Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors

September 27, 2012

1st Edition

Homeland Security

Interagency Security Committee

THE FINDINGS IN THIS REPORT ARE NOT TO BE CONSTRUED AS AN OFFICIAL U.S. GOVERNMENT POSITION UNLESS SO DESIGNATED BY OTHER AUTHORIZING DOCUMENTS.

Preface

This document has been produced by the Combating Terrorism Technical Support Office (CTTSO) Technical Support Working Group (TSWG). The CTTSO operates as a Program Office under the Assistant Secretary of Defense (ASD) for Special Operations and Low Intensity Conflict and Interdependent Capabilities (SO/LIC&IC).

The CTTSO is charged with providing a forum for interagency users to discuss mission requirements to combat terrorism, prioritize those requirements, fund and manage solutions, and deliver capabilities. The CTTSO accomplishes these objectives through rapid prototyping of novel solutions and field testing before the traditional acquisition systems are fully engaged. This low-risk approach encourages interdepartmental and interagency collaboration, thereby reducing duplication and eliminating capability gaps.

This document is intended to provide best practices for the screening and handling of all incoming packages and letters, whether delivered via the United States Postal Service (USPS), commercial common couriers, or special messengers. In the majority of government agencies, the "mailroom" is the central receiving and distribution function for all incoming and outgoing mail and packages. For the purpose of this document, the authors use terms such as "mail," "mail handling," and "mail center" in a manner reflecting the common vernacular. These terms are used in a broad sense to describe the processing and distribution of not only USPS mail and packages, but also other forms of written correspondence and packages—such as those provided by commercial common couriers and special messengers. From a mail screening and handling perspective, this expanded definition of "mail" and "mailroom" will help ensure that all incoming "mail" items are considered when evaluating the application of the recommended best practices. The authors in no way intend for the reader to interpret use of these or any such similar terms as being representative of the technical definition of "mail" that properly identifies the materials, products, processes, functions, authorities, brands, and facilities associated with the USPS.

The original version of this document was produced with restricted dissemination and is only available to Federal Government agencies (see Publications at www.tswg.gov). The Interagency Security Committee has modified the document to be fully releasable to private individuals and organizations. Multiple Federal agencies, the Interagency Security Committee, and two private sector organizations contributed to the creation of this releasable version of the Best Practices Guide. They are acknowledged at the conclusion of this document.

Table of Contents

Executive Summary

The *Best Practices for Mail Screening and Handling* guide is designed to provide mail center managers, their supervisors, and an organization's security personnel a framework for understanding and mitigating risks posed to the organization by the mail and packages it receives and delivers on a daily basis. A wide range of potential threats can be introduced into an organization by way of the mail center. Threats that involve chemical, biological, radiological, nuclear, or explosive substances (CBRNE) are both dangerous and disruptive. Some threats, such as white powder hoaxes and threatening letters, are merely designed to disrupt the activities of an organization or to express dissatisfaction with a particular individual or policy. The mail center screening and handling processes must be able to identify threats and hoaxes and eliminate or mitigate the risk they pose to the organization, its employees, and daily operations. This guide provides an introduction to and understanding of the most efficient and effective processes and procedures to handle and screen mail entering an organization's mail processing facilities.

There is no single set of "best practices" that is applicable to all mail centers. However, there are a number of factors that help determine both the type of mail screening facility that is required and the range of screening procedures that should be implemented by the mail center manager. The purpose of this guide is to help mail center managers understand these factors and evaluate them in terms of their specific operational requirements. The *Best Practices for Mail Screening and Handling* guide is structured with a "building block" approach.

Section 1, ***Introduction***, provides an introduction to mail screening and outlines the analytical approach necessary to develop appropriate and effective screening processes. Most importantly, it highlights the fact that mail screening is both an "art and science." The clear message for all users of the guide is that there are no guarantees that even the best screening technology and procedures will identify all potential threats before a letter or package arrives at the desk of the intended recipient. The guide is intended to provide an overview of best practices for mail screening and sorting activities. It is not intended to replace Federal Government mail handling or U.S. Postal Service regulations, policies, or directives. To ensure that users are fully aware of these regulations and policies, **Appendix 1, *Government Mail Center Regulations and Related Documents,*** has been added as supplement to this guide.

Section 2, ***Potential Threats in the Mail Stream***, provides a review of the potential threats that could appear in the mail stream. Specifically, CBRNE threats are discussed and defined. In addition, this section of the guide provides a basic introduction to hoaxes and their impact on the mail stream. Having discussed the potential threats in the mail stream, the guide then proceeds to provide the user with a structured approach to countering these threats. First, mail center managers should perform a risk assessment associated with their specific mail center operations. Consideration of certain factors (e.g., the type(s) of mail received, organizational profile, location, facility security) is examples of the elements that should go into such an assessment.

Section 3, ***Analyzing the Risk in Mail Streams***, focuses on defining and explaining the elements of this assessment. To be both efficient and effective, screening processes should be well-designed and properly integrated into the overall process of receiving, sorting, and delivering

mail and packages. Proper screening requires consideration and evaluation of both the facilities within which the screening will be performed and the technologies and processes that will be used for screening within these facilities. Proper screening technology selection requires a solid understanding of mail and package volumes, accountability procedures, transfer requirements, and courier routes. This is particularly important in small mail centers where a few individuals must perform multiple tasks sequentially. The mail center manager must ensure that the screening workflow itself does not create any unexpected security violations or unnecessary contamination.

Section 4, ***Mail Screening Facilities***, provides mail center managers with an understanding of the foundation for mail screening through a description and definition of the primary categories of mail screening and sorting facilities. For example, the best practice for organizations that have determined they are at a high level of risk is to create an off-site mail and package screening facility. Organizations that have a lower level of risk associated with their mail and package processing operations, or perhaps have more limited resources, may create an isolated on-campus facility that leverages the security features of the larger campus. In instances where the facility risk level, mail volume, and budgetary constraints make separate facilities infeasible, mail screening facilities can be located within the building that serves as the primary office facility. Finally, small mail centers that operate from a single room may choose to integrate a separate stand-alone negative pressure mail room (NPMR) within their existing space for mail screening purposes.

Mail screening technologies and processes can have a significant impact on the ability of a mail center to receive, sort, and deliver mail and packages in a timely fashion. Some screening processes, such as those for radiation, can be done relatively quickly with little delay or disruption in the normal mail handling procedures. Others, such as the procedures for biological agents, can delay mail for many hours or even days, depending on the technology being used and the degree of certainty desired for the results. Mail security personnel must understand technology and process requirements that reflect the degree of risk in their mail operations and seek to achieve acceptable levels of both security and speed.

Section 5, ***Mail Screening Technologies***, provides an overview of the challenges associated with mail screening technologies. In addition, it provides an in-depth look at the types of technologies that can be used to counter each of the known threats. This section provides an initial understanding of what should be considered when selecting screening technologies, as well as what should be considered when integrating these technologies into specific mail screening processes from an operational and a staff safety perspective.

Section 6, ***Designing and Implementing Mail Screening Processes***, provides the user of this best practices guide with a logical framework for understanding and tailoring an organization's specific mail screening and handling process. Beginning with a process-mapping approach, the guide provides a basic understanding of how to approach establishing the processes for CBRNE screening. Most importantly, this section provides a clear understanding of how the screening processes can be integrated into the basic operations of accepting, screening, clearing, and processing mail and packages to ensure that sorting and delivery, interoffice mail, and outbound mail processing all benefit from and are not hindered by the screening overlay.

Key factors to be considered in mail screening are not only what mail should be screened and how it should be screened, but also what specifically should be done when a suspicious mail item or threat is identified. Simply put, response procedures are as important as the screening process itself.

Section 7, ***Suspicious Mail Incident Response Procedures***, provides a primary description and checklist of actions required when an incident occurs. Topics such as alert procedures, evacuation, and post-event follow-up are discussed in this section. Communication is a key component of incident response, and this portion of the guide addresses both internal and external communication requirements.

The success of mail screening and handling technologies in any mailroom environment, while dependent on facilities and equipment, ultimately will succeed or fail based upon the staff assigned to the operation and how well they understand their mail screening responsibilities.

Section 8, ***Training of Mail Screening Personnel***, is specifically directed at defining the primary categories of training that should be conducted and the recurring training that may be needed, as well as the frequency of "testing the system."

Section 9, ***Conclusions***, expands this basic training theme by defining the need for a team approach to the many aspects of mail screening that take place inside a mailroom/center. In addition, this section highlights a sometimes overlooked requirement: the need to continually evaluate the organization's mail screening approaches and adjust processes, procedures, and equipment as the threat changes.

Summary

Well-designed and implemented mail and package screening procedures can identify suspicious items on a regular basis. Mail centers must have clearly documented incident response procedures in order to mitigate the risk posed by these items and avoid unnecessary disruption of their operations. Response procedures for handing suspicious mail will vary from organization to organization and will be based upon a combination of factors such as the type of item discovered, the location of the mail screening facility, internal facility configuration, the number of personnel in the facility, and specific organizational protocols. All procedures must address initial response procedures, evacuation procedures, internal and external communications, evidence-handling procedures, and post-incident requirements. The United States Postal Inspection Service (USPIS) has highly trained personnel who are familiar with the most current guidelines for responding to incidents involving suspicious mail or packages and who can help design appropriate procedures for specific mail centers. Incident response procedures should also be coordinated with local first-responder personnel, if possible.

The movement of mail and packages is an important part of an organization's daily operations. A successful mail and package screening program requires the integrated efforts of senior organization officials, mail center management, security officials, technology providers, public health officials, and local first responders. Working together, this diverse team can ensure mail is properly screened and delivered in an affordable and efficient manner. This *Best Practices for Mail Screening and Handling* guide provides a primary tool to be used in achieving this goal.

1. Introduction

1.1. Purpose

This *Best Practices for Mail Screening and Handling* guide is designed to provide mail center managers, their supervisors, and an organization's security personnel with a framework for understanding and mitigating risks posed to an organization by the mail and packages it receives and delivers on a daily basis. The best practices guide outlines the most efficient and effective processes and procedures to handle and screen mail entering facilities for chemical, biological, radiological, nuclear, and explosive (CBRNE) threats. It includes a discussion of alternative technologies that can be employed and a recommendation for the proper location and construction of a mail screening facility.

1.2. Approach

This guide is designed to help administrative services directors, mail center managers, and an organization's security personnel achieve the following objectives:

- Define and analyze the risks associated with various types of mail streams;
- Understand the most likely types of CBRNE threats that may appear in the mail;
- Analyze and compare the efficacy, efficiency, and economics of alternative mail screening technologies, facilities, and processes;
- Select the appropriate screening technologies, facilities, and protocols;
- Design an efficient workflow for mail screening and sorting processes;
- Understand and implement identification tools for suspicious mail and packages;
- Understand and implement contamination reduction strategies;
- Develop and implement appropriate training for mail center personnel;
- Develop suspicious substance-specific incident response procedures; and
- Define internal and external communications procedures.

