



# Best Practices for Safe Mail Handling

Interagency Security Committee



Homeland  
Security

## INTRODUCTION

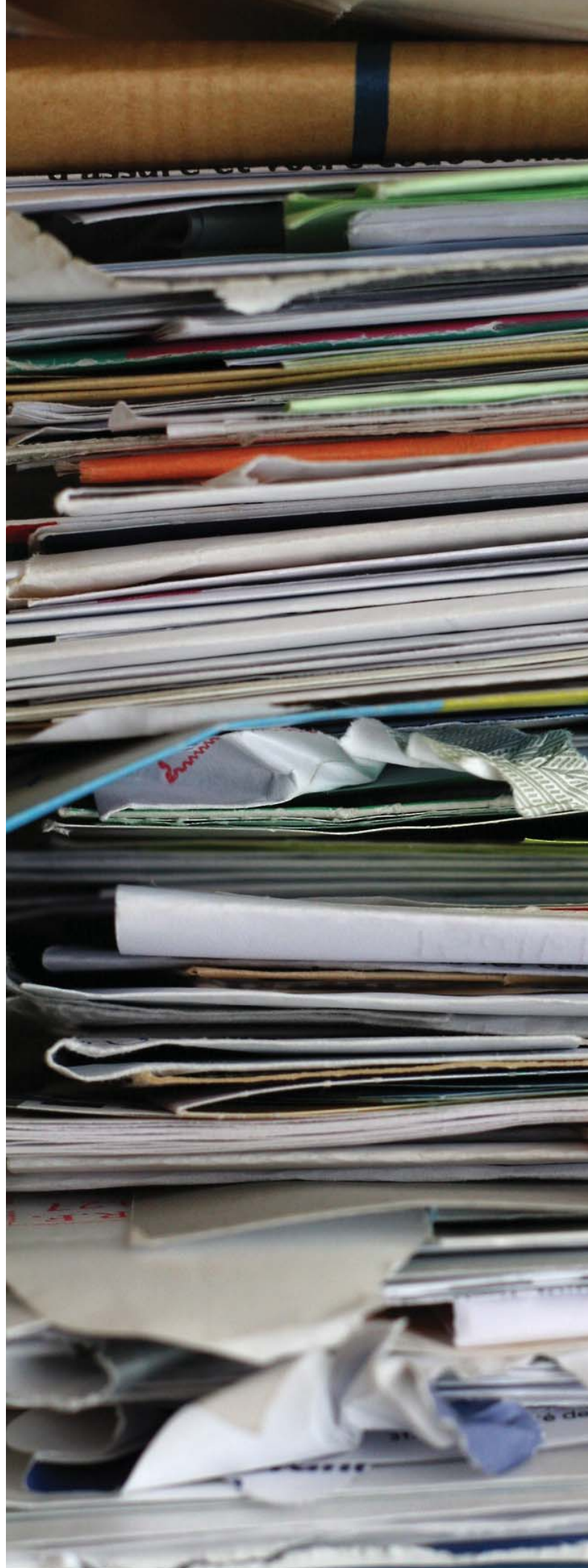
With the anthrax mailings of 2001, federal agencies have come to realize their mail centers may be the first point of attack by terrorists, either domestic or foreign. Federal agencies cannot assume these attacks will never be repeated; therefore, agencies must take the appropriate actions to mitigate risk.

The government processes hundreds of billions pieces of mail each year without incident; however, federal agencies must prepare for the worst case scenario. Threats can never be eliminated. For that reason, risk is the primary determinant of the degree to which agencies determine how security needs are to be met.

This Interagency Security Committee (ISC) document contains suggested information on government mail center operations that federal agencies can use to meet their needs. The document also contains some best practices for mail center operations that can assist security managers in establishing the best procedures for safe mail handling in their operations across the nation.

Although suggestions provided are applicable for many situations involving security threats, they are intended only as guidance. This document represents a compilation of information already available from open sources such as the CDC, GSA, and Postal Service websites, publications, and visits to federal mail centers (see Appendix A). The document also addresses dangerous mail handling and recommends preventive measures that agencies may implement to handle and deliver mail safely to their personnel.

The safe handling of mail can be expensive and time-consuming. Safe mail handling covers a broad spectrum and various approaches can be taken to provide security. There is no “One Size Fits All” solution for safe mail handling. Each operation must incorporate security measures that best mitigate the risk associated with each unique facility. The ISC will continue to explore innovative technologies that will effectively prevent, detect, and neutralize risks in mail centers.



