) has been designated as the lead Federal Agency for crisis management in all acts of terrorism and uses or threats of harmful biological or chemical weapons.

III. WHAT SHOULD I DO IF I RECEIVE A SUSPECT ANTHRAX THREAT BY MAIL?

- Do not handle the mail piece or package suspected of contamination.
- Notify your supervisor, who will immediately contact the Inspection Service, local police, safety office, or designated person.
- Make sure that damaged or suspicious packages are isolated and the immediate area cordoned off.
- Ensure that all persons who have touched the mail piece wash their hands with soap and water.
- Notify your local law enforcement authorities.
- 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 Inspection Service.
- Place all items worn when in contact with the suspected mail piece in plastic bags and have them available for law enforcement agents.
- As soon as practical, shower with soap and water
- Notify the Center for Disease Control (CDC) Emergency Response at 770-488-7100 for answers to any questions.

IV. WHAT IS ANTHRAX?

Anthrax is a bacterial, zoonotic disease caused by Bacillus Anthracis. Anthrax occurs in domesticated and wild animals, including goats, sheep, cattle, horses, and deer.

The skin form of the disease may be contracted by handling contaminated hair, wool, hides, flesh, blood or excreta of infected animals and from manufactured products such as bone meal. Infection is introduced through scratches or abrasions of the skin, wounds, inhalation of spores, eating insufficiently cooked infected meat or from flies. *The spores are very stable and may remain viable for many years in soil and water.* They will resist sunlight for varying periods.

V. WHAT ARE THE SYMPTOMS AND EFFECTS OF ANTHRAX?

After an incubation period of 1-7 days, the onset of inhalation anthrax is gradual. Possible symptoms include:

- **Fever**
- **Malaise**
- **Fatigue**
- **Cough**
- **Mild chest discomfort followed by severe respiratory distress**

This mild illness can progress rapidly to respiratory distress and shock in 2-4 days followed by a range of more severe symptoms, including breathing difficulty and exhaustion. Death usually occurs within 24 hours of respiratory distress.

VI. WHAT ARE THE CLINICAL FEATURES OF ANTHRAX?

Anthrax is an acute bacterial infection of the skin, lungs, or gastrointestinal tract. Infection occurs most commonly via the skin.

The cutaneous or skin form occurs most frequently on the hands and forearms of persons working with infected livestock or contaminated animal products and represents 95% of cases of human anthrax. It is initially characterized by a small solid elevation of the skin, which progresses to a fluid filled blister with swelling at the site of infection. The scab that typically forms over the lesion can be black as coal, hence the name anthrax - Greek for coal. With treatment, the case fatality rate is less than 1% among people who get the skin form of the disease. The fatality rate for untreated inhaled or intestinal anthrax is over 90%.

The inhaled form of anthrax is contracted by inhalation of the spores, occurs mainly among workers handling infected animal hides, wool, and furs. Under natural conditions, inhaled anthrax is exceedingly rare, with only 18 cases reported in the United States in the 20th century.

VII. WHAT IS THE TREATMENT FOR ANTHRAX?

Treatment with antibiotics beginning one day after exposure has been shown to provide significant protection against death in tests with monkeys, especially when combined with active immunization. Penicillin, doxycycline, ciproflaxin, are all effective against most strains of the disease. Penicillin is the drug of choice for naturally occurring anthrax. If untreated, inhaled anthrax is fatal.

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 anthrax acquired through the skin, is also believed to be effective against inhaled spores.

Effective decontamination can be accomplished 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. Remember, anthrax spores are stable, able to resist sunlight for several hours and able to remain alive in soil and water for years.

VIII. WHAT CONSTITUTES A SUSPICIOUS LETTER OR PARCEL?

Some typical characteristics which ought to trigger suspicion include letters or parcels that:

- Have any powdery substance on the outside.
- Are unexpected or from someone unfamiliar to you.
- Have excessive postage, handwritten or poorly typed address, incorrect titles or titles with no name, or misspellings of common words.
- Are addressed to someone no longer with your organization or are otherwise outdated.
- Have no return address or have one that can't be verified as legitimate.
- Are of unusual weight, given their size, or are lopsided or oddly shaped.
- Have an unusual amount of tape on them.
- Are marked with restrictive endorsements, such as "Personal" or "Confidential."
- Have strange odors or stains

IX. WHAT SHOULD I DO IF I'VE RECEIVED A SUSPICIOUS LETTER OR PARCEL IN THE MAIL?

- Do not try to open the mail piece!
- Isolate the mail piece.
- Evacuate the immediate area.
- Call a Postal Inspector to report that you've received a letter or parcel in the mail that may contain biological or chemical substances.