1.3. The Art and Science of Screening Mail and Packages

Mail screening is both an art and a science. It requires a properly built facility, clearly defined and consistently executed processes, well-trained and educated screening personnel, engaged security managers, and the support of all employees throughout an organization.

Threats in the mail stream are continually changing. New explosives, new electronic trigger devices, and new biological and chemical substances are appearing at more frequent intervals. Nuclear proliferation is making radioactive materials potentially more available than ever before. Terrorists are hiding explosives in common office supply

items and electronic devices, making them increasingly difficult to detect. Loading docks and delivery vehicles often provide easy access to buildings that have high levels of security screening at their lobby entrances. Mail screening processes must therefore be both appropriate for today's threats and flexible enough to deal with the sudden appearance of currently unknown suspicious substances or delivery mechanisms.

There are no guarantees that even the best mail screening technologies and procedures will identify all potential threats before a letter or package arrives at the desk of the intended recipient. Therefore, all employees, not just mail center personnel, should be trained to recognize suspicious mail and packages and know how to respond when such items appear. What happens to a piece of suspicious mail after it is identified can be just as important in reducing its potential impact on the organization as stopping it from appearing in the first place. This can be especially true in the case of "white powder letters" that contain no material that is actually harmful, but can be massively disruptive nonetheless. Although it is often difficult to initially identify whether the white powder is a nonthreatening substance, knowing how to respond to such letters appropriately can significantly limit the disruptive effect.

1.4. Additional Resources

This guide provides an overview of best practices for mail screening and sorting activities. It is not intended to replace Federal Government mail or U.S. Postal Service (USPS) postal regulations or internal organizational policies and directives. **Appendix 1**, ***Government Mail Center Regulations and Related Documents***, contains a list of related government mail center regulations and security-related documents that can be used to supplement the information in this guide.

2. Potential Threats in the Mail Stream

2.1. Overview

There is a wide range of potential threats that can be introduced into a facility by way of the mail center. Threats that involve CBRNE substances are both dangerous and disruptive. Some, like white powder hoaxes and threatening letters, are merely designed to disrupt the activities of an organization or to express dissatisfaction with a particular individual or policy. The mail center screening process must be able to identify all of these threats and eliminate or reduce the risk they pose to an organization's employees, facilities, and daily operations. **Appendix 2**, ***Suspicious Mail or Packages Poster***, provides a poster than can be used to help mail center employees visually identify suspicious mail and packages.

2.2. Chemical, Biological, Radiological, Nuclear, or Explosive Threats

2.2.1. Chemical

Categories of chemical threats include nerve agents, blood agents, pulmonary (choking) agents, blister agents, industrial chemicals, and irritants. Chemical threats can be presented in solid, liquid or gaseous/vapor form. They are difficult to detect until already deployed and their impact is almost always nearly instantaneous. Chemical weapons present unique challenges for both those who are seeking to use them as weapons and for those who are trying to detect their presence in mail and packages. If the goal is to target a particular facility or individual, both liquids and gases must be contained while the mail or package is being processed and then released when the item is opened by the recipient, by a timer, or by a remote electronic device. These requirements make use of chemical agents as mail-borne weapons somewhat difficult. However, chemical weapons can be packaged and deployed using almost any of the courier or local delivery services. Because of their light weight, some gases can also be compressed into small containers that can be mailed using USPS drop boxes. Mail and package screening systems must therefore be capable of identifying the release of chemical agents and, to the extent possible, containing the exposure to limited areas within the mail center or mail screening facility.

2.2.2. Biological

Biological agents are now a well-known and recognized category of mail-borne threat as a result of the anthrax letters that were discovered in October 2001. In addition, the biological agents that cause anthrax, plague, smallpox, and tularemia are most widely recognized as potential mail-borne biological weapons. As was demonstrated with the anthrax letters, large quantities of weaponized spores can be distributed using a common envelope. They can also be distributed through an aerosol method, although this would require a more sophisticated "bomb" enclosed in a flat or parcel. Due to their small size, and the high volumes of dust and paper residue common in most mail centers, biological agents can often go undetected by traditional visual inspections. Further complicating

screening requirements is the fact the incubation period for biological agents can be days or even weeks in some cases. Although this means an individual can be treated successfully once exposed, it also means that exposed individuals who are not aware of their contact with the biohazard can go for extended periods without receiving treatment, thereby hindering their probability of recovery.

One additional substance frequently included in any discussion of biological threats is ricin. Ricin is a poison found naturally in castor beans. Ricin can be made from the waste material left over from processing castor beans, and therefore can be considered readily available to anyone who would want to use it for terrorist purposes. A toxin, ricin cannot be easily absorbed through the skin, but is usually fatal when it enters the bloodstream through a cut or other form of open wound. Small particles of ricin can also be inhaled into the lungs, leading to death in two to three days. All of these factors make ricin a potentially dangerous substance when deliberately introduced into a mail center environment.

2.2.3. Radiological/Nuclear

Radiation threats include those produced by a nuclear detonation of some kind and those that are the result of unprotected exposure to radioactive material. Radiation can also be dispersed by combining a radiation source with a conventional explosive to create a "dirty bomb" that can be introduced into the mail stream as a package. Individuals exposed to radiation can suffer both immediate and long-term effects. Radiation detection systems that can be used in mail screening operations are capable of detecting and identifying various types of radiation particles (alpha, beta, and gamma). However, due to the difficulty in identifying alpha and beta particles from sources inside packages, most pagers and portals incorporated into mail center systems primarily target gamma radiation.

2.2.4. Explosives

Letter mail and packages are both susceptible to being used as mail bombs. New explosives and the miniaturization of the components necessary to initiate an explosion have made letter bombs more destructive and more difficult to detect. The similarity between the components of letter bombs and many common electronic devices has further exacerbated this trend. Fortunately, there is a wide range of detection technologies and approaches that can be used in even very small mail centers to identify explosive substances.

There is a wide range of explosives that have been used in letter and parcel bombs. Military explosives such as C-4 and "det cord," ammonium nitrate, and most recently pentaerythritol tetranitrate (PETN)-based explosives are all readily available and commonly used. Fortunately, explosives have a variety of characteristics that can be used to help detect them. In addition to their appearance and density, explosive substances emit a vapor trace that can be collected from letters and packages by using explosive detection canine teams or modern electronic sensors.

2.3. Dangerous Items and Contraband

2.3.1. Dangerous Items

In addition to items that are intentionally dangerous to the recipient, such as those discussed in the CBRNE section 2.2, mail can contain items that can cut or shock an individual when a letter is opened. Although unlikely to cause permanent harm, they do temporarily disrupt the activities of an individual or organization.

2.3.2. Illegal or Contraband Items

Illegal or contraband items, such as drugs, guns, knives, swords, and similar items, are also frequently shipped through the mail. Mail center screening processes must be prepared to identify and segregate these items in accordance with an organization's policies. In some organizations, such as security and law enforcement agencies, these items are allowed to be received through the normal mail center process.

2.4. Hoaxes

2.4.1. Definition

Hoaxes consist of suspicious mail items that are designed to present the appearance of a dangerous substance or other threat, but do not contain the actual substance necessary to cause harm. Hoaxes can be as disruptive to a mail center or an organizational facility as an actual threat.

2.4.2. White Powder Envelopes

The most common type of hoax is the "white powder envelope." Since the original anthrax letters, any white powdery substance can now be used to create the impression of anthrax. Sugar substitutes, baby powder, corn starch, and a myriad of other similar substances have successfully been used to simulate anthrax, leading to the evacuation of mail centers and office buildings. In addition, these hoaxes have also led to the writing of thousands of prescriptions for medications as a preventative measure for the employees of the mail operations. Frequently, white powder letters also contain threatening markings such as "anthrax inside" to create further suspicion and fear in the minds of the recipients. The goal for screening processes is to be able to identify these letters whenever possible and, in all cases, rule out the possibility that the white powder is a dangerous biological substance or toxin.

2.5. Threatening Content

2.5.1. Types of Threats

Suspicious mail may contain threatening language on the envelope itself or in the contents of the envelope. This can range from the aforementioned "anthrax inside" to language such as "Death to the President." Some letters will contain detailed descriptions of potential murders or terrorist attacks.

2.5.2. Proper Handling of Threat Letters

These letters must be identified and segregated as early as possible in the mail stream to both maintain their integrity as evidence and to limit any potential emotional harm to the intended recipient.

3. Analyzing Risk in Mail Streams

3.1. Types of Mail and Package Deliveries

Organizations receive mail and packages from a wide variety of sources every day. Some of these sources, such as USPS and major express couriers, have extensive security, screening, and control processes embedded in their day-to-day operations. Many others deliver items that can be considered to be from "trusted vendors" or other sources that limit the potential risk they pose to the intended recipient or other individuals within an organization. Unfortunately, even the best procedures and control measures do not completely eliminate risk; therefore, it is important to implement mail center procedures that provide both a second line of screening and the ability to track mail and packages from receipt to delivery. This section will briefly introduce the delivery services provided by various carriers and identify associated risks.

3.1.1. U.S. Postal Service

The USPS delivers a full range of items including letter mail, flats, and parcels. Although there is a variety of different categories of mail services (First Class, Priority, Express, etc.), all mail is routinely delivered by a USPS mail carrier or authorized agent. The USPS has a number of security measures in place that help reduce the risk posed by the mail and packages it delivers on a daily basis. These include personnel screening, suspicious mail training for their carriers, limits on the size and weight of packages that can be left in blue USPS mailboxes, and limited biohazard screening for B. Anthracis (the biological agent that causes anthrax) at its large processing centers. Despite these measures, mail and packages can be introduced into the USPS system by virtually anyone, without any requirement for mailer identification or a return address.

3.1.2. U.S. Postal Service Accountable Mail

The USPS offers extra services through the use of its Certified and Registered mail products that may also contribute to enhanced security. With Certified Mail, the mailer receives a receipt stamped with the date of mailing. Each item has a unique article number that allows delivery to be verified online. As an additional security feature, the recipient's signature is obtained at the time of delivery and a record is maintained by the USPS. Registered Mail provides an even higher level of security by incorporating a system of receipts to monitor the movement of the mail through the USPS sorting and delivery system. Both of these systems are designed to make sure the items being mailed are not lost or stolen. They do not, however, do anything to reduce the risk contents the mail piece may pose to the intended recipient.

3.1.3. Express Couriers

National express couriers (FedEx, UPS, etc.) provide pickup and delivery of express mail and packages. The security features associated with these services include end-to-end tracking and limited screening for potentially dangerous substances throughout the

sorting process. Like USPS items, there are few restrictions on who can introduce an item into the system and no mailer or shipper identification is required. Individuals can simply present their item to the clerk at a retail shipping facility and pay for the transaction in cash. In most cases, recipients are required to sign for items in order for them to be released by the express courier. This system provides security of the items being mailed, but again, does little to reduce the threat posed by the contents of the flat or parcel being received. Terrorists have recently begun to use global express couriers as channels for explosive packages. Packages that are transported by air pose a threat to both the air carrier and the intended recipient, evidenced by the October 2010 interception of improvised explosive devices in the form of computer printer cartridges originating from Yemen and destined for the United States. This practice of using air carriers has led to couriers instituting additional screening procedures and placing restrictions on outbound shipments from selected high-risk countries.

