S.M.S.
STATE MAIL SERVICES

1910 Darbytown Road
Richmond, Virginia 23231
Phone: (804) 236-3592
Fax: (804) 236-3595
StateMail@dgs.virginia.gov

http://sms.dgs.virginia.gov

Commonwealth of Virginia Mail Security Guide

A Resource for Keeping the Commonwealth Secure

February 2007

Table of Contents

Prefix

Introduction

Mail acts as a portal into state agencies and offices. Recent terrorist events have demonstrated a critical need for educating state employees on mail security. Every state agency is responsible for ensuring the safety of their employees and should provide guidance regarding potential threats in the mail stream. It is for this reason that each Commonwealth of Virginia mail center must have a functional security plan and offer their employees proper training.

State Mail Services (SMS), the postal service provided by the Department of General Services, recognizes the importance of safety in mail processing. SMS has created this Guide as a uniform resource to assist state employees in keeping the mail stream safe and secure. This Guide was designed to help state employees become more familiar with the proper processes for handling mail and to provide an outline of security planning and preparation for Commonwealth mail centers. The Guide offers general advice and recommends protective measures to help you assess, prevent, and respond to threats in the mail stream.

Should you have any questions regarding mail security, we urge you to contact State Mail Services at (804) 236-3592 or StateMail@dgs.virginia.gov.

Contributing Resources

Portions of the Commonwealth Mail Security Guide are excerpts from the United States Postal Service Guidelines and the US General Services Administration Mail Center Security Guides. See Appendix B for a complete list of resources.

Chapter
1

General Information about Mail Security

Suspicious Letters & Packages

One key element in the protection of the mail stream is the ability of employees to identify suspicious letters and packages. As such, SMS has screening procedures and equipment in place to examine all mail that they handle. See Appendix C for a suspicious mail poster.

What Constitutes a Suspicious Letter or Package?

Some typical characteristics of letters and parcels that may be considered suspicious are:

- Unexpected or from someone unfamiliar to you.
- Have excessive postage.
- A fictitious or no return address.
- Marked with restrictive endorsements, such as “Personal” or “To Be Opened by Addressee Only”.
- Poorly typed or handwritten addresses or misspellings of common words.
- Shows a city or state postmark that does not match the return address.
- Of unusual weight, given their size, or are lopsided or oddly shaped.
- Have excessive tape on them.
- Have a strange odor or chemical smell.
- Powdery substance on or leaking from the package.
- Leaking any type of fluid.
- Protruding wires, screws, or other meal parts.
- Making a sandy noise or any other noise when moved.
- Any item you consider out of the ordinary for your work area.

What to do if You Receive Mail that Appears Suspicious?

- Do not shake or open the contents of any suspicious package or envelope.
- Do not carry the package or envelope, show it to others, or allow others to examine it.
- Do put the package or envelope down on a stable surface; do not sniff, touch, taste, or look closely at it or at any contents which may have spilled.
- Do not attempt to clean up any spilled contents.
- Do alert others in the area about the suspicious package or envelope. Leave the area, close any doors, and take actions to prevent others from entering the area. If possible, shut off the ventilation system.
- Do ensure that all persons who have touched the package or envelope wash their hands, face, and arms with soap and water immediately.
- Do notify your supervisor and call the appropriate emergency responders (use Appendix D as a guide).
- Do make a list of all persons who have touched the package. Provide this information to the emergency responders upon their arrival.
- After the incident is resolved the agency mail supervisor should report it to SMS.

Suspicious letters and packages may consist of a variety of contents. Please review the following sections addressing anthrax and mail bombs.

Biologically Hazardous Materials

Anthrax is a bacterial, zoonotic disease caused by *Bacillus (B.) anthracis*. In humans three types of anthrax infections can occur based on the route of exposure. X-ray equipment is not capable of detecting biochemical agents; therefore, it is important that all unexplainable powdery substances in the mail be considered suspect and the proper procedures for suspicious items should be followed.

Types of Anthrax Infections

Exposure	Transmittal and Characteristics	Symptoms
Skin *Anthrax Type:* Cutaneous	Cutaneous anthrax is the most common naturally occurring type of infection. Cutaneous anthrax usually occurs after skin contact with contaminated meat, wool, hides, or leather from infected animals. The incubation period ranges from 1 to 12 days. Infection is introduced through scratches or abrasions of the skin.	Skin infection begins as a raised bump that resembles a spider bite. Within 1 to 2 days, the infection develops into a blister and then a painless ulcer, with a characteristic black necrotic (dying) area in the center. The lesion is usually painless, but patients also may have fever, malaise, and headache. Lymph glands in the adjacent area may swell.