## RISK ASSESSMENT

Assuming a comprehensive risk assessment has been completed on the facility in which the mail handling operations are housed and appropriate mitigating security measures have been established or identified for future implementation, the primary determinant for deciding safe mail handling requirements is a risk assessment on the mail handling operations themselves. This risk assessment should focus on the mail handling facility (room, area, etc.) and the processes and operations governing the handling of mail. The assessment should include the jobs, tasks, and personnel that would most likely be jeopardized if a suspicious or dangerous envelope or package entered the mail handling facility, or the agency's workplace.

All mail handling facilities have different risk levels. Guidance put forth in this document should be used, as appropriate, for the facility's mail handling risk level. Each agency's security professionals should collectively identify the most effective approach to reduce vulnerabilities, deter threats, and minimize the consequences of an incident. Many measures can be implemented immediately. Others require time and effort. Primary consideration should be given to your agency's mission or the mission of other tenant agencies that may make your facility a prime target. The risk assessment of the overall facility and mail handling operations should include the adequacy of state and local governments' response capabilities.



## MAIL HANDLING AND PROCESSING OPERATIONS

The first and best practice to minimize risk and exposure to personnel and the public is centralizing the mail handling/processing operation at a separate location. Centralization minimizes risk, reduces cost, and increases efficiency and effectiveness. It lessens risk by limiting exposure to one location and fewer personnel. It reduces cost by eliminating the redundancy of multiple mail centers, personnel, and equipment. Utilization of a trained staff working together at one location increases efficiency. Deploying better equipment at one location that greatly enhances risk reduction improves effectiveness.

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 sort the mail should perform the screening function. As such, these individuals are most likely to notice packages that are out of the ordinary. 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, each agency should distribute a list of suspicious package indicators to all personnel to increase their awareness of suspicious packages.



FIRST CLASS

# BEST PRACTICES

## best practices

Regardless of the number of mail handling locations, agencies should consider utilization of these best practices:

### Basic Steps

- Employ professional security personnel
- Security personnel should greet all personnel and visitors and examine personal belongings
- Restrict access to the facility to authorized users only
- Keep detailed logs of visitor arrivals and departures
- Install an intrusion detection system
- Use CCTV to record and store unobstructed surveillance of operation areas and exterior
- Ensure adequate lighting for operations area, exterior and CCTV
- Use easily distinguishable badges for staff and visitors and require that they be displayed
- Accountability for lock and key control should be in place
- Keep storage areas, boiler rooms, and telephone utility closets off limits to visitors
- Develop an emergency plan for response to a known or a suspected hazard
- Train workers to recognize and handle a suspicious piece of mail
- Identify a single point of contact to open mail
- Restrict drivers and deliveries to a specific area
- Establish a communication channel to report security deficiencies
- Screen all incoming mail
- Do not open mail in an unauthorized area
- Develop specific screening and inspection procedures for all incoming mail or package deliveries and train personnel in those procedures
- Develop specific mail center handling techniques and procedures for items screened and identified as suspicious and dangerous
- Develop verification procedures for confirming the contents of suspicious packages encountered through the screening process
- Establish procedures for isolating the suspicious package
- Conduct training sessions for mail room, security, and management personnel
- Conduct unannounced tests for mail center personnel
- Have appropriate protective wear available for mail handler's use:
  - Gloves
  - Masks
  - Smock
  - Protective glasses
- Know the number, location, time and response ability of the local HAZMAT team
- Conduct a "hot wash" and after-action review immediately following an event and produce a written report with follow-up corrective actions or process improvements

As the risk assessment dictates and budgets allow, programs should be augmented with additional countermeasures. The ISC will continue to research new technology that will lower risk and enhance safety.

## Enhanced Steps

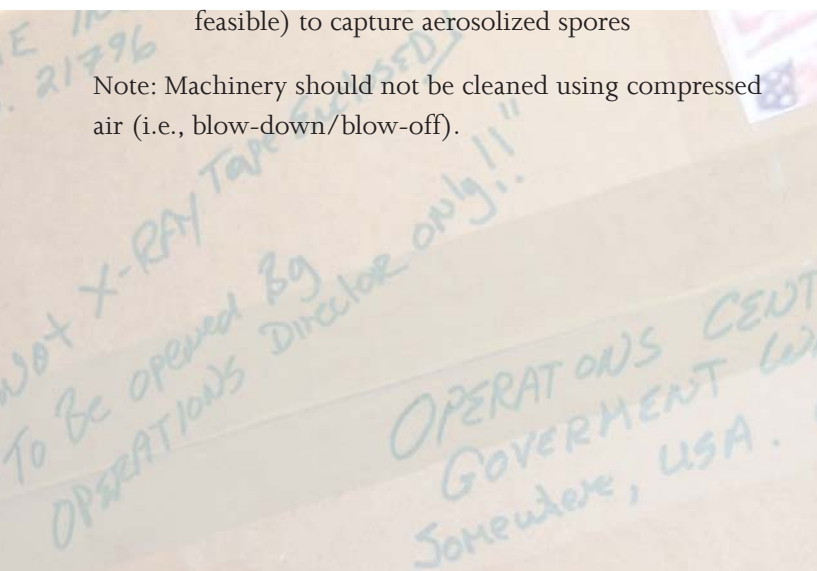
- Bomb detection / K-9
- X-ray all incoming mail
- Detection devices
  - Biological
  - Chemical
  - Radiological
- Hold mail 24 hours or until testing concluded
- Store mail in containment containers
- Down draft tables
- Separate air filtration unit
- Monitored mail operations
- Safe air room for mail processing
- Monthly swab testing of mail room
- Showers or decontamination system
- Wear protective clothing
- Duress alarm