3.1.4. Other Couriers

In addition to well-known national couriers, there is a full range of regional and local couriers that provide more limited delivery services. These couriers range from well-established enterprises with processes, sorting facilities, and vehicles comparable to the national carriers, to small businesses that provide bicycle or motorcycle couriers within a single metropolitan area. Background screening, training, and security procedures vary widely among this group; therefore, they must be considered as some of the potentially higher risk sources of suspicious items from the mail center perspective.

3.1.5. Other Deliveries

Though the primary focus of this guide is on mail center operations, there are numerous other individuals that deliver items to an organization on a daily basis. These include newspaper and magazine services, fast food vendors, gift shops, florists, office supply vendors with their own or contracted delivery vehicles, and large third-party logistics trucking firms that are hired to deliver products from the original manufacturer or retailer. Each of these sources of deliveries has an associated risk and must be considered on an individual basis. Wherever possible, it is best to incorporate them into the mail center screening and delivery system to the fullest extent. Deliveries of this type will often include items that are too large for traditional screening systems, so additional procedures to identify and verify vendors, delivery vehicle drivers, and recipients will be necessary. These procedures may be performed by the facility physical security personnel rather than mail center personnel.

3.1.6. Interoffice Mail

One source of mail and packages that often does not get an adequate review during an assessment of mail and package screening operations is interoffice mail. Created and delivered entirely within an office building or campus environment, interoffice mail is considered to be “safe” and from one “trusted source” to another. Unfortunately, this is not always the case, and interoffice mail must be considered another potential source of suspicious mail. Outgoing interoffice mail receptacles are often little more than open containers placed in or around mail box distribution points. Disgruntled employees,

visitors, maintenance personnel, and others can introduce suspicious mail directly into the internal mail sorting and delivery process, bypassing the screening technology and procedures that have been established for USPS and express courier deliveries.

3.2. Risk Profile

A risk profile should be completed on any existing mail center; prior to the design, installation, and implementation of any new mail center screening facility; and when modifying the screening capabilities of an existing facility. Although the mail center is the focal point of the assessment and profile, it should be completed with the assistance of the organization's security personnel and facilities manager, whenever possible.

The level of risk associated with an individual organization may vary widely from a similar facility in a different organization located across the street. In addition, although properly prepared risk assessments are sufficiently broad as to incorporate a variety of profiles, the mail center manager or person responsible for the mailroom function must recognize that risk levels can change rapidly.

In general, the risk associated with the operation of an organization's mail center can be viewed through three basic factors. The following "formula" can be used as the basis for determining an organization's mail center risk level:

RISK = THREAT + VULNERABILITY + CONSEQUENCE

3.2.1. Threat

The threat has been defined in terms of the CBRNE substances (plus hoaxes) described in Section 2. Any organization analyzing their potential risk status should consider all of these threats as potentially applicable to their organization.

3.2.2. Vulnerability

Vulnerability is the organization's assessment of the strengths and weaknesses of their operations and the physical characteristics of their mail center with respect to the known and projected threats. For example, could a biological or radiological threat be introduced into their organization through the mail stream; or could an explosive device be introduced in an undetected manner?

3.2.3. Consequence

In evaluating an organization's risk profile, a key driving factor to be considered is the consequence of an incident involving the mail center. For example, if the mail center were shut down, would the entire facility have to shut down as well? If a mail center incident requires evacuation of the building, what effect will that have on the daily operations of the organization? Will critical functions be disrupted? Will clients be affected?

One of the most significant aspects to be considered by any organization in evaluating the consequences of either a real or suspect incident is the potential financial impact.

If production is delayed for a day–what will that mean in terms of lost revenue? If employees are forced to leave their facility and cannot work for one, two, or more days, what is the cost of their salaries? One case study, involving a large international organization, demonstrates the severity of this impact. Immediately after the original anthrax attacks in the Washington D.C. metropolitan area, the organization received a letter containing white powder. This caused the entire organization to shut down for a period of 2 to 3 days while the substance was analyzed and ultimately determined to be a hoax. In a post-event analysis, the organization estimated that the cost of paying employee salaries for the period of the shut down exceeded five million dollars. Ultimately the organization determined that the cost of an offsite mail screening facility would cost only a fraction of the lost wages on an annual basis–thus it is critical that an organization include financial impact in their risk profile assessment.

3.2.4. General Risk Factors

A wide number of factors can be included in any risk profile, and they will vary from organization to organization. Although all potential risk factors cannot be listed here, the following provides some general guidelines to the type of factors that should be considered.

3.2.4.1. Public Posture

Is the organization a logical target for terrorist attacks? In evaluating this factor, an organization should look at its position with respect to where and how it is considered part of the industrial base. The following industrial areas may be considered as higher risk areas:

- Banking
- Energy
- Power
- Defense
- Legal
- Pharmaceutical
- Chemical
- Nuclear Facilities
- Bio-Medical Research
- Any organization considered part of the "Military Industrial Complex"
- Transportation
  - Air
  - Land
  - Sea
- Health and Medical
- Telecommunications
- Construction

3.2.4.2. Symbolism

A key factor to consider when evaluating the posture of an organization is the symbolism that can be attached to targeting that organization. Key factors to consider include:

- A well known or well publicized entity–Is the organization the type that if attacked would have continuous and widespread "down line" impacts? The anthrax attacks caused widespread concern and worries because virtually

everyone was concerned about their mail, regardless of whether or not they were individually considered a good target.

- Negative psychological impact–If an organization is targeted or the recipient of a threat, there can, and most likely will be, a perception that all entities associated with that organization are at risk, as well a potential risk for any organizations that deal with the targeted entity. The negative psychological impact can drive a lack of confidence in the organization, its position in the industrial sector, and a corresponding loss of confidence in government entities. For example, threats made against one or two prime entities in the banking industry have resulted in the entire industry being considered a target with potentially wide spread consequences.

3.2.4.3. Location

Organizations located in large, multitenant facilities (high rise office buildings, standalone office parks, etc.) are more at risk to be affected if any of the organizations in their facility are recipients of a mail-borne threat.

Likewise, organizations located in large urban centers are more likely to be affected by any threat presented in their city. A biological attack in New York City, as an example, would have all the organizations in NYC immediately concerned; whereas an attack on an organization that is relatively isolated may not be considered to have as wide a "footprint" with respect to collateral concerns.

3.2.4.4. Population

Terrorist threats attempt to instill fear in the largest number of individuals possible; therefore, organizations with large employee populations are at higher risk than smaller entities.

As with the Location factor, organizations located in areas with a high density population can also be at risk regardless of the number of their individual employees.

3.2.4.5. Intangibles

A wide range of additional factors must be considered when evaluating an organization's and facility's risk profile, some of which are organization or industry specific. For example, has the organization/tenants, or the area within the industrial sector, been the target of any previous terrorist attacks? Has the organization/tenants been the subject of any highly publicized negative press? Has the organization/tenants been the target of organized demonstrations, boycotts, labor disputes, etc.? Has the organization/tenants been the subject of attacks by disgruntled employees? A positive answer to any questions such as these should be considered in the risk assessment.

Other aspects that should be considered include, but are not limited to, such factors as:

- Facility layout–single building, multiple buildings, or campus;
- Single tenant or multiple tenants;
- Controlled access, public access, or a combination;

- Loading dock configuration;
- Visibility of the organization's facility that contains the mail center (e.g., signage, lighting, advertising); and
- Number and frequency of visitors and/or tourists to the facility and the area in which it is located.

All of these and similar factors will have a direct impact on an organization's overall risk profile.

3.2.4.6. Size and Volume of the Mail Stream

The risk associated with a mail center is also driven by its size and the mail volumes it supports. **Appendix 3**, ***Mail Center Classification***, provides an approach for appropriately classifying a mail center based on the organization it supports and its mail and package volume levels. Finally, **Appendix 4**, ***Mail Center Security Assessment Worksheet***, can help mail center and security managers take a snapshot of their existing facilities and processes. Completion of this worksheet can significantly enhance understanding of where significant risks may be present in existing mail center operations. It will also serve as the basis for the design of an appropriately scoped mail center screening facility and process.

4. Mail Screening Facilities

4.1. Primary Categories of Mail Screening and Sorting Facilities

4.1.1. Offsite Screening Facilities/Remote Delivery Sites

The best practice for organizations that have determined they are at a high level of risk is to create an off-site mail and package screening facility. Many organizations or subordinate components will incorporate this facility into a remote delivery facility where all deliveries, including supplies, furniture, and food for in-house cafeteria vendors, must be processed. Mail and packages will be received, screened, sorted, and prepared for delivery at this facility. Secure courier vehicles then transport the items to office locations for internal distribution. Security can be enhanced for these facilities by implementing scheduled, permission-based delivery procedures and tracking.

4.1.2. Isolated On-Campus Facilities

Organizations that have a lower level of risk associated with their mail and package processing operations, or more limited resources, may create an isolated on-campus facility that would operate much in the same way as an offsite facility. The only difference is the facility would be located within the security perimeter of the office complex maintained by the organization. Although these facilities lack some of the stand-off capability that a true offsite facility provides, they significantly reduce the ability of a suspicious mail piece or package to disrupt organization operations for extended periods of time. Separate mail screening facilities isolate any potential threat and enable first responders to address the issue without typically requiring a complete evacuation of the office space occupied by an organization's employees. Whenever possible, these on-campus screening facilities should not be co-located with other operations. They should also have separate security and heat, ventilation, and air conditioning (HVAC) systems.

4.1.3. Primary Office Locations

In instances where the security level, mail volume, and budgetary constraints make separate facilities infeasible or excessively impractical, mail center screening activities can be located within the building that serves as the primary office location for the organization. The mail center should be placed in a secure area with direct access to the outside of the building in order to limit movement of mail and packages within the building prior to screening activities taking place. If direct outside access is not feasible, mail and packages should be transported in a secure, negative pressure mail cart to minimize the spread of any potential biological contaminants.

4.1.4. Single Room Mail Center Operations

Due to their very limited mail volumes or severe space restrictions, many mail center operations are required to operate from a single room. Frequently, these mail centers must share a loading dock with other organizations or tenants in the building. These mail centers should seek to employ as many of the security capabilities resident in larger

facilities as possible. There are scalable, configurable, stand-alone negative pressure mail rooms (NPMRs) and small blast containment systems that can provide many of the benefits of systems designed for large footprint, multi-room mail centers.

4.2. Mail Screening Facility Core Requirements

Table 4-1, "Mail Screening Facility Design," outlines the core facility requirements and where they will be met for the various types of mail screening facilities discussed above. In instances where an organization is able to establish and construct a true offsite mail screening facility, the requirements may all be satisfied by capabilities that are resident in the facility itself.