Exposure	Transmittal and Characteristics	Symptoms
Inhalation *Anthrax Type:* Inhalation	Anthrax spores must be aerosolized to cause inhalational anthrax. Inhalation anthrax is contracted by inhalation of the spores. It occurs mainly among workers handling infected animal hides, wool, and fur. The number of spores that cause human infection is unknown. The incubation period of inhalational anthrax among humans is unclear, but it is reported to range from 1 to 7 days, possibly ranging up to 60 days.	Inhalation anthrax resembles a viral respiratory illness. Initial symptoms include sore throat, mild fever, muscle aches, and malaise. Symptoms may progress to respiratory failure and shock with meningitis. After an incubation period of 1 to 7 days, the onset of inhalation anthrax is gradual.
Ingestion *Anthrax Type:* Gastrointestinal	Gastrointestinal anthrax usually follows the consumption of raw or undercooked contaminated meat and has an incubation period of 1 to 7 days.	Gastrointestinal anthrax is characterized by acute inflammation of the intestinal tract. Initial signs are nausea, loss of appetite, vomiting, fever followed by abdominal pain, vomiting of blood, and severe diarrhea.

Prevention

Ways to limit physical exposure to mailings containing biologically hazardous material:

- Screen all mail.
- Know how to recognize suspicious mail.
- Follow the procedures for suspicious items.
- Do not open mail in an area where other personnel are present.
- Keep mail away from your face when opening.
- Wear appropriate protective gloves and masks if available.
- Use universal blood borne pathogen precautions as developed by your agency.

Administrative Controls

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 and emptied. In addition, restrict the number of people including support staff and non-employees from entering areas where aerosolized particles may be generated. This recommendation applies to contractors, visitors, and support staff.

Protective Equipment

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

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

Gloves should be provided in a range of sizes to ensure proper fit. The choice of glove material such as nitrile or vinyl should be based on safety, fit, durability, and comfort. Different types of gloves or additional layers of gloves may be needed depending on the task, the dexterity required, and the type of protection needed. Protective gloves can be worn under heavier gloves such as leather, heavy cotton for operations where gloves can easily be torn or if more protection is required to prevent hand injury.

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

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

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

Engineering Controls

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

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

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

Mail Bombs

People often think of a mail bomber as a person motivated by radical political beliefs. This stereotype is incorrect. If you adhere to this stereotype, you may improperly assess and respond to a bomb threat.

Revenge is the motivation that most often triggers a mail bomb or a bomb threat. Jilted spouses or lovers may seek revenge at the end of their romantic involvement. Former employees may seek revenge when a business relationship goes sour or there are layoffs. Law enforcement officers and members of the judiciary have been targeted for bombs and bomb threats by individuals seeking revenge for having been investigated or prosecuted. Mail bombs usually target specific individuals.

The chances of your workplace receiving a mail bomb are extremely remote. The vulnerability for you and your workplace depends on a variety of factors - both internal and external. No individual or agency is completely immune from such an attack.

Prevention

The best method to detect explosive devices in mail is for all mail to be X-rayed. State Mail Services screen all mail that is processed at their mail center. SMS personnel receive mandatory and periodic training on all X-ray and mail security equipment.

Bombs can be constructed to resemble almost anything and can be delivered in any number of ways. The probability of finding a stereotypical explosive device is almost nonexistent. The only common denominator that exists among bombs is that they are designed or intended to explode. Most bombs are homemade and are limited in their design only by the imagination of, and resources available to, the bomber.

In addition to the standard characteristics of suspicious mail, check for these irregularities which are often present in mail or package bombs:

- Letters or packages that are unusual in weight, lopsided, oddly shaped, or oddly sealed. Can you hear a sloshing sound? Does it feel unusually rigid, springy, or under pressure? Examine mail gently.
- Correspondence from an unexpected sender. Do the characteristics of the envelope or package resemble the expected contents? Does the addressee normally not receive personal mail at the office?
- A strange odor (i.e., smell of almonds or marzipan or any other strange smell) coming from the package or letter.
- Protruding wires, strings, tape, etc.
- Wrapping exhibiting previous use, such as having traces of glue, mailing labels, return addresses, or tape. Is it secured with several types of tape?
- An unusual sound or noise coming from the package (i.e., buzzing, ticking). Any such package should be treated with caution.
- The item was not delivered by a known carrier. Most bombers set up and deliver the bomb themselves.
- Being wrapped in string. These items are automatically suspicious, as modern packaging materials have eliminated the need for twine or string.
- A letter or package arriving before or after a phone call from an unknown person asking if the item was received.