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

- An industrial vacuum cleaner equipped with a high-efficiency particulate air (i.e. HEPA) filter for cleaning high-speed, mail-sorting machinery and local exhaust ventilation at pinch roller areas
- 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
- 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., blow-down/blow-off).

**The government processes hundreds of billions pieces of mail each year without incident; however, federal agencies must prepare for the worst case scenario. Threats can never be eliminated.**



## Continuity of Operations Plan

Implementing anticipatory measures is more likely to mitigate the negative effects of an event. Each federal agency mail center should have a back-up site or alternate location identified in their Continuity of Operation Plan (COOP) to enable mail processes to continue its essential functions. It is absolutely fundamental for each agency to be able to receive and send out mail if the primary mail operation has to be shut down. Advanced planning is a very important element for security protection.

### Recommended Measures Based on Project Specific Risk Assessment

Recommendations	Low and Moderate Risk Facilities	High Risk Facilities
Appoint a Mail Security Coordinator	✓	✓
Appoint an alternate Mail Security Coordinator		✓
Organize a Mail Security Response Team, as practical, depending on the size of the mail center staff		✓
Create, update, publish and review SOPs, Security Procedures, Disaster Plans, and Operating Plans	✓	✓
Keep a back-up copy of plan(s) off-site		✓
Staff, when possible, certified firefighters, biohazard handlers, and/or safety, environment and health personnel, or, train personnel in these duties; or establish a written agreement with a service provider to provide this capability		✓
Train personnel in policies and preventive procedures relative to mail security, i.e. biological, chemical, weapons or natural disasters	✓	✓
Limit access to personnel	✓	✓
Identify and escort visitors	✓	✓
Install intrusion detection system		✓
Establish HAZMAT response plans	✓	✓
Establish a relationship with local HAZMAT emergency service	✓	✓
Medical care available on-site		✓
Members of the team should be equipped with cell phones/pagers and available 24/7 days as appropriate for the situation		✓
Information, personnel updates, and response procedures should be published and distributed agency-wide		✓
Post SOP on handling suspicious packages	✓	✓
Maintain, publish and post phone numbers to call in an emergency - Postal Inspectors, Fire Dept., CDC, OSHA, Police, FBI, etc. (Contact one number at onset of the event. The responding Incident Commander will determine the appropriate follow-up notifications.)	✓	✓
Distribute updated Best Practices from CDC, OSHA, GSA, USPS, and Fire Department	✓	✓
Install CCTV cameras at entrances and exterior		✓
Install intrusion detection system	✓	✓
Require personnel to attend all local meetings pertaining to mail security issues		✓
Publish an After-Action Report or Incident Report after every incident with a plan for corrective action or process improvement		✓
Senior management should buy-in/sign-off on mail security procedures	✓	✓

## Mail Center Personnel Security Procedures

Recommendations	Low and Moderate Risk Facilities	High Risk Facilities
Provide in-depth screening/background checks when hiring new personnel	✓	✓
Make arrangements with employment agencies to ensure that a restricted, pre-screened group of individuals are available when needed to supplement the workforce		✓
Enforce/institute probationary period for evaluation of personnel	✓	✓
Establish a strict identification/personnel security program		✓
Require personnel to wear photo ID badges at all times	✓	✓
Instruct personnel to challenge any unknown person in a facility	✓	✓
Provide a separate and secure area for personal items (e.g., coats and purses). Prohibit personnel from taking personal items into the main workspace		✓
Establish incoming/outgoing personal mail procedures	✓	✓
Hire or designate security personnel for mail center area		✓
Establish health and safety procedures	✓	✓
Have on-site medical personnel or arrange for off-site facility/personnel	✓	✓
Encourage personnel to wash hands regularly	✓	✓
Encourage personnel to see a doctor if suspicious symptoms occur	✓	✓
Encourage personnel to attend health seminars, talks, info updates		✓
Provide approved personal protection equipment according to CDC guidelines	✓	✓