Table 4-1. Mail Screening Facility Design

Core Facility Capabilities	Off-site Screening Facility	Isolated On-Campus Facility	Primary Office Location	Single Room Mail Center
Perimeter Fence	Facility	Campus	Building	Building
Perimeter Security Guard	Facility	Campus	Building	Building
Monitored Closed Circuit Television (CCTV) Cameras	Facility	Campus	Building	Building
Intrusion Detection System	Facility	Mail Center	Mail Center	Mail Center
Access Control System	Facility	Campus and Mail Center	Building and Mail Center	Building and Mail Center
Security Guards	Facility	Campus	Building	Building
Visitor Control System	Facility	Campus and Mail Center	Building and Mail Center	Building and Mail Center
Separate Inbound and Outbound Loading Docks	Facility	Mail Center	Mail Center	N/A
X-ray Screening Room with Blast Containment	Facility	Mail Center	Mail Center	Loading Dock
Separate HVAC System	Facility	Mail Center	Mail Center	Mail Center
Screener Changing Rooms	Facility	Mail Center	Mail Center	N/A
Negative Pressure Screening Rooms	Facility	Mail Center	Mail Center	NPMR
Mail and Package Quarantine Rooms	Facility	Mail Center	Mail Center	NPMR
Accountable Mail Processing Rooms	Facility	Mail Center	Mail Center	Restricted Area
Inbound Mail Processing Room	Facility	Mail Center	Mail Center	Designated Area
Outbound Mail Processing Room	Facility	Mail Center	Mail Center	Designated Area
Internal and External Communications Systems	Facility	Mail Center	Mail Center	Mail Center
Emergency Facewash / Decontamination Facilities	Facility	Mail Center	Mail Center	Mail Center
Emergency Power Generator	Facility	Mail Center	Building	Building

For isolated on-campus mail screening facilities, the overall campus security system will provide some security protection for the mail center. For mail centers that are located in a primary office location, the office building security system will serve a similar function as a campus security system. Finally, for mail centers that consist of little more than a single large room, there may be a need to supplement the building and mail center security with a containment system such as an NPMR.

Tables in **Appendix 5**, ***Mail Screening Requirements***, provide both an example of one way to integrate and evaluate factors such as core requirements, the overall level of risk, the mail center classification, the current mail processes assessment, and any additional factors that security and management personnel deem significant as well as a starting point from which mail center managers and organization security personnel can begin to build out their own mail screening operation.

5. Mail Screening Technologies

5.1. Overview

5.1.1. Mail Center Screening Challenges

Mail screening technologies and processes can have a significant impact on the ability of a mail center to receive, sort, and deliver mail and packages in a timely fashion. Some screening processes, like those for radiation, can be done relatively quickly with little delay or disruption in the normal mail handling procedures. Others, such as the procedures for biohazards, can delay mail for many hours or even days, depending on the technology being used and the degree of certainty desired for the results. Mail security personnel must develop technology and process requirements that reflect the degree of risk in their mail operations and seek to achieve acceptable standards of both security and speed.

5.1.2. Alternative Approaches

There is no single set of "best practices" that is applicable to all mail centers. For some specific areas, there are clear best practices. All mail center personnel should have a background or security check prior to starting work. There must be a way to secure a mail center when it is not being used. Mail centers must have redundant capabilities consistent with their organization's continuity of operations plan (Backup/Fallback and/or Disaster Recovery Plans). Offsite mail centers provide better protection than a mail center located on the main floor of an organization's primary office building. Still, if available budgetary resources do not support the construction or leasing of an offsite facility and the courier vehicles required to transport mail back and forth, then the organization should seek to employ the best practices that apply to screening procedures for onsite mail centers. This document highlights the practices that are most suitable for mail centers located in everything from minimum to very high-risk facilities. Best practices for mail screening for medium to very high-risk mail centers include a full range of CBRNE screening processes. For minimum and low risk facilities, aggressive visual screening and X-ray scanning may be adequate.

Facilities judged to be at medium risk should provide separate, isolated HVAC systems in lobbies, loading docks, mailrooms, and other locations susceptible to mailborne threats that are isolated from other building areas. In addition to those measures undertaken for facilities at medium risk, high-risk facilities should ensure the envelope of isolated loading docks and mailrooms are full-height construction and are sealed to the floor, roof, or ceiling above. Finally, in addition to those measures undertaken for facilities at high-risk, facilities judged to be at very high risk should provide instrumentation to monitor the pressure relationship established by the isolated system.

Table 5-1, "Common Screening Technology Applications," provides an overview of what technologies and approaches are available to detect each of the potential threats that have been discussed in **Section 2**, ***Potential Threats in the Mail Stream***.

Table 5-1. Common Screening Technology Applications

SUBSTANCE	VISUAL INSPECTION	AUTOMATIC SENSORS	HANDHELD SENSORS	CANINE TEAMS	X-RAY SCANNERS	AIR SAMPLING SYSTEMS	CDC LRN* Tests	AUTOMATIC BIO ID SYSTEMS
Chemical	X	X	X			X		
Biological	X	X	**			X	X	X
Radiological		X	X					
Nuclear		X	X					
Explosives	X	X	X	X	X			
Dangerous Items	X				X			
Contraband	X		X	X	X			
Suspicious powders	X						X	
Threatening Content	X							

*****Centers for Disease Control (CDC) Laboratory Response Network (LRN)

** Current American Society for Testing and Materials (ASTM) guidance states that suspicious powders should be sent to the LRN for analysis of biological agents.

5.2. Integrating Technologies Into Mail Screening Operations

5.2.1. Mail Screening and Sorting Facilities

Mail screening should take place in a dedicated facility, hardened to protect against explosive devices, with a separate HVAC system and negative pressure mail screening facilities.

Mail centers that are within shared facilities or buildings housing an organization's offices should contain an NPMR that provides protection against the spread of biohazards during the initial screening process. At a minimum, the mail center should operate on a separate HVAC system that can be shut down in the event of a biohazard incident.

The facility dock area should have a minimum of two loading docks so that inbound and outbound materials do not pass through the same door. For the highest-level of protection, the negative pressure environment should begin at the inbound loading dock door(s). The doors should be separated from one another by an interior wall within the negative pressure environment.

Mail centers that do not have negative pressure environments should take special precautions to limit exposing the mail to the rest of the office building or facility. If the mail cannot be brought directly into the mail center through a loading dock, it should be transported through the building in a negative pressure mail cart or other sealed container.

Physical security requirements for the mail screening and sorting facility should be based on a thorough risk assessment. In instances where mail centers contain one or more rooms inside a larger building, the mail center should have a separate access control system. The mail center access control system should be connected to the overall building security system and monitored by personnel in the security operations center.

5.2.2. Personal Protective Equipment

Personal protective equipment (PPE) should be used by all personnel directly involved in the mail screening process and those whose duties require them to enter a room or area where deliberate biohazard screening is taking place.

Based upon guidance provided by the Centers for Disease Control (CDC), the minimum level of acceptable PPE for medium and higher risk environments includes a Tyvek suit, a National Institute of Occupational Safety and Health (NIOSH) approved, disposable Filtering Facepiece Respirator (FFR), Nitrile gloves, and foot coverings. Individuals must receive appropriate annual medical screening to ensure they are physically able to wear a respirator. The environmental health and safety representative within an organization can help coordinate, document, and monitor the required PPE implementations.

PPE should be donned prior to entering the mail screening portion of the negative pressure environment and removed prior to completely leaving any negative pressure environment. A properly constructed facility will include entry and exit chambers or ante-rooms where this process can be completed without contaminating adjacent warehouse space or offices.

The PPE itself should be considered potentially contaminated until any tests for hazardous substances have been completed with negative results. Reusable PPE should remain in the negative pressure environment, once it has been used for screening purposes. Disposable PPE should be sealed in a disposable container and removed once any tests for biohazards have been completed without incident.

For additional protection, mail screening personnel may also wear reusable NIOSH approved canister type protective masks with replaceable filters. The masks should be worn prior to entering the mail screening facility and removed only upon leaving the negative pressure facility.

For mail screening and sorting operations where the risk analysis has demonstrated that there is a low level of potential exposure to biological hazards, it is still recommended that mail center personnel wear a smock or similar covering, a NIOSH approved FFR, and Nitrile gloves. These items help protect the individuals from the high concentrations of paper dust and other similar substances routinely found in mail centers. The gloves also help protect the hands of mail center personnel during high volume mail sorting operations. In addition, mail screening personnel may also be offered thin cotton gloves to be worn under Nitrile gloves to minimize any irritation resulting from direct contact with Nitrile.

5.2.3. Radiation/Nuclear

Pedestal or wall-mounted radiation detection equipment should be placed along the vehicle route to the loading dock area at the first place a vehicle enters the secure perimeter.

Additional radiation detection devices should be mounted in the loading dock area and monitored by personnel within the organization's security command center.

Screening personnel working on the loading dock should be required to wear personal radiation detection pagers while they are unloading vehicles.

5.2.4. Chemical Screening

The mail screening facility should have chemical detection sensors located in the loading dock area and the mail and package screening rooms. Chemical sensors should be capable of detecting and identifying a wide range of chemical weapons and industrial chemicals.

Sensors should provide an audible and visual alarm that can be detected in the immediate area. Chemical sensors should also be linked to the organization's security command center and be monitored on a continuous basis.

5.2.5. Suspicious Items

Mail screening, sorting, and delivery personnel must be observant for suspicious mail and packages at every stage in the process. Many suspicious items such as hoax letters and packages containing hazardous materials can be detected early in the sorting process by properly trained mail handlers. For individual item screening, mail should be perforated, cut, and tumbled or opened prior to a sample being taken. These processes will enhance the likelihood that an adequate volume of material will be collected for proper identification to take place. They will also help identify suspicious powders that are not detected by systems focused on actual biological agents. Sample collection should be conducted according to American Society for Testing and Materials (ASTM) guidance.

Mail trays, tubs, and individual items must be inspected for obvious signs of white powder, liquids, or suspicious markings as they are unloaded from the courier or mail vehicle at the loading dock. If detected, suspicious items (and the associated tray or tub within which they were transported) should be immediately segregated.

Where possible, mail centers should implement a barcode, radio-frequency identification, or other tracking system that enables positive control over individual trays, tubs, and other mail equipment throughout the entire screening, sorting, and delivery process. This will enable easier "back tracking" and identification of potentially contaminated areas if a dangerous item is discovered downstream from the mail center.

5.2.6. Explosives

Explosives in mail and packages can be detected using a variety of technologies and approaches. The specific technology or approach that is adopted will reflect the risk

level, the volume of mail and packages received, and the speed with which the process must be completed.

Explosive detection canines (EDCs) can be used to inspect courier vehicles as well as mail trays or tubs before they are brought into the primary mail screening facility. EDC teams can screen a high volume of mail and packages for explosives in a relatively short period of time. Properly trained canines can detect all of the common explosives being used, including pentaerythritol tetranitrate, currently the explosive of choice for many terrorists.

