



# Best Practices for Safe Mail Handling

Interagency Security Committee



Homeland  
Security



# Homeland Security

The Interagency Security Committee (ISC) is pleased to issue Best Practices for Safe Mail Handling. This document was developed by the ISC Safe Mail Handling sub-committee and identifies best mail room operations practices used by federal agencies. This unclassified document is provided to assist security managers in implementing safe mail handling practices at their facilities.

Best Practices for Safe Mail Handling is available via the ISC secure portal. It is located in the library under ISC Published Documents. The document also is available publicly at <http://www.oca.gsa.gov>. Questions or comments should be directed to [TheISC@DHS.gov](mailto:TheISC@DHS.gov).

Dwight M. Williams  
Chair, Interagency Security Committee  
Chief Security Officer, Department of 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 of pieces of mail each year without incident; nevertheless, federal agencies must prepare for the worst case scenario. Threats can never be eliminated. For that reason, agencies should use risk to determine security measures.

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 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 Center for Disease Control (CDC), General Services Administration (GSA), and Postal Service websites, other 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.

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. Accordingly, 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 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 the agency's mission or the mission of other tenant agencies that may make the 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 at which screening of incoming mail for suspect items should occur. Individuals who normally sort the mail should perform the screening function. These individuals are most likely to notice packages that are out of the ordinary.

The basic screening procedures for 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.



# 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
- Have security personnel greet all employees and visitors and examine their 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
- Ensure that accountability for lock and key control is 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
- Establish procedures for isolating a 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
  - Smocks
  - Protective glasses
- Know the phone 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

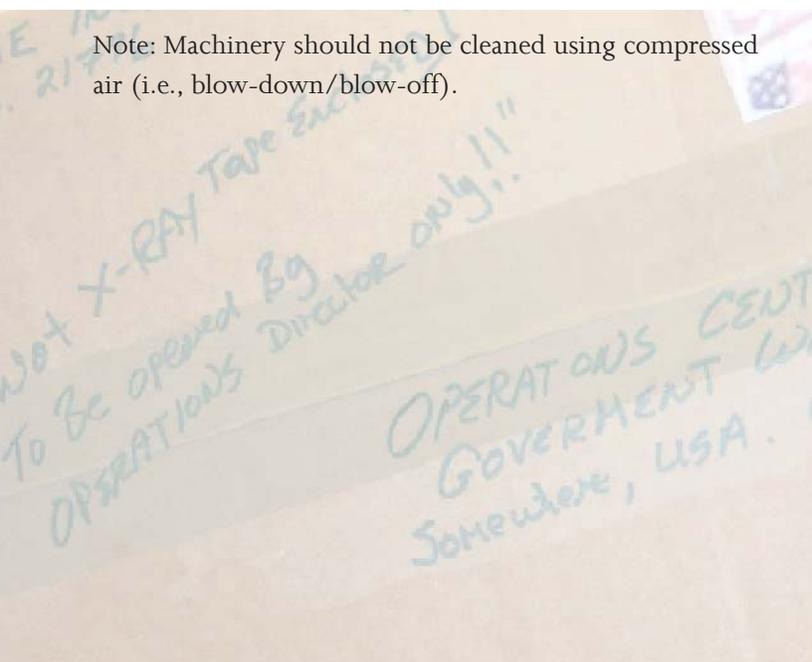
- Bomb detection / K-9
- X-ray for incoming mail
- Detection devices
  - Biological
  - Chemical
  - Radiological
- Hold mail 24 hours or until testing concluded
- Containment receptacles for mail storage
- Down draft tables
- Separate air filtration unit
- Monitored mail operations
- Safe air room for mail processing
- Monthly swab testing of mail room
- Showers or decontamination system
- 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; nevertheless, 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 its Continuity of Operation Plan (COOP) to enable mail processes to continue. 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	✓	✓