## TRAINING

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

1. Through training you can develop a culture of security awareness in your operation. Training is essential to ensure employee confidence in their safety. Managers should consider security training a critical element of their job. Additional guidance for suspected anthrax contamination is contained in Appendix B.
2. A complete training program will include:
  - a. Basic security procedures;
  - b. Recognizing and reporting suspicious packages;
  - c. Proper use of personal protection equipment;
  - d. Responding to a biological threat; and
  - e. Responding to a bomb threat.
3. Maintain a log of all employees and training attended, including the date completed. Follow up with refresher training on a regular basis.
4. In addition to educating the employees who work for you, you must educate all employees who work in the facility on best mail practices including security measures. Employee awareness of the measures you have taken leads to confidence in the safety of the packages that are delivered to their desktops.

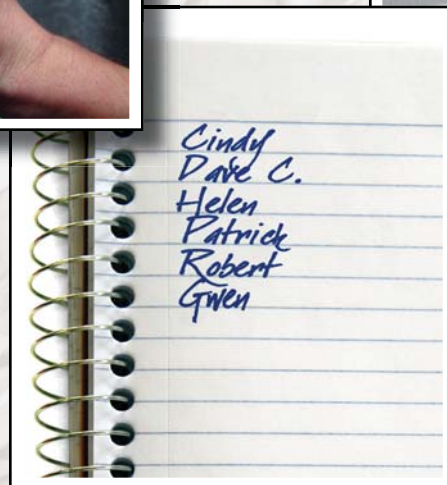
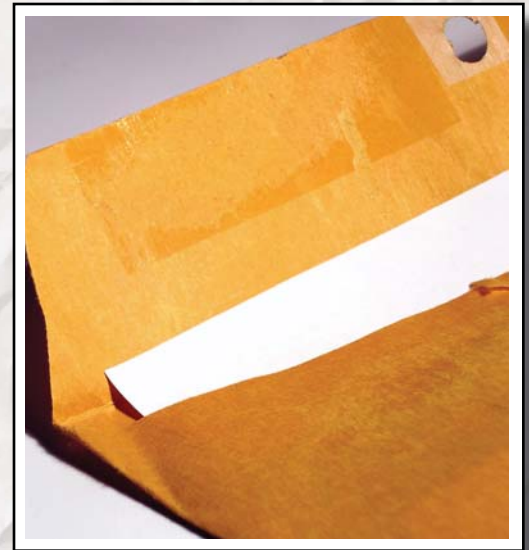
## Plan Review

Periodic training and exercises are vital to successful implementation of security policies. A well-trained staff can minimize the impact of dangerous mail handling. All training should place emphasis on life safety, security communication, efficiency, and roles and responsibilities to minimize risk.

The ISC strongly recommends an external review of your security plan. This may include a review by a security consultant, your agency security department, or a peer review.

Personnel suspicious of a letter or parcel should be trained to take the following measures:

- Be wary of unexpected packages and check the return address
- Notify their supervisor, security personnel, or local law enforcement
- Do not shake or bump the item
- Do not open, smell, touch, or taste
- Isolate the damaged or suspicious item immediately
- Cordon off the immediate area
- Ensure that all persons who have touched the mail piece wash their hands with soap and water
- List all persons who have touched the item, include contact information and have this information available for the authorities
- Place all items worn when in contact with the suspected mail piece in plastic bags and have them available for law enforcement agents
- Shower with soap and water as soon as practical



## Some Protective Measures for Suspicious Letters or Parcels

### Powder and Powder Spills

- Do not clean up the powder
- Cover the spilled contents immediately with anything (e.g., clothing, paper, trash can, etc.) Do not remove this cover!!!
- Leave the room and close the door, or section off the area to prevent others from entering
- Wash your hands with soap and water to prevent spreading any powder to your face
- Do not eat, drink, or smoke around suspected mail
- Notify your building security official or an available supervisor and report the incident to local enforcement
- Remove contaminated clothing as soon as possible and place in a plastic bag, or some other container that can be sealed, and give it to the emergency responders for proper handling
- Shower with soap and water as soon as possible



**Do not use bleach or other disinfectant on your skin.**

If possible, list all people who were in the room or area, especially those who had actual contact with the powder. Give this list to both the local public health authorities so that proper instructions can be given for medical follow-up, and to law enforcement officials for further investigation.