Hand-held and tabletop explosives trace detection equipment can be used to detect the presence of explosives within items or explosive residue on the outside of mail and packages. Most trace detection systems are of limited use in high-volume mail screening operations because of the requirement to collect an air sample or a swipe from an individual item for testing. They can be used effectively for second-level evaluations of suspicious items and for testing courier vehicles and personnel.

X-ray scanning systems have long been the most widely used technology to detect bombs and other dangerous items in mail and packages. Mail and flats can be screened while in trays or tubs. Packages should be screened individually. Most modern X-ray systems have software designed to help the screener identify explosives, based on the density of the substance. The effectiveness of X-ray screening is highly dependent on the training and attentiveness of the equipment operator. Mail centers that process a large volume of electronics will find X-ray scanning of packages to be especially challenging, due to the similarity of many electronic devices to explosive devices. X-ray scanning systems should be capable of producing and saving digital images from the scanning equipment that can be viewed remotely for additional evaluation purposes.

5.2.7. Biohazards

Mail and packages should be screened for a full range of potential biohazards as indicated by Federal, State, local, and/or organization-specific security guidelines.

Biohazard screening can be implemented on a piece basis or bulk (tray) basis. Piece-level screening increases the likelihood that biological agents will be identified, but decreases the mail processing throughput speed significantly.

For individual item screening, mail should be perforated, cut, and tumbled or opened prior to a sample being taken. These processes will enhance the likelihood that an adequate number of spores will be collected for proper identification to take place. They will also help identify suspicious powders that are not detected by systems focused on actual biological agents. Sample collection should be conducted using CDC-approved devices and collection media and ASTM guidance.

Screeners should collect samples from the trays and tubs used to transport the mail as well as from the mail itself. They should also collect samples from the mail screening and processing equipment itself.

It is strongly recommended that samples taken from the mail be processed by a CDC LRN laboratory facility, even if onsite testing equipment is being employed. Mail and packages should be kept in local quarantine until the results of the lab tests are released.

Onsite sampling and testing systems can be used in areas where CDC LRN laboratories are not reasonably available. There are a growing number of systems that can collect air samples and test for many biohazards likely to be used in suspicious mail and packages. Test results from such systems may not be valid for forensic evidence purposes; therefore, proper control of threat material is required from an evidentiary standpoint to support post-event testing by CDC LRN laboratories.

5.2.8. Dangerous and Contraband Items

Dangerous items are best identified using a combination of visual inspection and X-ray scanners. Visual inspection will also help identify the most common type of hoax letters. Many trace detection systems that are used for identifying explosives also have the ability to detect narcotics using the same approach.

5.2.9. Containment Systems

Negative pressure air rooms provide a significant level of containment of potential biohazards. They reduce the threat to personnel and facilities and make cleanup of any actual contamination easier to accomplish. These systems can either be built as integral components of the mail screening facility or can be provided as separate, portable configurations. In all cases, they will need access to, or must provide their own, heated and cooled air for the comfort of the mail screening personnel. These systems should not be connected to the facility's centralized HVAC systems. Negative pressure air rooms should be designed to achieve an appropriate number of Air Changes per Hour (ACH). Generally, for illustrative purposes, the CDC recommends ≥12 ACH as a minimum for infectious diseases. Mail room managers can use a number of references such as the American Society of Heating, Refrigerating and Air Conditioning Engineers (www.ashrae.org/) for detailed guidance in the creation of a negative pressure environment.

Mail centers that do not have negative pressure systems should have sealable plastic bags or other suitable containment systems available to enclose suspicious envelopes. The bags should be clear so that first responders and other security personnel can view the external information on the envelope. If an envelope has leaked white powder during handling or when it has been opened, it should be covered and disturbed as little as possible until first responders can complete a field check of the substance.

There are several different types of explosive containers that are sold for use in mail centers. While they do provide protection from explosives when used properly, most first responders now recommend that mail center personnel limit their handling of letters and packages that may contain explosive devices. If a letter or package being X-rayed reveals that it contains an explosive device, it should be left inside the X-ray scanner itself. The scanner will provide a level of protection for mail center personnel while they evacuate the local area pending further analysis by security personnel or first responders.

5.2.10. Decontamination of Mail, Personnel, and Facilities

Specialized equipment exists to decontaminate mail; however, decontamination requirements related to specific incidents should be managed by first responder personnel and accomplished with equipment they provide. Contaminated facility cleanup should only be conducted in conjunction with public health officials and in accordance with CDC guidance, Environmental Protection Agency regulations, and other hazardous material regulations.

Decontamination of an organization's mailroom personnel or those affected in other areas of a facility should generally be managed by first responders and accomplished with equipment they provide. Emergency showers and eyewash stations should be available to mail screeners who are exposed to suspicious powders or other irritants as part of the organization's mail screening infrastructure. These facilities should be located in areas that are easily accessible to screeners and do not require individuals to leave the immediate screening area.

The procedures for use of these emergency decontamination facilities should be reviewed by local first responders to ensure that any steps taken by an organization will not impact any further decontamination by first responders and/or in any way compromise the overall personnel decontamination process.

6. Designing and Implementing Mail Screening Processes

6.1. Process Mapping

To be both efficient and effective, mail screening processes should be well-designed and properly integrated into the overall process of receiving, sorting, and delivering mail and packages. This requires mail center managers to map out their current end-to-end mail receiving and delivery processes before inserting screening technologies or processes. Many aspects of screening technology selection will require a solid understanding of mail and package volumes, accountability procedures, transfer requirements, and courier routes. This is particularly important in small mail centers where a few individuals must perform multiple tasks sequentially. Process mapping also enables the mail center manager to ensure that the screening workflow does not create any unexpected security violations or unnecessary contamination.

6.2. Integrating Screening Procedures

The following is a partial list of top-level processes that should be mapped and evaluated with regard to mail screening requirements for mail and packages. Not all apply to every mail center operation. Each item presents opportunities for suspicious mail to enter the mail sorting system or be transferred from one employee to the next. Each also provides an opportunity for suspicious mail to be identified, isolated, and contained before it can cause harm to the intended recipient.

6.2.1. U.S. Postal Service

6.2.1.1. Mail and Package Pickup from Designated U.S. Postal Service Facility

Only authorized personnel specifically identified by the organization should be allowed to sign for materials from U.S. Postal Service (USPS) facilities.

6.2.1.2. Transportation to the Mail Center or Mail Screening Facility

Courier vehicles provided by the organization should provide security for mail and packages during transport. Vehicles should not be left unattended at any time.

6.2.1.3. Tracking and Accountability Processes

All accountable mail items and packages should be tracked from the moment they are picked up or received until they are delivered to and signed for by the intended recipient.

6.2.1.4. Transfer of Mail and Packages to Mail Center Screening Personnel

Mail and packages should not be left unattended on the loading dock or in a publicly accessible area.

6.2.2. Express Couriers and Other Delivery Services

6.2.2.1. Receipt of Mail and Packages from Courier

Courier personnel should be positively identified by mail center personnel before accepting any items.

6.2.2.2. Tracking and Accountability Processes

All express items and packages should be tracked from the moment they are received until they are delivered and signed for by the intended recipient.

6.2.2.3. Large Volume/Bulk Shipments

Mail center personnel should not sign for items "in bulk" without validating they are receiving the actual items on the manifest.

6.3. Screening Processes

Individual screening processes may vary based on the specific technology being employed.

6.3.1. Radiation/Nuclear

Trucks and delivery vehicles should be screened as they are approaching the mail screening facility, and again at the loading dock.

6.3.2. Chemical

Continuous screening of the environment in and around the mail screening facility and/or mail center should be conducted.

6.3.3. Explosive

Screening of vehicles, mail, and packages should be done using explosive detection canine teams prior to bringing items into the mail screening facility. Screen mail tubs or trays and individual packages using an X-ray scanner equipped with explosive detection software.

6.3.4. Dangerous Items and Contraband

Screening for dangerous items should be done using aggressive, visual screening and the X-ray scanner.

6.3.5. Biohazard

Samples should be collected from mail and packages and tested for common biological hazards at a CDC LRN laboratory or using onsite Polymerase Chain Reaction (PCR) equipment. As a "best practice," it is strongly recommended that any on-site testing that is accomplished be verified and confirmed by the LRN. All mail items should be kept in quarantine in a negative pressure environment until negative test results have been obtained.

6.4. Sorting and Delivery Processes

6.4.1. Mail Sorting and Package Sorting

Mail and packages should be sorted in a secure facility that provides access only to mail center personnel.

6.4.2. Inbound Courier Services

Mail that is being transported from the screening facility to the locations where it will be delivered should be secured at all times. An organization's mail transport vehicles should be locked and sealed from the time they leave the screening facility until they are opened by an authorized individual at the delivery site.

6.4.3. Inbound Delivery

Items being delivered should not be left unattended. The intended recipient or an authorized individual should sign for accountable mail and packages.

6.5. Interoffice Mail

6.5.1. Interoffice Mail Pickup

Interoffice mail should be picked up from a secure area or a designated individual. Interoffice mail "drop sites" should not be accessible to the general public. Best practices include use of special accountable interoffice envelopes that can be tracked from sender to recipient using the mail center tracking system.

6.5.2. Interoffice Mail Screening

If the organization's risk assessment suggests that interoffice mail may be accessible to external personnel, mail center personnel should transport interoffice mail back to the mail screening facility for screening processing. If this is not possible due to distance or time limitations, mail center personnel should conduct an aggressive visual screening of interoffice mail while it is being sorted for delivery.

6.5.3. Interoffice Mail Sorting and Delivery

Interoffice mail should be treated like all other mail and delivered only to the intended recipient or an authorized individual.

6.6. Outbound Mail Processes

6.6.1. Pickup of Outbound Mail

Outbound mail should be picked up only from secure drop boxes or authorized individuals. Outbound mail should be kept secure at all times until it arrives at the mail center for further processing. Outbound "drop sites" should not be accessible to the general public.

6.6.2. Processing Outbound Mail

Outbound mail should be inspected for signs that it is suspicious. Mail and packages containing authorized, hazardous materials should be properly marked.

6.6.3. Transferring Outbound Mail to U.S. Postal Service or Couriers

Outbound mail should not be left unsecured on the loading dock or at other locations while awaiting pickup by the USPS or express couriers. Mail being transported to USPS

facilities should be secure at all times. Courier vehicles should not be left unattended or unlocked.

7. Suspicious Mail Incident Response Procedures

7.1. Initial Alert Procedures

Suspicious mail response procedures will vary by organization and will be based upon a combination of factors such as the type of item discovered, the location of the mail screening facility, internal facility configuration, the number of personnel in the facility, and specific organization emergency response protocols. There are, however, a number of common steps that should be taken:

- Remain calm. Alert others in the immediate area that you have identified a suspicious item. Ensure that the organization's security command center or local law enforcement and first responders are notified. If in a multi-tenant facility, building management should also be contacted.
- Do not attempt to move the suspicious item. Put the envelope or package on a stable surface if it is currently being carried or handled by mail center personnel.
- Do not sniff, touch, or taste any contents that may have spilled.
- Do not open the letter or package.
- Do not shake or empty the contents of a suspicious letter or package.
- Do not carry the letter or package or allow others to examine it.