## GENERAL 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 them.

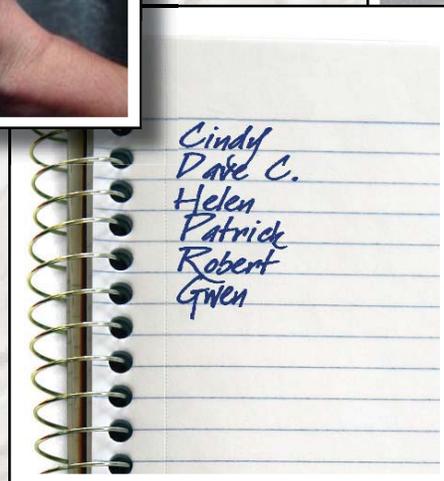
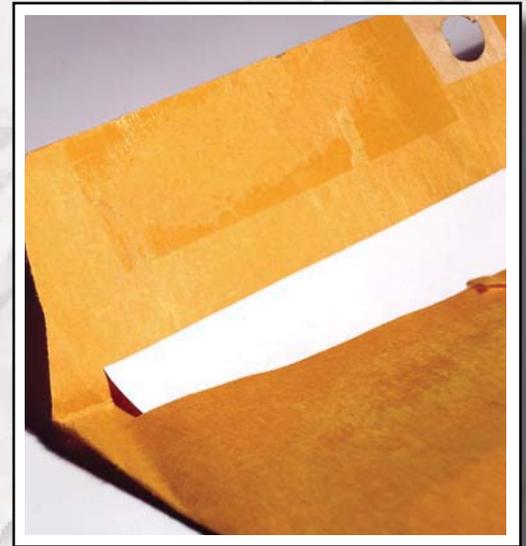
## Plan Review

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 the fire department
- Call your postal inspector



## Quick Reference

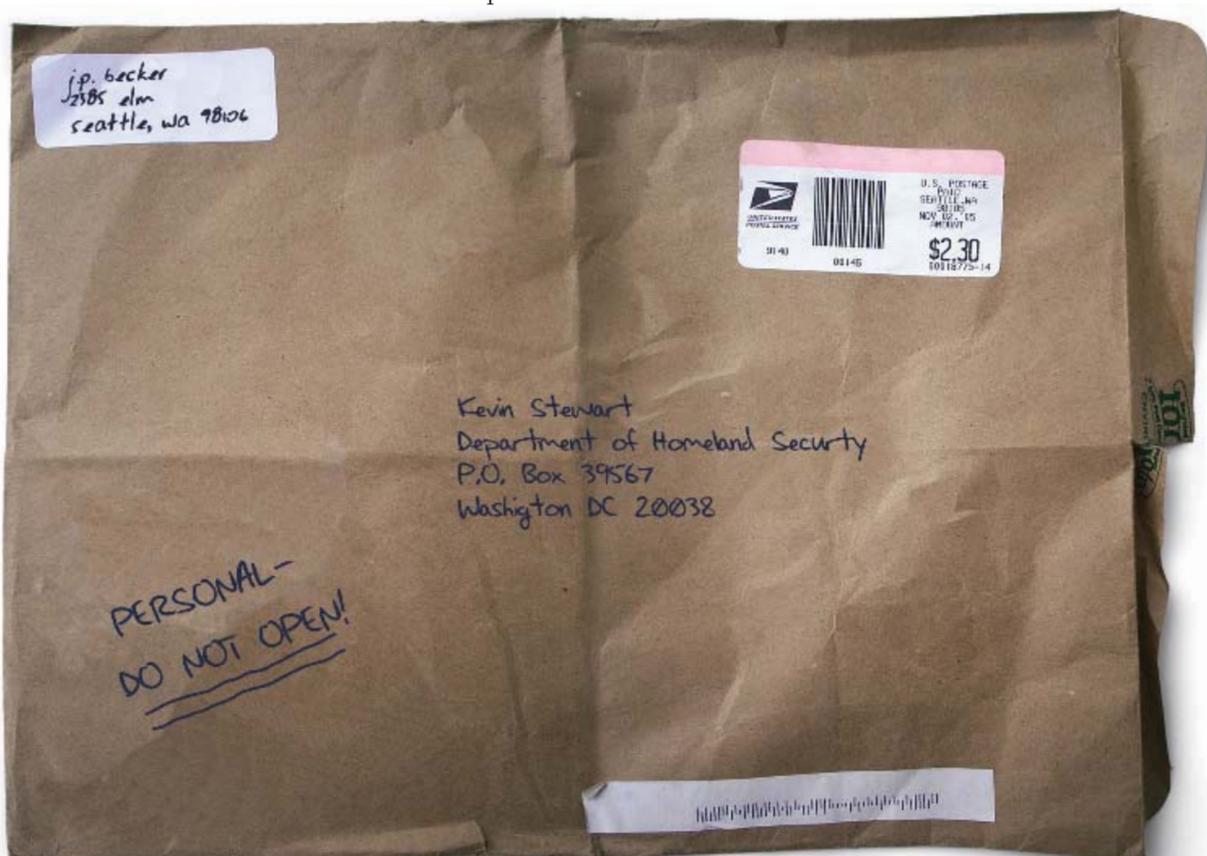
For a Bomb	For Radiological Threats	For Biological or Chemical Threats
<ul style="list-style-type: none"><li>• Evacuate immediately</li><li>• Call Police</li><li>• Contact postal inspectors</li><li>• Call local Fire Department-HAZMAT Unit</li></ul>	<ul style="list-style-type: none"><li>• Limit exposure - don't handle</li><li>• Distance (evacuate area)</li><li>• Shield yourself from object</li><li>• Call Police</li><li>• Call local Fire Department-HAZMAT Unit</li><li>• Contact postal inspectors</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>• Call local Fire Department-HAZMAT Unit</li><li>• Contact postal inspectors</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). The Federal Protective Service (FPS) is part of the Department of Homeland Security and is responsible for security for many federal buildings and locations. If you need FPS assistance, call 1-877-4FPS-411.