### Air Contaminates

- Turn off local fans or ventilation units in the area
- Leave area immediately
- Close the door, or section off the area to prevent others from entering
- Notify your building security official or an available supervisor and report to local police and FBI
- Shut down air handling system in the building, if possible

If possible, list all people who were in the room or area. Give this list to both the local public health authorities so that proper instructions can be given for medical follow-up, and to law enforcement officials for further investigation.

### Suspicious Packages and Possible Letter Bombs

Mail bombs may bear restricted endorsements such as “Personal” or “Private.” These characteristics are important when the addressee does not usually receive personal mail at the office.

Mail bombs may have distorted handwriting, or the name and address may be prepared with homemade labels or cut-and-paste lettering.

Letter bombs may feel rigid, or appear uneven or lopsided.

If you are suspicious of a mailing and are unable to verify the contents with the addressee or sender:

- Do not open it
- Treat it as suspect
- Isolate it
- Contact building security
- Call the police
- Call your postal inspector



## Quick Reference

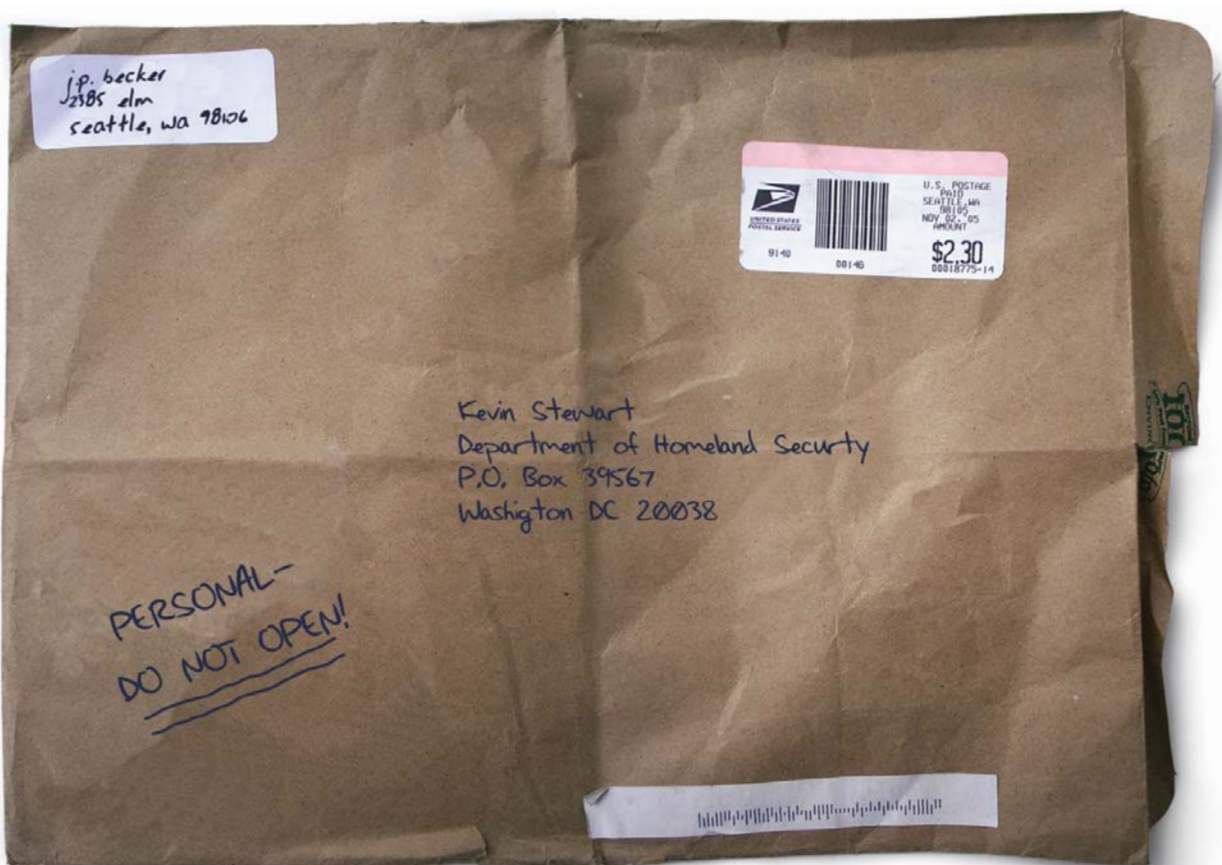
For a Bomb	For Radiological	For Biological or Chemical
<ul style="list-style-type: none"><li>• Evacuate immediately</li><li>• Call Police</li><li>• Contact postal inspectors</li><li>• Call local Fire Department- HAZMAT Unit</li></ul>	<ul style="list-style-type: none"><li>• Limit exposure - don't handle</li><li>• Distance (evacuate area)</li><li>• Shield yourself from object</li><li>• Call Police</li><li>• Contact postal inspectors</li><li>• Call local Fire Department- HAZMAT Unit</li></ul>	<ul style="list-style-type: none"><li>• Isolate - don't handle</li><li>• Wash your hands with soap and warm water</li><li>• Call Police</li><li>• Contact postal inspectors</li><li>• Call local Fire Department- HAZMAT Unit</li></ul>