7.2. Specific Substance Initial Response Procedures

7.2.1. Explosive Device

Immediately leave the mail screening area and initiate local evacuation procedures. If the mail or package is inside an X-ray scanner, leave it there. Do not use cell phones or radios within the immediate proximity of the suspicious package. Ensure that this prohibition is part of all mail screening training.

7.2.2. Chemical Substance

Leave the mail screening area. Close any doors to prevent others from entering the area. If possible, shut off any fans and the ventilation system of the local facility.

7.2.3. Biohazard Substance

Remain in the negative pressure mail screening environment until directed to leave by first responders/HAZMAT personnel. If there is no negative pressure system, shut off any fans and the ventilation system of the local facility and await arrival of first responders/HAZMAT personnel. Follow guidance from emergency response personnel.

7.2.4. Radiation or Nuclear Substance

Leave the immediate area where the radiation source appears to be located. Do not touch any source material or the packaging materials surrounding it.

7.2.5. Dangerous and Contraband Items

Report suspicious items to the mail center manager and/or security command center for further inspection. Notify local law enforcement as required.

7.2.6. Threatening Content

Report suspicious items with threatening content to the mail center manager.

7.3. Evacuation Procedures

Specific evacuation procedures will vary from site to site and must be coordinated in advance with organization management (to include property or facility managers, as appropriate), safety, and security personnel.

List all persons who were in the room or area when the suspicious letter or package was recognized or who may have handled the letter or package. Be prepared to provide the list to local public health authorities and law enforcement officials if requested.

When possible, write down the information regarding the appearance of the letter or package and photograph the item with a digital camera.

All suspicious items should be maintained as evidence as part of a criminal investigation until released by the appropriate law enforcement agency.

7.4. Internal Communication

All incidents involving suspicious mail and packages must be reported immediately to mail center management personnel and/or security, or local law enforcement and first responders. If the facility is a multi-tenant facility, building management should be contacted as well.

Within the mail center, managers should provide employees an initial briefing and regular updates during an ongoing incident. This is especially important when a suspicious item has necessitated the evacuation of the mail center.

As soon as possible, mail center personnel should be briefed on any required or recommended medical treatment in accordance with guidance provided by emergency medical personnel, first responders, and/or public health officials.

7.5. External Communication

The mail center manager must work directly with organization management and security personnel to outline procedures and protocols for initiating contact with external agencies including public health agencies.

In emergency situations, the mail center manager must be able to place calls directly to local first responder personnel. This matter must be addressed before a potential event takes place.

Designated security personnel within the organization or the mail center manager should serve as the primary point of contact with local law enforcement and first responders at the mail center during an ongoing incident.

Mail center personnel should never speak directly to the media about an ongoing incident. All external communications about an incident should be controlled by the organization's office of public affairs or similar office, in conjunction with the controlling Federal, State, or local authorities.

7.6. Post-Event Follow-Up

The mail center manager and the organization's security personnel should conduct a joint review of the incident and response actions with mail center employees and first responders following the incident.

Employees should be given an opportunity to speak with medical personnel, human resources representatives, environmental health and safety professionals, and other organization personnel as desired.

The mail center manager should also document and share information about the incident with other mail center managers as permitted by organization security protocols and general policies and procedures.

Suspicious mail will often lead to an investigation by local police, the U.S. Postal Inspection Service (USPIS), or the Federal Bureau of Investigation. Mail center personnel should be taught not to destroy evidence by vacuuming up white powder, shredding suspicious letters, disposing of dangerous packages, or similar activities.

7.7. Other Resources

Other resources and guidance on handling suspicious mail items can be found at the Centers for Disease Control and Prevention's Web site:

- Anthrax: http://emergency.cdc.gov/agent/anthrax/faq/mail.asp
- Alert Health Network: http://emergency.cdc.gov/documentsapp/anthrax/10312001/han51.asp

Appendix 1 provides additional sources and references.

8. Training Mail Screening Personnel

8.1. Suspicious Mail Characteristics

All mail center personnel should receive at a minimum annual training on identifying and handling suspicious mail and packages. It is important they understand the risks associated with the various threats that can be introduced through the mail, the characteristics of each, and the proper response to suspicious items.

Posters, videos, and online training packages are available to help mail center managers conduct training. Organization security personnel, USPIS, and commercial security contractors can provide suspicious mail training to mail center personnel.

8.2. Use of Screening Technology

In addition to suspicious mail identification and handling, all best practices mail screening facilities incorporate the use of a range of different screening technologies. Most technologies tend to be focused on identifying a specific type of potential hazard (biological, chemical, etc.), but a few, such as X-ray scanners and vapor trace detectors, have multi-substance capabilities.

In order for screening technologies to be effective, mail center screening personnel should be trained on their proper use and maintenance. This training is best accomplished by highly qualified trainers supplied by the equipment vendors themselves. No individual should be allowed to operate the screening equipment unless properly trained in its use. All screeners should also undergo refresher training on the equipment they use on at least an annual basis.

Mail center personnel should also receive training on the proper use of PPE. This includes fit testing, donning, removal, and disposal of the PPE.

8.3. Incident Response Procedures

All mail center personnel should receive training in suspicious mail response procedures. This training includes handling suspicious mail and packages, communications with other mail center personnel and the organization's management and security personnel, evacuation procedures, interacting with first responders and public health officials, and when necessary, follow-up decontamination procedures.

When conducting incident response training, it is important to involve all the first responder and public health organizations likely to be called to an incident at a mail screening facility. In doing so, mail center personnel, first responders, and public health officials become more comfortable working with one another. This training would also reduce the likelihood of an overreaction and a major disruption when an incident does occur. Mail center managers and the organization's security personnel should conduct regular rehearsals and evaluate the performance of the mail center during these rehearsals.

9. Conclusions

9.1. The Team Approach

A successful mail handling and screening program requires the integrated efforts of senior organization officials, mail center management, security officials, technology providers, and first responders. Working together, this team can ensure that an organization's mail is properly screened in an affordable and efficient manner. If an incident does occur, a well-functioning team will significantly reduce the adverse effects suspicious mail and packages have on the employees and operations of the organization. **Appendix 6**, ***Mail Screening Best Practices Checklist***, takes into consideration all the factors of a mail handling and screening process and provides evaluators a checklist of both best practices and minimum recommendations to help the team develop mail handling and screening processes appropriate for their facility.

9.2. Implementing Appropriate Technology and Procedures

The specific technologies that are required for each mail center vary from one organization to another based on the organization's respective risk assessment, security countermeasures, and characteristics of the mail center's daily operations.

Well-designed and consistently-executed screening processes are essential for both identifying suspicious items and limiting their impact once discovered. Any deviation from approved procedures can easily lead to suspicious mail or packages being missed or the inadvertent cross contamination of other items, equipment, facilities, or employees.

9.3. Adjusting Approaches as the Threat Changes

A certain level of threat is always present. Any piece of mail or a package may contain a dangerous substance or threatening content. Well-trained personnel with the appropriate tools can help mitigate that threat.

An organization's security personnel should constantly advise mail center personnel of any changes in the organization's threat level or any particular threats to individuals so that mail screeners can better perform their day-to-day screening activities and, if necessary, upgrade processes or technologies.

Appendix 1 – Government Mail Center Regulations and Related Documents

Federal Emergency Management Agency Risk Management Series

- Federal Emergency Management Agency (FEMA) 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*
- FEMA 430, *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*
- FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*

U.S. Postal Service Standards

- *Mailing Standards of the United States Postal Service*, Domestic Mail Manual
- *Mailing Standards of the United States Postal Service*, International Mail Manual

U.S. Postal Inspection Service Publications

- Publication 166, Guide to Mail Center Security, March 2008
- Poster 84, *Suspicious Mail*
- Notice 71, *Bombs by Mail*
- Publication 54, *Notice of Bomb Threat*

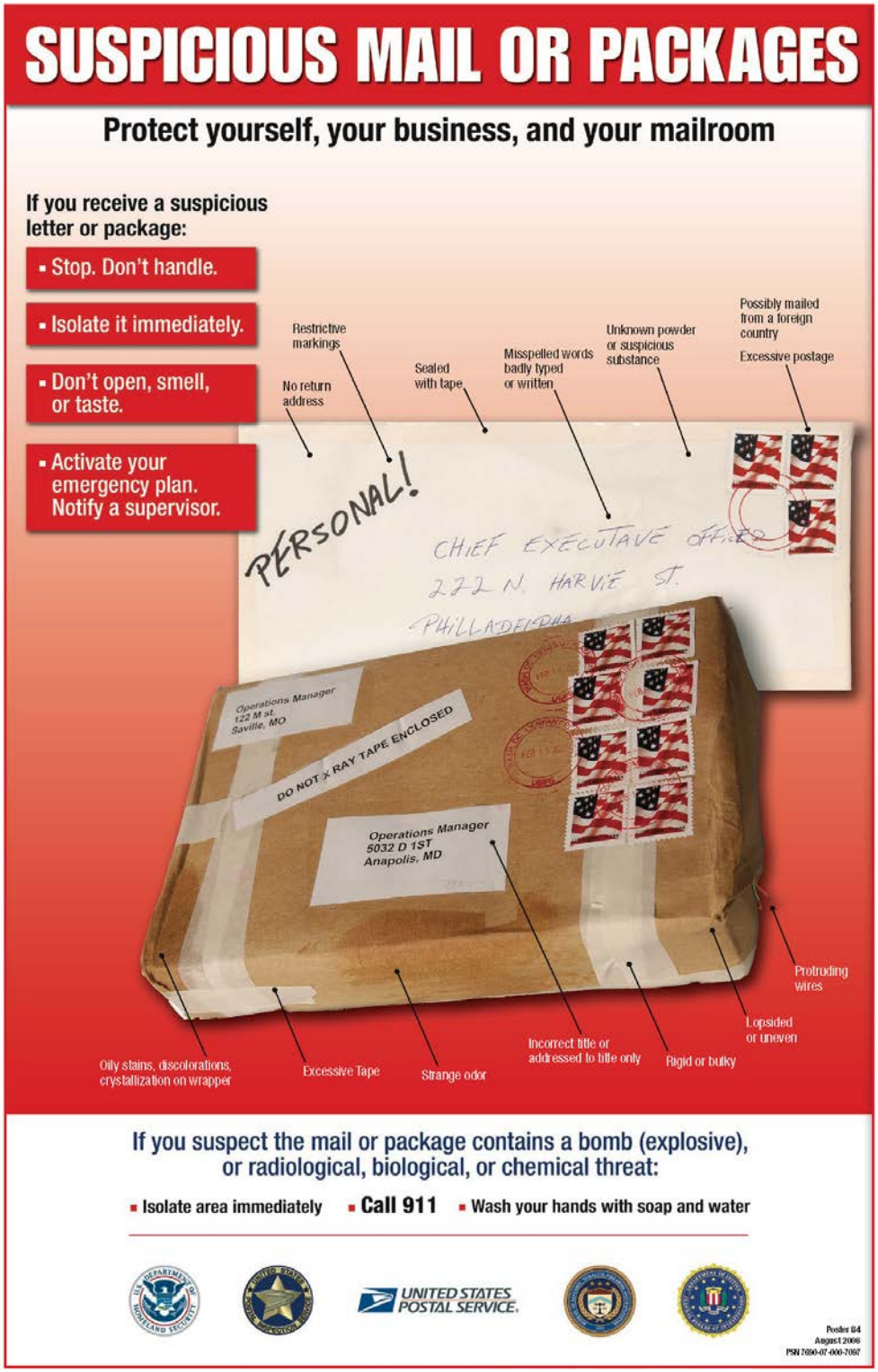
Regulations and Directives Utilized by Federal Agencies