What to do if You are Suspicious of a Mail Bomb?

If you suspect a package contains a mail bomb and are unable to verify the contents, remember to take the necessary safety precautions.

If a suspicious delivery is spotted and has not been touched:

- Do not touch it.
- Do not allow anyone else to touch it.
- Activate the building’s evacuation plan.
- Leave doors and windows open during evacuation.
- Keep people away from the area.
- Notify your supervisor and call the appropriate emergency responders (use Appendix D as a guide).
- Do not handle the suspicious object, and do not try to carry it outside.
- Do not place the item in water.
- After the incident is resolved the agency mail supervisor should report it to SMS.

If an item is suspected during handling:

- Handle it very gently and while making sure not to turn it over or unbalance it, place the item in a corner of the room.
- Make sure the device is placed away from windows.
- Make sure the windows are open.
- Activate the building's evacuation plan.
- Leave doors and windows open during evacuation.
- Keep people away from the area.
- Notify your supervisor and call the appropriate emergency responders (use Appendix D as a guide).
- Do not try to carry the device outside.
- Be available for emergency responders to talk to you about the incident.
- After the incident is resolved the agency mail supervisor should report it to SMS.

Chapter

2

Mail Center Security

The purpose of this chapter is to assist Commonwealth mail managers in continuing to keep mail centers both safe and secure.

Mail Center Security Plan

Each agency mail center should have an active security plan. A mail center security plan has several objectives that should include:

- Protecting staff and building occupants.
- Avoiding unwarranted, costly, and disrupting evacuations.
- Providing a visible mail screening operation that demonstrates to all employees that management is committed to their safety.
- Supporting employee morale and reducing stress by providing reassurance to all employees regarding the safety of mail.
- Minimizing the likelihood of litigation. (This could arise from suggestions that the mail center manager had not taken proper measures to keep employees safe while at work).

A strong plan for mail center security, supplemented with regular training exercises, rehearsals, and reviews, helps instill a culture that emphasizes the importance of security.

Smaller Mail Facilities

Many agencies have facilities where mail operations are performed in a small room, in a corner of a room, or one corner of a desk. In 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 their plans. Small facilities should adopt recommendations that are appropriate to them. Chapter One of this Guide offers direction for individual employees. Your threats and vulnerabilities will determine the measures to protect your facility.

Risk Assessment

The first step in developing a security program is a site-specific risk assessment of your mail center and its operations, in coordination with your agency and bureau/department. The objective of a risk assessment is to determine the likelihood that identifiable threats may hinder an agency or its mission. Each site has different threats and risk levels, and this will lead to different security measures for each site. A thorough understanding of the risk assessment process will allow for better preparation to meet potential threats and eliminate or mitigate consequences. A risk assessment incorporates the entire process of asset and mission identification, threat assessment, vulnerability assessment, impact assessment, and risk analysis.

Conducting a Risk Assessment

As mail center manager, you should be an active participant in the risk assessment process along with appropriately trained and experienced security personnel. Offices located at Capitol Square in Richmond should contact Virginia Capitol Police to aid with risk assessments.

Step One: Asset and mission identification – What are you trying to protect?

The first step in a risk assessment is identifying the assets and missions that must be protected. During the asset identification step you should identify and focus only on those assets important to the mission or operation. By identifying and prioritizing these assets, you will be taking the first step towards focusing resources on what is most important. Assets can be tangible (e.g., people, facilities, equipment) or intangible (e.g., information, processes, and reputations). Obvious mail center assets include personnel, postage meters and other related equipment, computers, accountable mail, high-value shipments, the safe or vault and its contents, stamps, pre-printed permit stationery, and the mail delivery roster.

Since the mail center is a vulnerable point of entry for threats, your risk assessment must also identify the assets and missions of your customers; that is, the people to whom you deliver mail. A deliberate attack may not be directed at your mail center. It may be directed at your customers and their missions. The next step is to identify the threats that may adversely impact the assets or mission you identified.

Step Two: Threat Assessment – What bad things could happen?

The next step in the risk assessment is determination of potential threats. The threat assessment looks at the full spectrum of threats – natural, criminal, accidental, or terrorist – for a given location. The assessment should examine supporting information to evaluate the likelihood of occurrence for each threat.