X. HOW CAN I LIMIT PHYSICAL EXPOSURE OF THE MAIL ROOM TO SUSPECT ANTHRAX MAILINGS?

- Identify single point of contact to open mail.
- If possible, **DO NOT** open mail in area where other personnel are present.
- Have appropriate gloves available for individual use.
- Screen all mail for suspicious packages.

XI. ADDITIONAL RESOURCES:

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 WMD. The FBI will coordinate the Federal Government's efforts to prepare the nation's response community for threats involving Weapons of Mass Destruction (WMD). The WMD Unit works in conjunction with other Federal, State, and Local Crisis Managers specific to WMD and will perform an Interagency Threat Assessment. If a threat is received, please contact your local FBI office, FBI Special Information Operations Center (SIOC). Their Web site is http://fbi.gov.

The Centers for Disease Control and Prevention (CDC) is responsible for coordinating all public health and would be contacted at the Emergency Preparedness and Response Branch, National Center for Environmental Health to report an incident at 770-488-7100. Their Web site is http://cdc.gov.

MAIL BOMB SCREENING AND DETECTION: PLANNING YOUR RESPONSE

I. WHAT ARE THE CHANCES OF MY FIRM RECEIVING A MAIL BOMB?

The chances of your firm receiving a mail bomb are extremely remote. The chances are considerably greater of receiving a telephoned bomb threat or finding a suspicious and potentially harmful device placed at your office or on your property. The number of instances over the last six years has been minimal. By comparison, the U. S. Postal Service safely delivers five hundred million letters and packages every day.

The key is to have a comprehensive bomb threat response plan to deal with mail bombs, bomb threats, and suspicious placed devices. When properly planned and implemented, a bomb threat response plan will prevent any such incident from creating panic among your workforce or inflicting physical harm to your employees or facilities.

Postal inspectors are the experts in mail bomb detection and investigation. We offer the following suggestions to help you formulate a comprehensive bomb threat response plan that addresses bomb threats and placed devices. We also offer a ten-step mail bomb screening program to help your mail center personnel detect suspicious devices in the U.S. mail or delivered by private courier.

II. HOW VULNERABLE IS MY FIRM?

The vulnerability of you and your firm depend on a variety of factors – both internal and external. Experience has shown that no individual or organization is completely immune from attack. A sound assessment of your vulnerability is critical to the preparation of a bomb threat response plan.

Consider the following possible sources of danger in evaluating your firm's vulnerability:

- Foreign terrorism

  Does your firm have foreign officers, suppliers, or outlets? If so, in what countries? Are you doing business in countries where there is political unrest or civil strife?

- Domestic hate groups

  Is your firm a high-profile organization whose services, research, or products are the subjects of public controversy?

- Workplace Violence

Has your firm 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 firm itself?

Positive answers to any of these questions will help you and your security manager identify potential sources of bombs or bomb threats.

III. WHAT MOTIVATES PEOPLE TO SEND MAIL BOMBS?

There is a popular stereotype of the typical mail bomber as a person motivated by radical political beliefs. This stereotype is incorrect and it may cause your organization to improperly assess and respond to existing threats. Law enforcement authorities find that revenge is the motivation which most often "triggers" a mail bomb or bomb threat.

Jilted spouses or lovers may seek revenge when their romantic involvement is finished. Former business partners or employees may seek revenge when a business relationship goes sour, or 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 that have been investigated or prosecuted.

Postal inspectors have found that mail bombs generally target specific individuals. Placed devices, however, are generally intended to disrupt organizations and injure indiscriminately. Bomb threats may target either individuals or organizations.

IV. HOW CAN I DETERMINE IF SECURITY PRECAUTIONS AT MY FIRM ARE ADEQUATE?

Good question! Your bomb threat response plan should be part of an overall corporate security program, addressing all personnel and physical security issues. If no such plan exists, your firm must appoint individuals from corporate management and security to formulate the bomb threat response plan.