## 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>

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

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

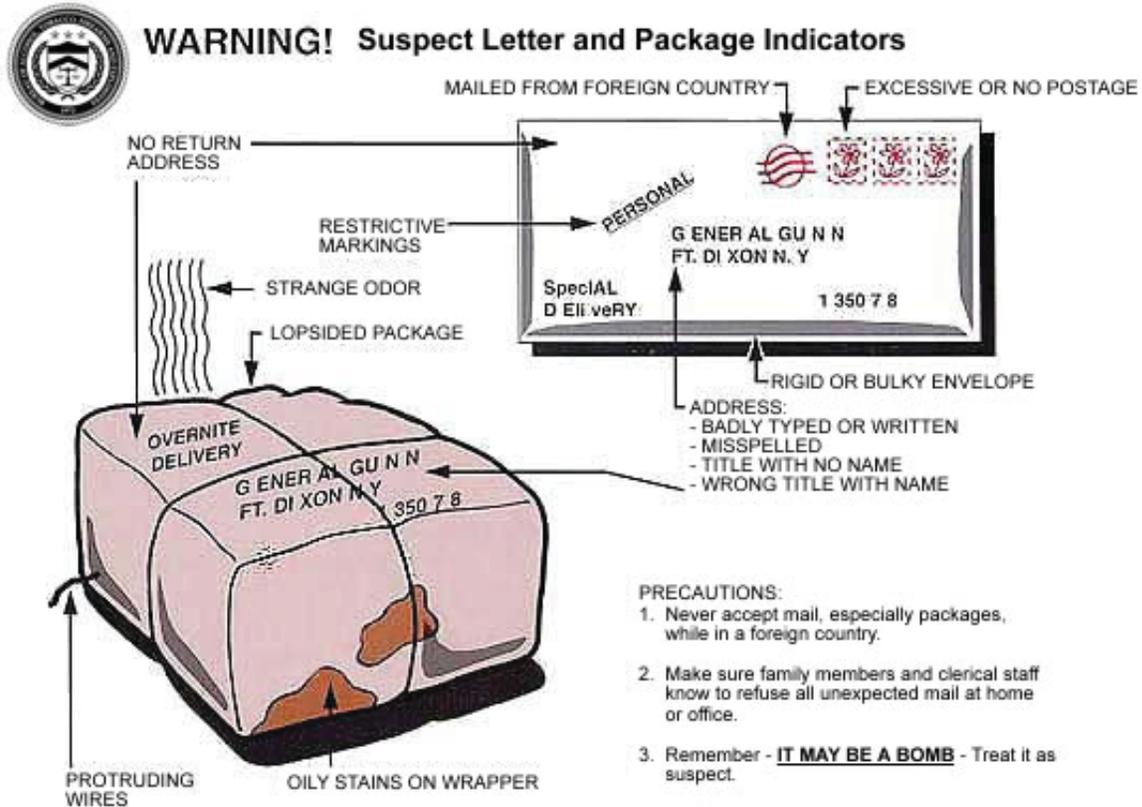
<http://www.usps.com>

# APPENDIX B

## appendix b

### Training Reference

Source: [http://www.usps.com/news/2001/press/pr01\\_10229sa\\_print.htm](http://www.usps.com/news/2001/press/pr01_10229sa_print.htm)



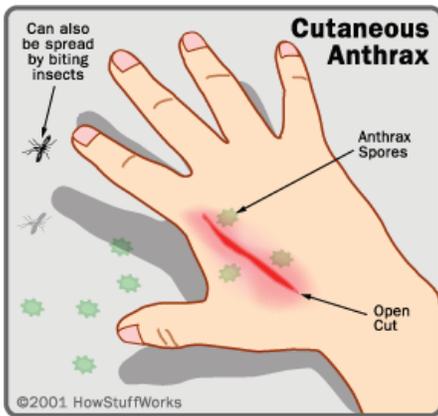
FOR MORE INFORMATION ON BOMB SECURITY OR BOMB THREATS, CONTACT YOUR LOCAL ATF OFFICE.  
ATF I 3324.1 (6/95)

Image of suspect letter and package indicators courtesy of ATF

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

## What Are the Types of Anthrax Infections?

Anthrax infection can occur in three forms: cutaneous (skin), inhalation, and gastrointestinal.

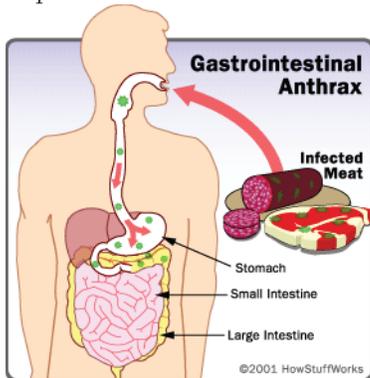


### Cutaneous anthrax:

Most (about 95%) anthrax infections occur when the bacterium enters a cut or abrasion on the skin, such as when handling contaminated wool, hides, leather or hair products (especially goat hair) of infected animals. Skin infection begins as a raised itchy bump that resembles an insect bite but within 1-2 days develops into a vesicle and then a painless ulcer, usually 1-3 cm in diameter, with a characteristic