For natural threats, you should research historical data that shows the frequency of occurrence for tornadoes, hurricanes, floods, fires, and earthquakes in your area.

For criminal threats, look at local crime rates and consider whether your customers' assets and missions make you or them more attractive to criminals.

For accidents, look at the layout of and machinery in your mail center, also consider your building's mechanical equipment, especially plumbing. Look at your historical accident rate (you should be keeping accessible, long-term records of accidents).

For terrorist threats, look at the missions performed by your customers and the visibility of executives located in the facilities that you serve.

For each of these identify the specific threats that might impact your mail center or facility. Then determine how they might affect the mail center and then estimate how likely each threat is to occur. When making these estimates rely exclusively on data and information obtained from research and interviews, not on intuition.

Significant threats to a government mail center include:

- Foreign terrorism - Agencies with high public visibility or international missions have a greater risk of being targeted by foreign terrorists. Also, agencies located in proximity to significant targets may be victims of collateral effects.
- Domestic hate groups - Some citizens are actively involved with anti-government hate groups and have adopted tactics similar to foreign terrorists.
- Disgruntled employees/workplace violence - Reorganizations, layoffs, and terminations may lead to theft, sabotage, or violence. Additional steps should be taken to protect individual employees who are being harassed, stalked, or threatened inside or outside the workplace.
- Accidents – such as workplace accidents, vehicle accidents, floods from major plumbing leaks, and building fires.
- Acts of nature - such as wildfires, floods, severe weather, or earthquakes.

One very important part of this step is simply looking at your mail stream. Certain agencies and organizations receive threatening mail almost daily; while others have seldom, if ever seen a threatening mail piece of mail.

A threat may be introduced by anyone who sends anything through the mail with the intent to frighten, disrupt, injure, etc. It could be the animal rights activist or the environmental radical, the pro-rights or pro-life extremist, the disgruntled employee, the angry spouse, or simply a disappointed citizen. It could be anyone. Remember that you do not have to be a target in order to become a victim.

A key question that must be answered in a threat assessment is: How visible is your agency, your facility, or an executive who works in your facility, and to what extent does his/her visibility make it more or less likely that a criminal or terrorist might select your facility for an attack? Some Commonwealth agencies are, of course, highly visible, but many agencies and facilities are relatively unknown to the general public and are, therefore, much less at risk.

Step Three: Vulnerability Assessment – What are your weaknesses?

You have identified your assets, missions, and threats, the next step is to determine how vulnerable your assets and missions are to the threats. In this step look for exploitable situations created by inappropriate facility design, inadequate equipment, or deficient security procedures. In the mail center, examples of typical vulnerabilities (which you might also call points of weakness) may include:

- Poor access controls
- Lack of x-ray equipment
- Inadequate security training or rehearsal
- Lack of stringent service contract management
- Unscreened visitors in secure areas

This step requires looking at each asset from the outside inward just as a potential adversary might look at your location or operation. Specifically, begin by studying each asset and asking questions such as: "If I wanted to physically harm this facility, I would….?" Or "If I wanted to attack a specific person?" or "If a major hurricane struck?" And so on down the list of potential threats and undesirable events. The significance of each vulnerability depends on how easily an adversary could exploit it, or an accident or natural disaster could compromise it.

Step Four: Impact Assessment – What would happen if your security measures failed?

Once you have identified each significant asset and mission, next determine what the impact or consequence would be if that asset were lost, damaged, or destroyed, or if your agency were temporarily prevented from performing that mission, or if its ability to perform it were significantly impaired. The overall value of the asset or mission is based upon the severity of this effect.

For example, if there was a failure or breakdown in your building's plumbing system and your mail center was flooded, preventing you access for several days, what would be the impact on your agency's mission?

Another example: If an improvised explosive passed through the mail center without being identified, reached its intended target in your facility, and detonated, what would the consequences be on the facility and the people who work there – the intended victim and everyone else?

Part of the impact assessment will be a determination of the impact on the mail center, the facility, and/or the agency if a specific asset were damaged or destroyed, or if a specific mission were impaired or temporarily halted.

Step Five: Risk Analysis – What does it all add up to?

The final step in the risk assessment process is to combine the four previous steps to evaluate, for each asset and each mission, how the impact, threat, and vulnerability assessments interact. The final product is a statement defining the risk level for each asset and mission.

Security in Mail Center Operations

Guidelines for the operations of Commonwealth mail centers.