Postal inspectors recommend including the mail center manager, or a designee, in the planning group because that person, as Mail Center Security Coordinator, will be responsible for the mail bomb-screening program.

Command Center Organization

Representatives from corporate management, security and the mail center should form the nucleus of a Command Center working group to deal with any emergency where bombs or bomb threats must be confronted. Members of the Command Center working group, and their alternates, should be specified by name and title. Most importantly, Command Center members should have authority to make important decisions as to how the firm will respond to any bomb threat situation, including evacuation of company facilities.

The Command Center must be at or near the communications center of the firm. The Command Center should be equipped with telephone numbers for police, postal inspectors, the Bureau of Alcohol, Tobacco and Firearms (BATF), the fire department, and emergency medical

services. An employee roster with all current telephone numbers, including home, office, pagers, and cellular telephones should be maintained. Current copies of the firms' floor plans or building blueprints are also of critical importance.

Preparation should include planning for evacuation routes and alternates, easily adapted from fire escape routes, and evacuation signals. Evacuation routes should be furnished to all supervisors. However, we recommend fire alarms 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.

Your local police and fire departments should be contacted about their respective bomb search policies. In the event of a threat, will they help conduct the search? If so, what will they need from your Command Center?

The bomb threat response plan must include provisions to ensure that non-postal deliveries (except commercial shipments) are channeled through the mail center. Since all organizations receive mail and other parcel deliveries, a mail bomb-screening program through which all parcel deliveries are channeled is an essential component of this process.

By the same token, telephone threats received by company receptionists, or others, should be brought to the attention of the security officer and then relayed to the mail center manager, who needs to be informed of any specific information which would assist the mail bomb screening process.

Lastly, the bomb threat response plan should encompass all facilities at the site, including outbuildings, and parking lots or garages immediately adjacent to buildings occupied by employees. If the firm maintains offices at multiple sites, security officers at each site must be included in the communications loop.

Postal inspectors highly recommend consultations with security experts knowledgeable in terrorist tactics and vulnerability assessment.

V. WHAT ABOUT THE DANGER OF BOMBS PLACED AT OUR OFFICE?

Since the majority of explosive devices are **placed**, not mailed, it is imperative that your security plan includes sound controls over those that can physically gain access and move about your facility and the immediate surroundings. Such steps can reduce much of your risk.

Physical Security

Consider the following suggestions:

- Have security guards greet all visitors and examine personal belongings being brought into the building or office area.
- Restrict access to the facility or office through locked or guarded entryways.
- Keep storage rooms, boiler rooms, telephone & utility closets, and similar hiding places locked or "off-limits" to visitors.

- Use easily distinguishable identification badges for staff personnel and for visitors.

- Require visitors to be accompanied by staff employees to and from the office or facility entrance.

- Request visitors to display identification to security personnel when they sign in (keep detailed logs on all visitors' times of arrival and departure).

- Consider using the services of a Certified Protection Professional to evaluate your firm's personnel and physical security safeguards in detail.

VI. WHAT ABOUT BOMB THREATS?

Your firm's bomb threat response plan must address the possibility of receiving bomb threats in writing or by telephone. While all threats should be taken seriously, your firm's response may depend on the circumstances present at any given time.

Each bomb threat presents three basic options:

1. Evacuate everyone immediately and search;
2. Evacuate some employees while a search is undertaken; or
3. 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 will probably result in false alarms placed by employees anxious to exploit the policy. It is better to judge the credibility of each threat individually. The decision to evacuate all or part of the facility should be made by the command center-working group. Whatever the policy, it should not be publicized.

Written threats provide physical evidence which 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. Telephone threats offer an opportunity to obtain more detailed information, perhaps even the caller's identity. For that reason, telephone receptionist or others who take calls from the public should be trained to remain calm and to solicit as much information as possible. They should keep the caller on the line, asking him to repeat the message several times, and attempt to gather additional information, such as caller ID information, etc.

Telephone receptionists should be trained to remain calm and ask the following questions:

- 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?

Enclosed is a Publication 54, Bomb Threat form for recording telephone bomb threats.