black necrotic (dying) area in the center. The scabs that typically forms over the lesion can be black as coal, hence the name anthrax, which is Greek for coal. Lymph glands in the adjacent area may swell. About 20% of untreated cases of cutaneous anthrax will result in death. Deaths are rare with appropriate antimicrobial therapy.

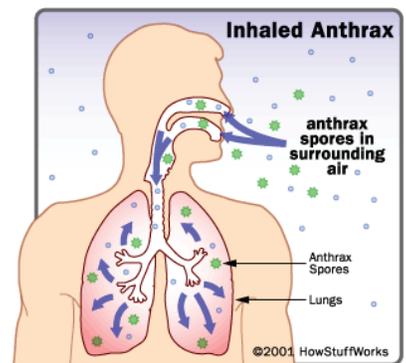
### Inhalation anthrax:

Initial symptoms may resemble a common cold – sore throat, mild fever, muscle aches and malaise. After several days, the symptoms may progress to severe breathing problems and shock. Inhalation anthrax is usually fatal.



### Gastrointestinal anthrax:

The intestinal disease form of anthrax may follow the consumption of contaminated meat and is characterized by an acute inflammation of the intestinal tract. Initial signs of nausea, loss of appetite, vomiting, fever are followed by abdominal pain, vomiting of blood, and severe diarrhea. Intestinal anthrax results in death in 25% to 60% of cases.



## Treatment for patients with inhalation and cutaneous anthrax

The CDC made treatment recommendations for cases of inhalation and cutaneous anthrax associated with the bioterrorism attack of 2001. These recommendations can be found at <http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5042a1.htm>.