Incoming Mail Procedures

All Commonwealth mail centers should have procedures regarding staff processing incoming mail. Items that should be a part of incoming mail procedures include:

- Limit access for anyone who delivers mail to your center; deal with them at a counter.
- Make personal protection equipment available for all employees, including gloves and masks.
- Require employees, vendors/contractors, and guests to wear photo identification at all times.
- Instruct employees to challenge any unknown person in the facility.
- If possible, acquire an X-ray machine to scan mail. If mail volume is too low to justify acquiring an X-ray machine, talk with State Mail Services about partnering with another agency to X-ray. All mail, regardless of carrier, should be X-rayed – be sure to include couriers and small package carriers.
- Once the mail has been X-rayed, inspect the mail for suspicious characteristics. If possible, do this in an area isolated from the rest of the mail center.
- Give extra care and attention to letters and packages addressed to any senior official whose names and/or positions give them higher public visibility.
- Establish procedures for handling unexplained or suspicious packages. See Chapter One for guidelines and Appendix D for a template to notify appropriate emergency responders.

Before calling emergency responders, mail center personal may attempt to find if the addressee of the suspicious package has any knowledge of the contents. 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 a package from the sender? If so, what is the approximate size of the item?
- Ask the sender to fully explain the circumstances surrounding the sending of the parcel and to describe the contents. At this point, management and security must make a decision whether to proceed to open the parcel or not.
- If the sender is unknown, is the addressee expecting any business correspondence from the city, state, or country of origin of the package?
- Is the addressee aware of any friends, relatives, or business acquaintances currently on vacation or on business trips in the area of origin?
- Has the addressee purchased or ordered any merchandise from any business concern whose parent organization might be located in area of origin?

If the verification process determines that the sender is unknown at the return address or that the return address is fictitious, consider this scenario as an indication that the parcel may be dangerous.

Offsite processing is an option an agency should consider if their security assessment identifies a high level of risk. Agencies interested in offsite processing of incoming mail should contact State Mail Services.

Loss Prevention

Security is vital to mail center operations. Lack of security can result in theft of supplies, postage, mail, and valuable information contained in sensitive mail. The following are some suggestions for improving theft prevention in your mail center operation:

- Screen job applicants before hiring them – do credit and criminal checks, and try to talk with references and former employers.
- Be aware of what may prompt an employee to steal.
- Integrate accounting procedures for all forms of postage – meters, stamps and permits.
- Establish procedures to control access for employees, known visitors, and escorted visitors.
- Require visitors to sign a log, and if possible, install access control equipment. (Key control, card readers, or buzz entry are a few options)
- Permit only authorized employees to accept mail.
- Conduct regular checks of your postage meters to ensure employees are not using agency meters for personal mail. Maintain meter logs carefully, and lock meters when not in use. Where feasible, remove the meter from the equipment and store it in a locked cabinet during off-hours.
- Carefully package shipments of valuable materials; send them via certified mail, and make sure their outside labeling does not identify the contents.
- Implement inventory controls to ensure proper access and accountability for stamps, permit envelopes, and labels. Perform regular audits of the inventory.
- No personal mail should be sent using the meter or permit imprints. If the agency allows staff to drop personal mail at the mail center, separate it from official outgoing mail, and insist that staff provide their own stamps for personal mail.
- Review bills from carriers regularly to guard against unauthorized use.
- Check periodically to determine if mail messengers are making unauthorized stops or leaving the mail unattended in unlocked delivery vehicles.
- Report all criminal activity to the appropriate law enforcement agency.

Physical Security in a Mail Center

The location and design of a mail center is one of the most important components of a security program. Suggestions for physical security:

- If possible, make the mail center an enclosed room with defined points of entry. If you cannot put the mail center in its own room, then set aside a defined space that is used only for processing mail. Do not have employee lockers within the mail center. If possible, locate the mail center near the loading dock. This will allow the mail to travel directly to the mail center from outside and minimize the impact that any potentially contaminated mail will have on the rest of the building.
- Within the mail center, establish a separate space for processing incoming mail. For a small mail center, this might be no more than a defined part of a table or desk. In a large mail center, this could be a separate room. Be sure to check the ventilation system of the area you choose to ensure adequate airflow.
- In locations where the risk assessment, the volume of mail, and cost-benefit analysis make it appropriate, the mail center should have its own air handling and ventilation system. You may also consider establishing negative air pressure for the area where you process incoming mail or for the entire mail center. Down-draft tables with HEPA filters are a good way to limit employee exposure to routine dust as well as possible airborne hazards. You may also want to consider an isolated room with its own ventilation system and HEPA filters.
- If you regularly see suspicious letters or packages in your mail stream, you may want to obtain a glove box or biochemical hood in which to open them (a biochemical hood operates with negative air pressure). In any event, you should establish a relationship with a first responder organization that has a glove box or hood, so that they can open suspicious mail.
- Install security alarms at each access point and monitor them for after-hours activity.
- Create secure areas such as safes or locked cabinets that can be used to store meters, express shipments, and valuables. Reset combinations and re-key locks after significant employee transitions.
- Provide a separate and secure area for personal items (e.g., coats and purses). Consider prohibiting employees from taking personal items into the workplace.
- Where appropriate, use surveillance cameras to monitor the service counter and all entrances.
- Make sure that supervisors and team leaders are clearly visible from the floor. Proper supervision is a prerequisite for keeping personnel and your mail center safe. Leaders must be easily accessible to respond to emergency situations.
- Post signs around the mail center listing whom to call in the event of various emergencies such as fire, theft, suspicious package, etc. This is probably the most important step you can take in preparing for emergencies or suspicious letters and packages.

Training and Testing

Preparing your mail center and employees to handle a threat will have a lasting impact on the safety of everyone in your agency. Education and awareness are the essential ingredients to preparedness. Employees need to remain aware of their surroundings and the packages they handle. You must carefully design and vigorously monitor your security program to reduce risk.

Through training, you can develop a culture of security awareness in your operation. Through rehearsal, you can ensure that critical lessons have been learned and retained. Managers should consider security training and rehearsal a critical element of their job.

In addition to educating the employees who work for you, you should educate the employees who work for your agency. Employee awareness of the measures you have taken leads to confidence in the safety of the packages that are delivered to their respective work areas.

One key to performance during an emergency is testing of the plan in advance. Test contingency plans in a way that does not alarm employees but follows the steps to take if there is an event. The dress rehearsals reinforce previous trainings and in an actual emergency, proper procedures will more likely be followed.

Rehearse scenarios and test contingency plans with employees to ensure that in the event of an emergency they will know how to respond. These rehearsals will help ensure that the lines of communication function as planned and that everyone knows their role. Hold post-test meetings to address problems, and resolve them before the next test.

Training is necessary to qualify someone to inspect letters and packages by X-ray. You should ensure that all of your personnel and any contractors who staff the X-ray machine have sufficient and current training.

Mail center employees should be trained to recognize and report suspicious packages. Characteristics of a suspicious package or letter vary, depending upon the types of mail that your operation routinely processes. What may be considered suspicious in one mail center may not necessarily be suspicious in another.

Copies of a suspicious letter poster should be displayed in every mail center. An example poster is available in Appendix C. Phone numbers of who to call should also be posted. An example is located in Appendix D.

Prevention is the key for keeping Commonwealth mail centers safe and secure.

Appendices

Appendix A

Abbreviations

Abbreviation	Definition
DGS	Department of General Services
GSA	Federal General Services Administration
HEPA	High Efficiency Particulate Air
HVAC	Heating, Ventilation and Air Conditioning
MSC	Mail Stop Code
SMS	State Mail Services
UPS	United Parcel Service
USPS	United States Post Office

Glossary

Address: The physical location's postal details to which information, sales literature or mailing can be sent.

Anthrax: A disease of humans that is not communicable; caused by infection with Bacillus anthracis followed by septicemia. See Chapter One for additional information.

Bulk Mail: Quantities of mail prepared for mailing at reduced postage rates, including discounted first class mail and advertising or non-preferential mail (standard mail). The Postal Service uses the terms "bulk" and "presorted" interchangeably. The term includes parcel post, circulars, or advertising mail generally sent in quantity.

Business Reply Mail: Specially printed return card or envelope, often with respondent's name and address information printed or affixed on it, which is included in the package to facilitate responding to an offer. Postage and fees are collected when the mail is delivered back to the original sender.

Dead Mail: Mail that is undeliverable as addressed and cannot be returned to the sender (usually because there is no address on the piece).

Emergency: A sudden unforeseen crisis (usually involving danger) that requires immediate action.

Endorsement: Handwriting or hand stamping on a mail piece, which designates class (First), handling (Fragile or Address Service Requested).

False Positive: Occurs when a system classifies an action as a possible threat implying a condition exists when in fact it does not.