The bomber's intentions may be to damage property, not injure or kill anyone. If so, the person receiving the call may be able to obtain useful information before the caller ends the conversation. Under no circumstances should the person taking the call hang up if the caller is still on the line.

The person taking the call should write down the threat verbatim, in the caller's own words, and record any additional information as indicated on Pub. 54. Once the threat has been received, corporate security and management must decide on the proper response such as evacuation procedures. Police and fire departments should be notified immediately.

Searches may be conducted by individuals from within the firm who have volunteered for such duty, but they must be trained for this purpose. Remember, police agencies often **will not** conduct searches of private facilities. You and your employees know your facility and are more likely to observe unusual items that police and fire personnel could overlook.

Search Team Deployment

If your local police and fire departments will not assist in the search for an explosive device, company search teams will have to be deployed. Teams 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.

Search techniques should be kept confidential and training should be limited to employees with a "need to know."

Search teams should be outfitted beforehand with a few elementary tools, such as screw-drivers, 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.

A complete building search should begin with the areas most accessible to the public. Typically, this means beginning with the building's exterior and moving indoors through the main entrance or lobby to waiting rooms, rest rooms, stairwells, and elevators.

Once inside, a two-employee team should begin its search at the same point and work in opposite directions around the room or office back to the center of the room.

They should begin at floor level and work their way up in four-foot increments. The search patterns should overlap somewhat. This process should be repeated in a methodical manner from office to office and from floor to floor throughout the facility. If a suspicious item is found, the area should be cordoned off and the police called. Once cleared, the search should 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.

Under no circumstances should volunteers attempt to handle or remove suspicious devices.

VII. WHAT IF A SUSPICIOUS PARCEL OR DEVICE IS FOUND ON OUR PROPERTY?

We recommend incorporating procedures into your bomb threat response plan for dealing with suspicious placed devices. These devices have been handled in the delivery system and are not likely to explode merely by moving them to a safer location.

Therefore, some of these actions differ from recommended tactics concerning mailed devices or those delivered by courier.

For suspicious items found placed on your property:

- Do not touch the suspicious device. It may "trigger" a detonation.
- Report the situation to your security office immediately.
- 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 or a timing mechanism may be set to activate the device within minutes of placement.
- If possible, open windows to minimize the effect of any concussion caused by detonation.

VIII. HOW DO WE SCREEN MAIL AND OTHER PACKAGES DELIVERED TO THE MAIL CENTER?

Postal inspectors have devised a mail bomb screening program that can be adapted to virtually any mail center operation, regardless of the size of the firm. To be successful, the mail bomb-screening program depends on a well-trained mail center staff, good communication within the firm's management, security and mail center, and the cooperation of employees at every level.

The **KEY POINTS** which follow will guide the mail center manager or security manager through the ten steps necessary to establish a mail (and privately delivered package) bomb screening program.

KEY POINTS

1. Perform a vulnerability assessment to determine if your organization or a particular employee is a potential target.

2. Appoint a Mail Center Security Coordinator and an alternate to be assigned responsibility for and to ensure compliance with the developed plan.

3. Establish direct lines of notification and communication among the mail center security coordinator, management, and security office.

4. Develop specific screening and inspection procedures for all incoming mail or package deliveries and train employees in those procedures.

5. Develop specific mail center handling techniques and procedures for items identified through screening as suspicious and dangerous.

6. Develop verification procedures for confirming the contents of suspicious packages encountered through the screening process.

7. Designate an isolation area for use with suspicious packages encountered through the screening process. Establish a safety zone around the isolation area.

8. Construct a holding container for suspicious packages.

9. Conduct training sessions for mail center, security and management personnel to validate the practicality of all phases of the Mail Bomb Screening Program.

10. Conduct unannounced tests for mail center personnel.

IX. BOMB SCREENING PROGRAM

Vulnerability Assessment

The security officer and top management should meet to evaluate the probability of your organization or its personnel becoming targets for mail bombs and bomb threats. The following are typical questions asked during this assessment. They can be used to develop any 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 individual employees' privacy, and all information should be treated as extremely sensitive. This information should be shared with the mail center security coordinator in the event a suspicious package is received, but should not be disseminated to other employees.

- Does your organization provide products, materials, technical assistance, or operate facilities within any country involved or connected with current terrorist activity or any government suffering domestic unrest?