**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).**

## CONCLUSION

Threats to a mail handling operation can impact the entire facility as well as cause panic for the general population. It is fundamental to incorporate protection of the personnel and the facility with the identification of the threat. Many federal agencies have satellite facilities where mail operations are performed in a small room, one corner of a room, or one corner of a desk. At these facilities, responsibility for processing mail is divided among professional and support staff. Security plans for small facilities are, of course, limited by both the size of the facility and the resources available to develop and implement plans. Small facilities will therefore, adopt those recommendations from this document that are appropriate to them.

Best practices are dependent upon an agency's needs; there are too many variables to recommend a uniform mail handling process. Strategic objectives are useful to help policy makers develop the framework for facility specific goals. Every mail management program should include familiarity with 41 CFR Sections 101-9 and 102-192 for Mail Management (note compliance section on Subpart G – Facility Mail Managers). Each agency must evaluate its own situation and objectively weigh the threat circumstances in order to render a prudent decision.



# APPENDIX A

## appendix a

Visit these sites for additional resources:

Centers for Disease Control and Prevention  
<http://www.cdc.gov>

Federal Bureau of Investigations  
<http://www.fbi.gov>

Federal Protective Service/ISC Portal  
<https://fps.esportals.net>

FEMA's Rapid Response Information System (RRIS). This web site provides descriptions and links to eight major chemical and biological agent resources.  
<http://www.fema.gov/hazard/hazmat/index.shtm>

General Services Administration  
<http://www.gsa.gov/mailpolicy>  
41 CFR Parts 101-9 and 102-192 for Mail Management  
<http://www.gsa.oca.gov>

Occupational Safety and Health Administration. OSHA is the main federal agency charged with the enforcement of safety and health legislation.  
<http://www.osha.gov> and <http://www.osha.gov/SLTC/bioterrorism/pkghandling.html>

Office of Compliance  
<http://www.compliance.gov/emergency/safemailhandling.html>

U. S. Postal Service  
<http://www.usps.com>

# APPENDIX B

## appendix b

### Training Reference

Source: [http://www.usps.com/news/2001/press/pr01\\_1022gsa\\_print.htm](http://www.usps.com/news/2001/press/pr01_1022gsa_print.htm)