- Federal Management Regulation 41 Code of Federal Regulations 102–192, Mail Management
- 30 CFR 233.11 USPIS Screening Authority
- National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, 2009
- Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements, dated February 2008
- Federal Continuity Directive 2, Federal Executive Branch Mission Essential Function and Primary Mission
- Federal Preparedness Circular 65, FEMA

Other Resources

- CDC Video: "Protecting Your Health" (for People Who Process, Sort, and Deliver the Mail), accessed at http://emergency.cdc.gov/agent/anthrax/training/mailhandlingvideo.asp

Appendix 2 – Suspicious Mail or Packages Poster



Appendix 3 – Mail Center Classification

1. Mail Center Size

1.1. The classification of mail centers as small, medium, or large depends on several factors, particularly when viewed from a mail screening and handling standpoint. The generally accepted view is that incoming mail is screened, as opposed to outgoing mail. The rationale for this approach is that outgoing mail poses a low probability of threat. The greatest threat, as demonstrated by actual events, comes from external sources who are attempting to use the mail stream as a vehicle for introduction of their particular threat to an area, organization, group, office, or individual. Therefore, when focusing on best practices and procedures for mail screening, it is incoming mail that is most important. The following factors should be considered when sizing mail centers for mail screening.

1.1.1. **Daily Mail Volume.** When considering volume, it is necessary to include the number of First Class letters and flats received, the number of packages, and the number of parcels or letter envelopes received from third-party couriers (e.g., FedEx, UPS, DHL, TNT, etc.). It should be noted in a wide range of operational areas there is general acceptance that "standard mail" (e.g., magazines, newspapers, and other types of mail that can be processed and delivered in "bulk" form) is exempt from the normal screening processes. "Standard mail" is considered to be from a known originator; therefore it is not considered a threat. Generally, this mail is not considered when establishing daily mail volume for screening processes. The daily throughput of a given mail center will have a significant impact on the design and operation of any proposed mail screening and handling procedures.

1.1.2. **Number of Customers.** This factor considers the number of recipients of mail being processed by a given mail center. The daily volume of mail per recipient often varies significantly. For example, some mail centers have 500–700 mail recipients, each receiving an average of 40–50 pieces of mail per day. Other mail centers have comparable customer populations, but recipient mail per day is consistently in the single digits. This is important, because it affects the level of effort required to meet established delivery standards to the target population. If mail screening procedures are to be added to the processing flow, their impact on level of effort and its timing also must be determined. The ability and/or willingness of the customer base to accept delays will have a direct impact on the type, amount, and nature of screening employed. In many cases, the number of mail center customers has resulted in the use of automated mail processing equipment to sort incoming mail. Automation should be considered when defining mail screening best practices for a specific location.

1.1.3. **Geographical Distribution.** Is the mail center centralized, or do satellite mail centers and/or distribution points exist? Satellite mail centers may require redundancy in any proposed mail screening and handling procedures. Although the type of incoming mail screening may be similar, such as X-ray scanning, the scale of the screening solution could vary between primary mail centers and satellite locations that support the same organization.

1.1.4. **Staffing Level.** The staffing level of a given mail center will be a direct result of the factors described above. The number of full-time and part-time personnel, their skill sets and levels of training, and the ability to augment the staff factor into the design and selection of mail screening and handling best practices.

2. **Classifying Your Mail Center**

2.1. Table A3-1 presents a basic strategy for the sizing of mail centers. The size classification is derived by quantifying a range for the factors described above, driven primarily by daily incoming mail volume. This approach provides a basic level of classification which can then be integrated with other elements to arrive at the recommended type of facility and screening technologies to be employed in a given situation.

TABLE A3-1

MAIL CENTER CLASSIFICATION

	Daily Mail Volume	Staff	Number of Satellites
Class A – Small	< 1000	< 10	N/A
Class B – Medium	1000 -9,999	10 - 49	< 3
Class C – Large	10,000+	50+	3 or more

2.2. When considering a standard set of best practices and mail screening and handling procedures, one must recognize that no single solution will fit all mail centers. In addition, when looking at the myriad of technological applications that could be brought to bear, the number of potential solutions expands rapidly. Any solution presented will be impacted by the factors mentioned above, as well as additional factors and subjective judgments. For example, if CBRNE screening is required, the nature, type, and number of CBRNE technologies may vary by organization. Today's commercial off-the-shelf (COTS) technologies for biological detection range from simple manual test kits to fully automated sensor and evaluation suites. Capabilities for explosives detection range from the use of canines, to manually swabbed packages, to a host of fully automated solutions. In developing a best practices approach, a range of technologies may be required to ensure that the unique attributes of individual mail centers are fully accommodated.

Appendix 4 – Mail Center Assessment Worksheet

ADMINISTRATIVE INFORMATION	REQUIREMENT	STATUS (Y, N, NA)	DETAILS
Date Completed			
Completed By			
Organization			
Headquarters Address			
Office Manager	Name: Phone: E-Mail:		
Mail Center Manager	Name: Phone: E-mail:		
Buildings Served	Building Location	# of Floors	# of Mailstops
1.			
2.			
3.			
4.			

LOCATION and FUNCTION	REQUIREMENT	STATUS (Y, N, NA)	DETAILS
Facility Level of Risk	Has a risk assessment been completed on the facility? If so, what level of risk does the facility have?		
Office Location	Is the facility located in an urban area?		
	Is the facility located in a high-crime area?		
	Is the facility located in a shared office building?		
	Is this a high visibility government office location?		
	Are any other high-visibility or high-risk organizations in the building?		
Function	Is this a headquarters location?		
	Are there regular visitors to this location?		
	Are there senior executives who receive mail at this location?		
General Office Security	Does the office building have its own external security system?		
	Does the office building have an access control system?		
	Is there a sign-in process for visitors to the office building?		
	Is there restricted access to the government office itself?		
General Mail Security	Are mail and packages delivered to the office building?		
	Do the major international carriers (FedEx, UPS, DHL, TNT, etc.) deliver items directly to the building?		
	Do other local couriers deliver packages directly to the building?		
	Is there a centralized mail distribution point for all tenants of the building?		
	If it is a multi-client building, are any screening services (X-ray, etc.) provided by the management of the office building?		
	Does the government organization have mail and packages delivered directly to its office location?		
	Have there been previous suspicious mail incidents at the facility?		

MAIL CENTER ASSESSMENT	REQUIREMENT	STATUS (Y, N, NA)	DETAILS
Mail Center Location	Is the mail center located in an offsite facility?		
	Is the mail center located in the main office building?		
	Does the mail center have doors that restrict access to non-mail center employees?		
Mail Center Security	Are there CCTV cameras overlooking the main access points to the mail center (employee entrance, customer entrance, loading dock)?		
	Does the mail center have an access control system?		
	Are the access doors to the mail center locked during the day?		
	Are windows in the mail center secured throughout the day?		
	Is there a designated customer service area separate from the mail processing area?		
	Are visitors to the mail center allowed access to the facility?		
	Is there a sign-in list for authorized visitors to the mail center?		
Other	Are there any other mail center facility-specific security issues?		

MAIL CENTER EMPLOYEES	REQUIREMENT	STATUS (Y, N, NA)	DETAILS
Pre-Screening	Are employees pre-screened during the hiring process to identify potential risks?		
Temporary Employees	Does the mail center use any temporary employees to process or deliver mail?		
Employee Identification	Do employees wear visible picture ID badges at all times?		
Employee Training	Are employees trained on proper mail center security procedures?		
	Are employees trained on proper suspicious mail handling procedures?		
	Are employees trained on proper mail center evacuation procedures?		
Other	Are there any other mail center employee-specific security issues?		

INBOUND MAIL/PKG SCREENING	REQUIREMENT	STATUS (Y, N, NA)	DETAILS
Identification	Are suspicious mail identification wall posters displayed at all screening and mail sorting stations?		
	Are employees trained on the identification of suspicious mail?		
Handling	Does the mail center have well-documented suspicious mail handling procedures?		
	Are the employees familiar with the suspicious mail handling procedures?		
	Is emergency contact information for security, police, fire, and medical personnel displayed near mail screening and sorting locations?		
	Are screened items kept segregated from non-screened items?		
X-Ray Screening	Is the mail center conducting X-ray screening of incoming mail and packages?		
	Are the employees conducting X-ray screening properly trained and certified?		
	Has the X-ray equipment been inspected in accordance with the required schedule for the area?		
Personal Protective Equipment	Are gloves and masks available for individuals to use during the screening process?		
Containment Systems	Is the mail center facility protected by a negative pressure air room?		
	Are there temporary storage systems for suspicious mail and packages?		

INBOUND MAIL/PKG RECEIVING	REQUIREMENT	STATUS (Y, N, NA)	DETAILS
General	Are there documented mail and package handling procedures?		
	Are employees trained on proper mail and package handling procedures?		
	Is there a list of approved couriers authorized to pick up and deliver mail and packages to the mail center?		
Mail	Is mail picked up or received only by employees specifically authorized to do so?		
	Is accountable mail requiring signature or other specialized handling procedures properly processed by an employee authorized to do so?		
	Is mail stored in a secure area while waiting further processing?		
Packages	Are packages left unsecured on the loading dock or in other areas outside the mail center?		
	Are packages being delivered signed for by an authorized employee of the mail center?		
	Does the mail center maintain a log (paper or electronic) of the packages it receives?		
	Are packages stored in a secure area while waiting further processing?		

MAIL/PKG DELIVERY OPERATIONS	REQUIREMENT	STATUS (Y, N, NA)	DETAILS
Sorting	Do mail center personnel maintain proper chain-of-custody control over mail and packages during the sorting process?		
	Are mail and packages properly signed out to courier services?		
Couriers	Does the mail center use third-party courier services to transport mail from the sorting facility to delivery locations?		
	Does the mail center use mail center employees to transport mail from the sorting facility to delivery locations?		
	Do personnel wear proper identification when performing courier services?		
	Are courier vehicles kept locked when transporting mail and packages?		
	Do couriers maintain positive control over mail and packages at all times?		
	Do couriers maintain proper chain-of-custody documentation for accountable mail and packages?		
Final Delivery	Do mail center personnel perform final delivery of mail and packages?		
	Do mail center personnel deliver mail to centralized mail box locations?		
	Do mail center personnel deliver mail and packages to individual recipients?		
	Do final recipients properly sign for accountable mail and packages?		