Flat: The general term for non-letter or flat-size mail. These large mail pieces exceed the dimensions for letter-size mail and are specially sorted without bending so that the mail piece remains flat.

First Class: The type of mail the average citizen sends every day. First class mail receives fast delivery service at a high postage and includes priority, post cards, letters, and sealed parcels. Mail that is personal correspondence, bills and statements of account are first class mail.

Mail Bomb: Also called parcel bomb or letter bomb, is an explosive device sent via the postal service, and designed to explode when opened, injuring or killing the recipient, usually someone the sender has a personal grudge against, or more indiscriminately as part of a terrorist campaign.

Mailing Permit: Permission to mail at bulk (presorted) rates.

Metered Mail: Mail with postage printed by a USPS approved meter; stamps are not used.

Package Services (formerly Standard B and, before that, 4th class): Small parcels like compact discs and checks that weigh 16 ounces or more.

Parcel: A parcel is a mailable or shippable item other than a letter, book, or other document. Often called a package.

Postmark: A cancellation mark stamped on mail by postal officials; indicates the post office and date of mailing.

Postal Classifications: The Postal Service divides mail into different services, called ‘classes’. Each class of mail has different features, service levels, postage rates, and presort requirements. The cost of mailing varies with each classification.

Periodicals (formerly known as 2nd class): Commercial and nonprofit rates. Magazines and newspapers and other printed publications that are issued at least four times per year at regular, specified intervals. Periodicals usually must have a list of subscribers or requesters.

Presort: The process by which a mailer prepares mail so that it is sorted to the finest extent required by USPS standards. Presorting is required to bypass certain operations at the Post Office because the mailer groups pieces in a mailing by ZIP Code or by carrier route or carrier walk sequence. This process allows the mailer to take advantage of a discounted postage rate.

Risk Assessment: A study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

Undeliverable: When a mailing can not be delivered as addressed.

Appendix B

Resources

Additional resources for information about mail security include:

Virginia State Mail Services - http://sms.dgs.virginia.gov

Occupational Safety and Health Administration (OSHA) – http://www.osha.gov

Centers for Disease Control (CDC) - www.cdc.gov

Federal Bureau of Investigation (FBI) – www.fbi.gov

Federal Emergency Management Agency (FEMA) – www.fema.gov

Bureau of Alcohol, Tobacco, and Firearms (BATF) – www.atf.treas.gov

Military Mail Facility Security and Handling Suspicious Mail – http://www.usapa.army.mil/pdffiles/p25_52.pdf

General Services Administration (GSA) – www.gsa.gov

GSA Mail Management Office - www.gsa.gov/mailpolicy

US Postal Service (USPS) – www.usps.com

USPS Postal Inspection Service - www.usps.com/postalinspectors

USPS Mail Security Information - http://www.usps.com/communications/news/security/welcome.htm