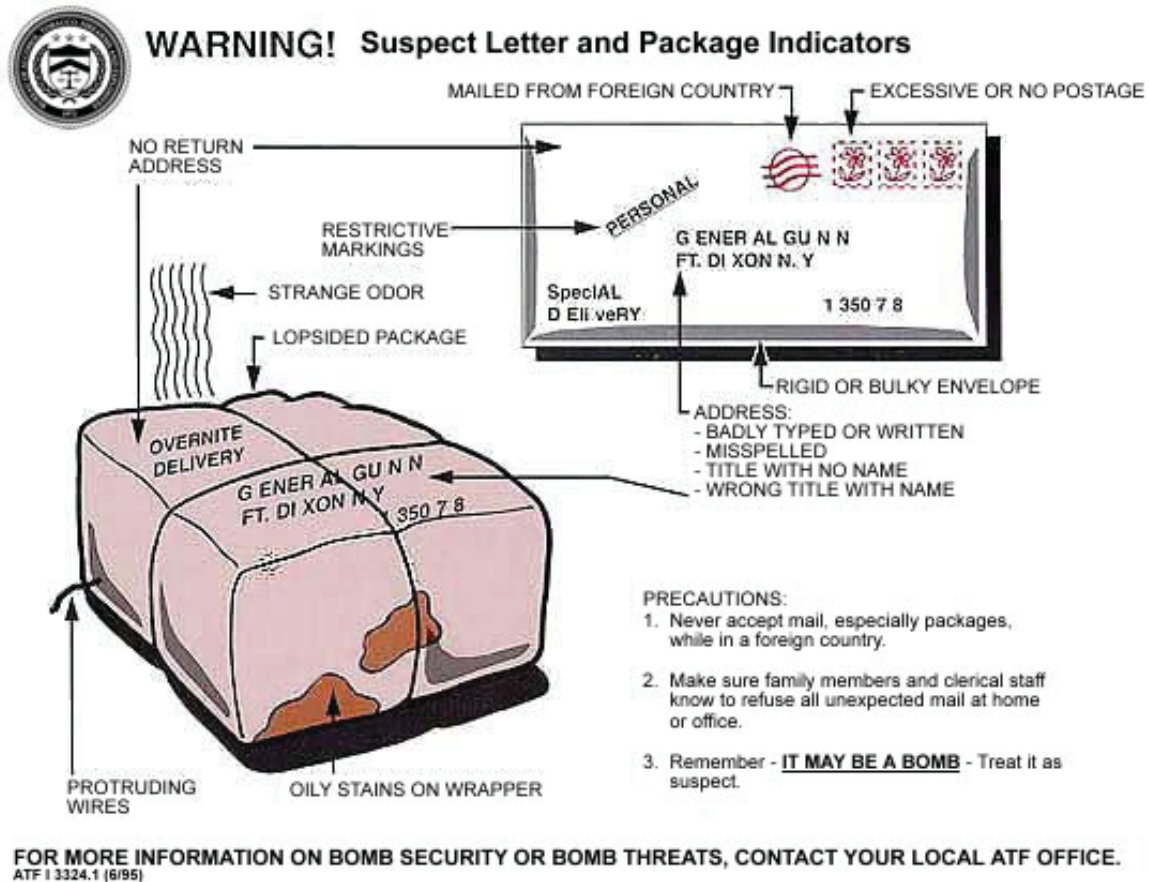


Image of suspect letter and package indicators courtesy of ATF

<http://www.atf.treas.gov/explarson/information/indic.htm>

## What Should You Do If You Receive an Anthrax Threat?

These threats require prompt action by health, law enforcement and laboratory personnel. Coordination and communication across agencies are necessary to protect the public and first responders from agents such as anthrax.

If you opened a letter that claims to have contaminated you with anthrax and there is no substance in the letter or envelope, no one including the person opening the letter, is at risk. No decontamination or treatment is necessary. Notify your supervisor and they will notify the appropriate officials.

If you opened a letter that claims to have contaminated you with anthrax and there is a substance in the letter or envelope the Centers for Disease Control and Prevention (CDC) in Atlanta recommends the following steps:

- Do not shake or empty the contents of any suspicious envelope or package
- Double bag the letter or package in zipper-type or zip-lock type plastic bags using latex gloves, or some other type of container to prevent leakage of contents. If you do not have any container, then COVER the envelope or package with anything (e.g., clothing, paper, trash can, etc.). DO NOT REMOVE THIS COVER.
- LEAVE the room and CLOSE the door, or section off the area to prevent others from entering
- Notify your immediate supervisor and both local police and the FBI, who will arrange to collect the letter/package and assess the threat situation
- WASH your hands with soap and water to prevent spreading any powder to your face
- Ensure that all persons who have touched the letter wash their hands with soap and water
- LIST all people who were in the room or area when this suspicious letter or package was recognized. Give this list to both the local public health authorities and law enforcement officials for follow-up investigations
- Place all items worn at the time in plastic bags and keep them available for law enforcement; If possible change clothing in the workplace and DO NOT let anyone else touch the clothing
- Shower with soap and water
- Notify Center for Disease Control (CDC) Emergency Response at 770-488-7100 for any questions or if you require further information. You can access their web site at:

[http://www.cdc.gov/ncidod/dbmd/diseaseinfo/anthrax\\_g.htm](http://www.cdc.gov/ncidod/dbmd/diseaseinfo/anthrax_g.htm)

## 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 route and only very rarely via the others.

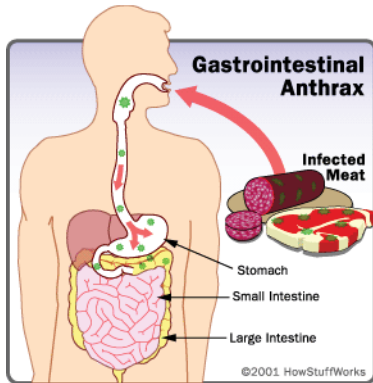
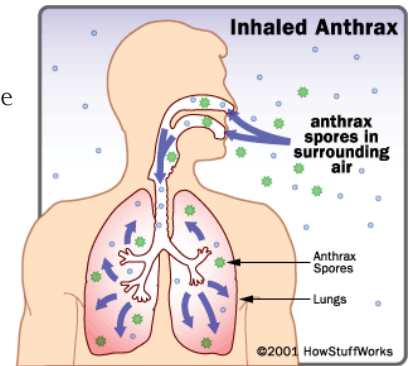


The cutaneous or skin form occurs most frequently on the hands and forearms of persons working with infected livestock or contaminated animal products and represents 95% of cases of human anthrax. It is initially characterized by a papule which progresses to a fluid filled blister with swelling at the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

The skin form of the human 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.