- Has your organization 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 represent countries suffering domestic unrest?

- Does your organization manufacture or produce weapons or military support items for international arms trade that would normally bear markings identifying the organization as the manufacturer?

- Does your organization support political or social causes that would make it a likely target for radical domestic "hate" groups?

- Has any member of your organization's management made public statements or authored papers on any facet of current terrorist activity or topics, or taken any controversial public position?

- Has any employee advised that he or she has been the target of physical violence or harassing activities such as threatening phone calls or threats?

- Has any employee (current or former) threatened violence against either the organization or another employee in connection with a real or alleged grievance?

Appointment of the Mail Center Security Coordinator

Management should ensure that the mail center security coordinator (the coordinator) and an alternate are mature, responsible, and emotionally stable. This selection should be made from those persons already participating and trained in the overall bomb threat response plan.

Duties of the mail center coordinator:

- The coordinator must oversee the mail bomb screening process, seeing that all deliveries are channeled to the mail center, train employees in detecting suspicious packages, verifications, safe handling, and communications with security and management in any crisis.

- The function of the coordinator is to assume command of the situation when a suspicious package is identified by mail center employees in the screening process.

- The coordinator is initially responsible for seeing that personnel who have detected the suspect postal item place sufficient safety distance between themselves and the item and those employees, in general, do not cluster around the item out of curiosity.

- The coordinator will then notify management directly and provide them with specific details of the item and carry out the remaining steps of the plan under the direction of management and security.

Direct lines of communication are vital

Direct channels of communication between the mail center security coordinator, management, and security is vital.

A "command center" of management and security representatives should be the focal point of communications when the bomb threat response plan is operational. The mail center security coordinator must be able to communicate directly with managers in this command center.

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

Screening procedures

Incoming mail in any organization follows much the same pattern. Bags or bundles of mail, and other courier deliveries are delivered to a centralized mail center for distribution. (If this centralized receiving procedure is not currently in operation, steps should be taken to institute such a program immediately). The actual initial sorting of the mail for delivery to units, divisions, or individuals must be done by hand, with each item being picked up, its address read, and the mail item placed into its proper distribution box for delivery.

This is the point where screening of incoming mail for suspect items should occur and those individuals who normally handle this mail sorting function should perform the screening. This is critical because those individuals are most likely to notice packages that are out of the ordinary.

This procedure can also be used when an employee who has already received the package is concerned that it may contain an explosive device. This normally results from some personal situation that may or may not have been brought to management's attention.

Based upon past patterns of mail bomb construction, packaging, mailing, and addressing, the screening of incoming mail should involve the search for those items of mail which have one or more of the recognition points listed on the enclosed *Poster 26, Letter and Package Bomb Indicators.* Please display this poster in your mail room.

It is important to remember that the general screening procedures of incoming mail and packages are by no means foolproof. **In many cases, the only person to detect anything suspicious about a package is the ultimate recipient.** For this reason, these same mail bomb recognition points should be distributed company wide to all employees to increase employee sensitivity to this threat. Your vulnerability assessment should dictate the degree of heightened awareness to the danger of mail bombs and identify the employee for whom this training would be most beneficial.

IMPORTANT

Because of the increased sophistication of mail and placed bombs, fewer of the devices can be readily identified by merely examining the exterior of the package. Employees should be told:

- If they are not expecting a package, be suspicious.
- Check the return address, if they do not recognize the return address, contact the security office (which will attempt to contact the sender).
- **DO NOT OPEN THE PACKAGE** until satisfied it is harmless.

X. RESPONSE PROCEDURES FOR SUSPECTED MAIL BOMBS ENCOUNTERED DURING SCREENING

A. Upon notification that a suspicious package has been found, the mail center coordinator should:

1. Ask the employee 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 the remaining employees a suspicious package has been found, the points of recognition, and to remain clear of the isolation area.
3. Place suspect item in reinforced container and take it to the isolation area.

4. Record from each side of the item all the 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).

(<u>IMPORTANT NOTE</u>: *Be sure to copy information in exact spelling and location on item.)*

5. Contact management and security and inform them a suspicious item has been detected through the screening process.

6. Inform the police and postal inspectors (if mailed) giving all information recorded from the suspect item.

B. When management or security receives the notification from the mail center coordinator, their actions should, in general, follow these guidelines:

1. Accurately record all information pertaining to the suspect item in an incident log.

2. If at all possible, dispatch a security officer with a Polaroid camera to photograph all sides of the suspect item, without moving it, as it rests in the holding container. Exact details of the item markings are thus made available for study and use by the bomb scene officer.