### Different strains of anthrax and response to antibiotics

Yes, there are different strains of anthrax. Some strains may be naturally resistant to certain antibiotics and not others. In addition, there may be biologically mutant strains that are engineered to be resistant to various antibiotics. A laboratory analysis can help to define which strain of anthrax is present and which antibiotic would be the most effective in treating it.

## How Is Anthrax Made Into a Weapon?

Anthrax is an acute infectious disease caused by the spore-forming bacterium *Bacillus anthracis*. Anthrax most commonly occurs in wild and domestic lower vertebrates (cattle, sheep, goats, camels, antelopes, and other herbivores), but it can also occur in humans when they are exposed to infected animals or to tissue from infected animals or when anthrax spores are used as a bioterrorist 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.

### **Risks to employees in a positive anthrax environmental sample**

Risk would depend on where the environmental sample was, the amount of material, and if it was collected in an air sample or on a surface. The risk also would depend on the person's contact with the type of sample in terms of breathing or touching the sample.

### **Safety Issues/Mail cross-contaminated with anthrax**

The CDC does not have specific studies to address this, however, cross-contamination of the mail could occur during the processing, sorting, and delivery of mail when an envelope comes in contact with an envelope, piece of equipment (e.g., an electronic sorting machine), or other surface that is contaminated with anthrax spores. In addition, airborne spores in contaminated postal facilities before they were cleaned might play a role.

### **Safety Guidelines**

The recommendations are divided into four categories. They are engineering controls, administrative controls, housekeeping controls, and personal protective equipment for workers. The guidelines describe measures that should be implemented in mail-handling/processing sites to prevent potential exposures to anthrax spores.

- [www.bt.cdc.gov/documentsapp/anthrax/10312001/han51.asp](http://www.bt.cdc.gov/documentsapp/anthrax/10312001/han51.asp)
- [www.cdc.gov/mmwr/preview/mmwrhtml/mm5043a6.htm](http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5043a6.htm)
- Every facility is different and should be evaluated. The recommendations implemented should be selected on the basis of the evaluation of the work site. This evaluation should focus on determining which processes, operations, jobs, or tasks would be most likely to result in an exposure should a contaminated envelope or package enter the work site.

### **Controls mail-handling/processing operations should consider implementing for detecting anthrax spores**

#### **Engineering controls**

Anthrax spores can be aerosolized during the operation and maintenance of high-speed, mail-sorting machines, potentially exposing workers and possibly entering heating, ventilation, or air-conditioning (HVAC) systems. Engineering controls can provide the best means of preventing worker exposure to potential aerosolized particles, thereby reducing the risk for inhalation anthrax, the most severe form of the disease.

#### **Administrative controls**

Strategies should be developed to 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, restrictions should be in place to limit the number of people including support staff and non-employees entering areas where aerosolized particles may be generated. This recommendation applies to contractors, business visitors, and support staff.

#### **Housekeeping controls**

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

## **Protecting workers from exposure to anthrax spores**

Personal protective equipment for workers in mail-handling/processing sites must be selected on the basis of the potential for exposure to anthrax spores. Handling packages or envelopes may result in skin exposure. 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 sites where airborne particles may be generated such as where mailbags are unloaded or emptied may also be exposed through inhalation.

### **Examples of personal protective equipment and clothing that could be used to protect workers**

- 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. Skin rashes and other dermatological conditions are a potential hazard of wearing gloves. Latex gloves should be avoided because of the risk of developing skin sensitivity or allergy.
- Gloves should be provided in a range of sizes to ensure proper fit.
- The choice of glove material should be based on safety, fit, durability, and comfort. Sterile gloves such as surgical gloves are not necessary.
- 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 for operations in which gloves can easily be torn or if more protection against hand injury is needed.
- For workers involved in situations where 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, 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 (see "Guidelines for Hand Hygiene and Environmental Infection Control," 2002 and 2003, available at <http://www.cdc.gov/handhygiene>).
- 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.

### **Some postal settings present a greater risk than others for anthrax exposure**

- People working with or near machinery capable of generating aerosolized particles, such as electronic mail sorters, 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 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.