The spores are very stable and may remain viable for many years in soil and water. They will resist sunlight for varying periods.

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



The gastrointestinal form of form of anthrax may be contracted by eating insufficiently cooked, infected meat. This form has not been seen in the U.S. for decades.

Anthrax is not contagious; therefore, quarantine and general decontamination of an entire building or office are not necessary. Thorough cleaning is necessary for any area where the spores may have been released.

### 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

A mild illness can progress rapidly to respiratory distress and shock in 2-4 days. This is followed by a range of more severe symptoms including difficulty breathing, exhaustion, tachycardia, and cyanosis. Shock and death occur within 24-36 hours after onset of severe symptoms.

### What Is the Treatment for Anthrax?

Treatment with antibiotics beginning one day after exposure to a lethal aerosol challenge with anthrax spores (8,000 - 22,000 spores) has been shown to provide significant protection against death in monkeys, especially when combined with active immunization. Penicillin, doxycycline, and ciproflaxin are all effective against most strains of B anthracis. Penicillin is the drug of choice for naturally occurring anthrax.

If untreated, inhalation anthrax is fatal. For post-exposure prophylaxis, the administration of antibiotics should be continued for at least 4 weeks in those exposed and if available, those exposed should receive 3 doses of vaccine before antibiotics are discontinued.

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 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.

### How Is Anthrax Made Into a Weapon?

Biological agents can be prepared and used either in liquid or dry form. Procedures and equipment for preparing liquid biological agents are simple, but the resulting product is difficult to disseminate into small-particle effective aerosols. Conversely, procedures for producing dried biological agents, such as anthrax spores are complex and require more sophisticated equipment, yet this product is readily disseminated by any number of devices.

If an organization has the capability to produce viruses by means of tissue culture technology, then it could process a liquid agent into a dry powder. The dried agent might have the consistency of bath powder. An ideal dry agent should have free-flowing properties. If the powder were derived from a highly sophisticated process, however, it would contain very small particles and be highly charged with static electricity. A less sophisticated process yields a coarse-appearing powder comprised of large particles (10-20 microns) and is not particularly difficult to handle.

Unlike nuclear and chemical agents, biological agents are not detectable with the five human senses. You would never realize you may have been exposed to a biological agent until you started becoming sick with certain symptoms.

### **What Sources are Available to Help Me?**

There are a variety of resources available to help federal Mail Managers cope with these threats and develop better means of responding:

The Awareness of National Security Issues and Response (ANSIR) Program is the FBI's National Security Awareness Program. It is the "public voice" of the FBI for espionage, counterintelligence, counter terrorism, economic espionage, cyber and physical infrastructure protection and all national security issues. The program is designed to provide unclassified national security threat and warning information to U.S. corporate security directors and executives, law enforcement, and other government agencies. It also focuses on the "response" capability unique to the FBI's jurisdiction in both law enforcement and counterintelligence investigations.

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: <http://www.fbi.gov/contact/fo/fo.htm>.

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 website is <http://cdc.gov>.

The Federal Protective Service (FPS) is part of the Department of Homeland Security and is responsible for security in all federally leased space. The FPS Police number is 1-877-4FPS-411 (1-877-437-7411).

The U. S. Postal Inspection Service is the law enforcement branch of the U.S. Postal Service, empowered by federal laws and regulations to investigate and enforce federal statutes related to crimes against the U.S. Mail, the Postal Service, and its employees. The Postal Inspection Service extends full cooperation to all federal, state, and local authorities in law enforcement matters to ensure greater protection to the public. For assistance with postal-related problems, contact the nearest Inspection Service Division listed in your local telephone directory.

<http://www.usps.com/postalinspectors>

### **Post-Decontamination Considerations**

- Law enforcement personnel should interview all potential victims and document their names, addresses, and phone numbers
- Decisions to provide treatments for Biological Threat Agents should be made by public health authorities
- Consider mental health counseling for potentially exposed persons
- It is important that sample results be relayed to exposed persons once available to either initiate additional medical procedures if tests are positive or to eliminate fears and anxiety if tests are negative
- If explosive devices are ruled out and the evaluation for potential chemical, biological, or radioactive source material is negative, then response continues as a law enforcement investigation