3. Contact the addressee of the suspicious package for verification of the item by asking specific questions. (Verification questions are presented below.)

4. Attempt to resolve the verification by contacting the “sender” as indicated on the suspicious package’s return address.

5. If the return addressee proves to be fictitious, or you cannot locate the sender within a reasonable period of time, notify the police and postal inspectors 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.)

6. Notify appropriate management level personnel of the detection, through mail screening, of a suspicious package.

7. Stand by to offer in-house assistance to the police and postal inspectors upon their arrival.

Verification of suspect package by addressee and/or sender

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, it may be opened by security with relative safety. 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.

Below are sample 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 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 other 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 the city, state, or country of origin?

If the verification process determines that the sender is unknown at the return address, or the return address is fictitious, consider that as a very serious indication that the parcel may be dangerous.

Establishing an isolation area for suspicious packages

When the mail screening process identifies a suspect item, it is essential to rapidly remove personnel from the area and the potential bomb from the workflow. The potential bomb should be placed in an area of isolation. Security personnel and the mail center coordinator should jointly evaluate the spaces or areas available around the mail center and select one which offers a degree of isolation where a parcel may be placed pending verification and/or the arrival of the police. In selecting and creating the isolation area, the following points should serve as general guidelines:

- The isolation area should be easily accessible from the mail screening area.

- While hand transporting a suspect postal item from the screening area to the isolation area, it should not be necessary to move into or through areas of high employee population or heavy traffic.

- If at all possible, access to the isolation area should not involve the opening of doors, climbing of stairs, or passage through areas of clutter or poor illumination.

- The total distance from the mail screening area to the isolation area should not exceed 50 yards.

- The isolation area should, whenever possible, be located outdoors and sheltered from the elements (a covered loading dock or an open shed area).

Construct holding/carrying containers

A holding/carrying container should be available in settings where no loading dock or outside covered area is available to hold a suspicious item until police or postal inspectors arrive. It should be placed away from high traffic areas where other employees are working. The container should be constructed of heavy wood or exceptionally strong plastic (not metal) and light enough for one or two individuals to carry. The container is not intended to contain an explosion, but it would help direct the force of any explosion away from other employees, flammables, or windows. It is extremely important that the container be well ventilated.

Testing

We cannot overemphasize the need to test contingency plans with mock suspicious parcels placed in the mail center or elsewhere in the facility. Naturally, these tests should be conducted in such a manner as to not alarm employees. These “dress rehearsals” help ensure that your lines of communication function as planned and that everyone who has a role to play knows his part.

There is no better way to test the efficiency of an emergency contingency plan than to conduct scheduled tests. Hold post-testing meetings to go over problems and resolve them before the next test. Use the Bomb Threat Response Plan key points checklist on page 16 to periodically review your firm’s preparations.

XI. SUMMARY

A successful mail bomb response plan begins with a commitment from your organization to protect its employees and their working environment. The plan cannot succeed without the cooperation of many different individuals involved in the process of establishing and maintaining a safe work environment. The mail center manager’s role should be a significant one in this effort. The Postal Inspection Service can provide assistance to help you achieve your goals.

BOMB THREAT RESPONSE PLAN:

KEY POINTS CHECKLIST

[ ] Bomb threat response plan complements overall physical security plan. Are the premises secured against unauthorized entry?

[ ] Command Center Staff should include corporate management, security, and mail center security coordinator. First step is to perform vulnerability assessment.

[ ] Command Center Staff must have authority to deal with any threat received and to order evacuation.

[ ] Equip Command Center with telephone numbers of police, fire department, 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 mail center.

[ ] Train mail center employees to recognize suspicious parcel and mail bomb characteristics during screening.

[ ] Advise all employees to contact mail center if they receive a parcel they are not expecting and which cannot be explained

DO NOT OPEN ANY PARCEL UNTIL VERIFIED TO BE SAFE

UNITED STATES POSTAL SERVICE

PLEASE POST

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