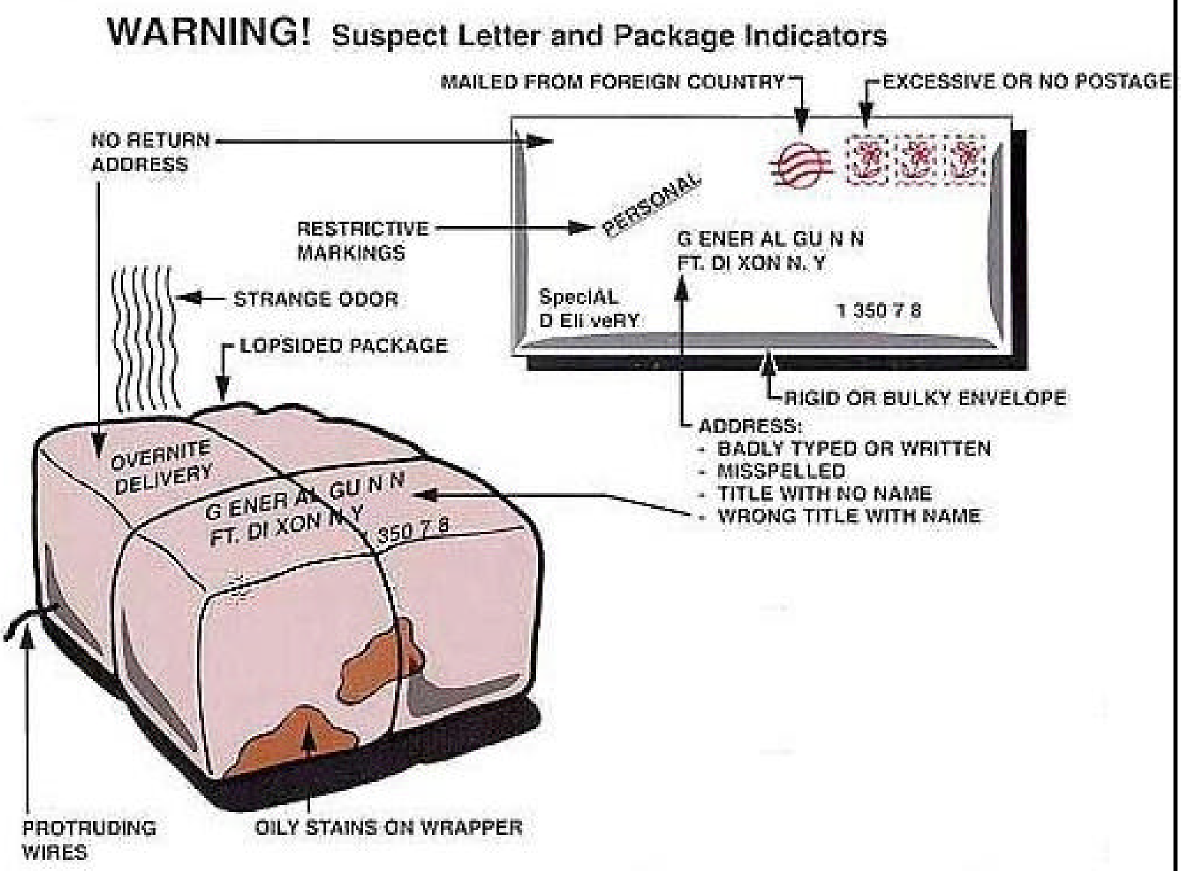
Appendix C

Suspicious Mail Poster

The next page contains the SMS Mail Security Poster. All Commonwealth mail centers should have this or similar information posted.

You may download a copy of the poster at SMS website.

State Mail Services
Suspicious Letter or Package
Advisory for All State Employees



What should you do if you receive a suspicious letter or package?

Handle with care. Don’t shake or bump.

Isolate and look for indicators.

Don’t open, smell or taste.

Treat as a Suspect! CALL 911

If parcel is open and/or a threat is identified …

For a Bomb

Evacuate Area Immediately
Call 911 (Police)

For Radiological

Limit Exposure - Don’t handle
Distance (Evacuate area)
Shield yourself from object
Call 911 (Police)

For Biological or Chemical

Isolate - Don’t handle
Call 911 (Police)
Wash your hands with soap and warm water

Police Department ____

Fire Department ____

Virginia Capitol Police (For state offices located in Capitol Square) (804) 786-HELP

Agency Safety Officer or Floor Warden____

Immediate Supervisor ____

Appendix D

Emergency Contact Sheet

The next page contains an emergency contact sheet for mail centers. All Commonwealth mail centers should have this or similar information posted.

State agencies in the Richmond metropolitan area should consult the State Mail Services website for a list of emergency contacts.

S.M.S.
STATE MAIL SERVICES

Mail Center Emergency Contacts

If you encounter a suspicious letter or package, evacuate the area immediately and then utilize the following contacts:

1. Agency Emergency Notification: ______________________________

____

After Hours: ______________________________

Follow the emergency notification plan for your work area. This may include setting off the nearest fire alarm or alerting the appropriate supervisor or safety personnel. There should be multiple contacts listed, which may include the agency safety officer or the floor warden.

2. Emergency Responder: ______________________________

____

Dial 911 or contact your local HAZMAT team/fire department, as appropriate. For offices located at Capitol Square contact the Virginia Capitol Police. Prior to an incident occurring make sure you communicate with your local emergency responders to identify your appropriate contact.

3. USPS Postal Inspectors: ______________________________

After Hours: ______________________________

After a credible threat has been established contact the US Postal Inspectors *(only when USPS mail is involved)*. Prior to an incident ever occurring make sure you communicate with your local US Post Office to identify your appropriate contact.

4. State Mail Services: (804) 236-3592 or StateMail@dgs.virginia.gov

After the incident is resolved report it to SMS. SMS is also available to assist with additional mail security questions.

Information about this Facility

Address: ______________________________

____

Maintenance Contact: ______________________________

After Hours Maintenance: ______________________________

Other Important
Information:

For additional mail security resources visit:
http://sms.dgs.virginia.gov