OUTBOUND MAIL/PKG PROCESSING	REQUIREMENT	STATUS (Y, N, NA)	DETAILS
Interoffice Mail	Do mail center personnel pick up, sort, and deliver interoffice mail?		
	Is interoffice mail sorted at the central mail center facility?		
Outbound Mail and Packages	Do mail center personnel pick up outbound mail and packages from centralized locations within the office building?		
	Is outbound mail transported to the post office by mail center personnel?		
Postage Meter Security	Are adequate control measures in place to avoid misuse of postage meters, stamps, and other payment systems?		

MAIL VOLUME	DAILY VOLUME OF PIECES		
Inbound Mail			
Inbound Flats			
Inbound Packages			
Outbound Mail			
Outbound Flats			
Outbound Packages			

Appendix 5 – Mail Screening Requirements

MAIL CENTER SCREENING REQUIREMENTS RATING

1. Evaluation Criteria

1.1. Determining the proper mail screening approach requires a combined evaluation that includes the overall level of risk, the mail center classification, the current mail processes assessment, and any additional factors that security and management personnel deem significant.

1.2. The table below provides one way to integrate and evaluate all of these factors. The mail screening requirements rating provides an indication of the recommended Best Practices and Minimum Recommended mail screening facility and technology approaches for a particular organization and mail center location. Table A5-1, "Mail Screening Requirements Rating," and Table A5-2, "Mail Screening Recommendations Best Practices," provide an overview of each facility, technology, and process approach.

TABLE A5-1

MAIL SCREENING REQUIREMENTS RATING

Facility Risk Rating	Mail Center Class A (Small)	Mail Center Class B (Medium)	Mail Center Class C (Large)
1	1A	1B	
2	2A	2B	
3	3A	3B	3C

2. Mail Screening Approaches. Table A5-2, "Mail Screening Best Practices," provides a starting point for mail center managers and organization security personnel to use to begin to build out their own mail screening operation. It is a baseline set of screening processes founded on best practices currently in use in government and commercial facilities around the world. Specific or unique situations may require significant upgrades to the recommended processes, or they may permit reductions in the level of screening recommended for a site, based on its risk rating and its mail center classification.

TABLE A5-2

MAIL SCREENING BEST PRACTICES

FACILITY TYPE	VISUAL SCREENING	DANGEROUS CONTRABAND	HOAX SCREENING	EXPLOSIVE SCREENING	CHEMICAL SCREENING	BIOLOGICAL SCREENING	RAD/NUKE SCREENING	CONTENT SCREENING
1A	X	X	X					
1B	X	X	X					
2A	X	X	X	X				
2B	X	X	X	X				
3A	X	X	X	X	X	X	X	X
3B	X	X	X	X	X	X	X	X
3C	X	X	X	X	X	X	X	X

Appendix 6 – Mail Screening Best Practices Checklist

1.0 FACILITY DESIGN	BEST PRACTICE	MINIMUM RECOMMENDED
1.1 Location	1. Mail center is located in an offsite facility outside the main primary office or campus location. 2. Offsite facility is not located in a high-traffic or high-visibility area.	1. Mail center is located in a facility or specific area controlled by the organization. 2. Mail center is in a designated room away from the primary office activities.
1.2 Security	1. Mail center has a separate CCTV security system that is monitored 24/7. 2. Facility is enclosed by security fence. 3. Access to secure area is monitored by a guard. 4. The visitor control system issues temporary badges that include a picture.	1. Mail center itself has a separate access control system. 2. Only mail center personnel are allowed access to the mail screening and handling areas.
1.3 Loading Dock	1. Access to loading dock is restricted to mail center personnel and approved delivery vehicles. 2. Loading dock has inbound and outbound doors separated by a sufficient distance to avoid cross contamination.	1. Access to loading dock is restricted to individuals and vehicles inside the campus or building security perimeter. 2. Access to loading dock can be closed or restricted when not in use.
1.4 Biohazard Containment	1. Mail center has a negative pressure system that begins at the loading dock and includes dedicated screening and temporary quarantine areas. 2. The negative pressure mail center has a separate HVAC system.	1. Mail center personnel have the ability to shut off flow to the HVAC system that supports the mail center. 2. Access to mail center does not require personnel to carry unscreened items through core office areas.

2.0 TRACKING & ACCOUNTABILITY	BEST PRACTICE	MINIMUM RECOMMENDED
2.1 USPS Mail	1. Inbound mail is tracked throughout the initial screening process at the tub or tray level using internally-generated barcodes.	1. Inbound mail is tracked, processed, segregated, and delivered on a daily basis.
2.2 USPS Packages	1. All packages are barcoded and tracked from receipt, throughout the screening process, and until delivered to the recipient or a designated representative. 2. Undeliverable packages are secured in the mail center in a separate area until delivery can be made.	1. All packages are barcoded and tracked from receipt, throughout the screening process, and until delivered to the recipient or a designated representative. 2. Undeliverable packages are secured in the mail center in a separate area until delivery can be made.
2.3 Express Couriers	1. All packages are tracked using the dedicated courier tracking number/barcode from receipt, throughout the screening process, and until delivered to the recipient or a designated representative. 2. Undeliverable packages are secured in the mail center in a separate area until delivery can be made. 3. All items are screened using an X-ray scanner at an offsite facility.	1. All packages are tracked using the dedicated courier tracking number/barcode from receipt, throughout the screening process, and until delivered to the recipient or a designated representative. 2. Undeliverable packages are secured in the mail center in a separate area until delivery can be made.
2.4 Supplies and Other Items	1. Mail center personnel must confirm all items against the delivery manifest. 2. Items must be entered into the tracking and/or procurement system. 3. All items must be screened and stored in a secure facility until delivered or consumed.	1. Mail center personnel must confirm all items against the delivery manifest. 2. Items must be entered into the tracking and/or procurement system. 3. All items must be screened and stored in a secure facility until delivered or consumed.

3.0 PERSONAL PROTECTIVE EQUIPMENT	BEST PRACTICE	MINIMUM RECOMMENDED
3.1 Clothing	1. PPE includes a Tyvek outer garment, hood, gloves, boots, and a minimum N95 respirator (FFP Mask). 2. A smock may be substituted for a Tyvek suit for individuals not involved in biohazard screening.	1. PPE includes wear of smock, gloves, and N95 mask (FFP Mask). 2. PPE is made available to all personnel.
3.2 Wear	1. Mail screeners dress in PPE prior to entering the screening facility and remove it before leaving the negative pressure environment.	1. Smocks are left in the mail center when not in use. 2. If worn, gloves and masks are donned prior to screening and sorting mail.
3.3 Disposal	1. PPE is enclosed in sealed bags and remains in the negative pressure environment until the daily mail has tested clean. 2. PPE is disposed of on a daily basis.	1. Smocks are left in the mail center when not in use. 2. Other PPE items are disposed of on a daily basis.

4.0 SCREENING EQUIPMENT & PROCESSES	BEST PRACTICE	MINIMUM RECOMMENDED
4.1 Chemical	1. Mail center has an air sampling system with automatic alert capability. 2. Sensors are located at the loading dock and inside mail screening facilities. 3. Chemical sensor system is monitored by the mail center security operations.	1. Mail center personnel visibly inspect mail and packages for the presence of liquids. 2. Mail and packages with obvious contaminants are set aside for further inspection by security or HAZMAT personnel.
4.2 Biological	1. Mail and packages are screened inside a negative pressure environment. 2. Items are visually inspected for signs they may contain a biological hazard. 3. Air samples are collected from the outside and inside of all mail and packages. 4. Samples are collected from mail tubs and trays. 5. Collection device filters are tested for biological hazards by a CDC-approved laboratory. 6. Mail and packages are quarantined until negative test results are obtained.	1. Items are visually inspected for signs they may contain a biological hazard. 2. Suspicious items are segregated until released by mail center supervisors, security personnel, or first responders. 3. No mail is released for delivery until suspicious mail has been cleared.
4.3 Radiological/ Nuclear	1. Inbound delivery vehicles are screened for radiation using pedestal or wall mounted sensors. 2. Radiation sensors are integrated into the central security system and monitored 24/7. 3. Mail center personnel wear radiation pagers while screening and processing mail. 4. If radiation is detected in an item, mail center personnel leave the immediate area.	1. Mail center personnel visually screen items for signs that a radiation producing device is enclosed. 2. Mail center personnel wear radiation pagers while screening and processing mail.
4.4 Explosives	1. Vehicles and mail/packages are screened by explosive detection canine teams before being allowed inside the screening facility. 2. Items are visually inspected for signs they may contain an explosive device. 3. Mail is screened at the batch level (tubs or trays) using an X-ray scanner. 4. Packages are screened individually with an X-ray scanner. 5. Mail center personnel conducting scanning operations are networked with remote security personnel for technical support as necessary. 6. Suspicious items are segregated until released by mail center supervisors, security personnel, or first responders.	1. Mail center personnel visually screen items for signs that an explosive device is enclosed. 2. Suspicious items are segregated until released by mail center supervisors, security personnel, or first responders.

4.0 SCREENING EQUIPMENT & PROCESSES	BEST PRACTICE	MINIMUM RECOMMENDED
4.5 Contraband and Dangerous Items (continued)	1. Items are visually inspected for signs they may contain dangerous or contraband items. 2. Mail is screened at the batch level (tubs or trays) using an X-ray scanner. 3. Packages are screened individually with an X-ray scanner. 4. Mail center personnel conducting scanning operations are networked with remote security personnel for technical support as necessary. 5. Suspicious items are segregated until released by mail center supervisors, security personnel, or first responders.	1. Mail center personnel visually screen items for signs that they may contain dangerous or contraband items. 2. Suspicious items are segregated until released by mail center supervisors, security personnel, or first responders.

5.0 SUSPICIOUS MAIL INCIDENT RESPONSE	BEST PRACTICE	MINIMUM RECOMMENDED
5.1 Incident Response Plan	1. Mail center has a formal emergency response plan. 2. Response plan is reviewed and updated at least quarterly. 3. Copies of the response plan are maintained by the mail center, security personnel, local managers, and when appropriate, first responders and public health officials.	1. Mail center has a formal emergency response plan. 2. Response plan is reviewed and updated at least quarterly. 3. Copies of the response plan are maintained by the mail center, security personnel, local managers, and when appropriate, first responders and public health officials.
5.2 Training	1. Mail center personnel have received, read, and been briefed on the suspicious mail and emergency response plan. 2. Mail center personnel and related organizations have conducted a tabletop exercise of the emergency response plan. 3. Mail center personnel and related internal organizations have completed a live exercise of the emergency response plan. 4. Local first responders and, as appropriate, public health officials have conducted a site visit of the mail center location and reviewed emergency response procedures.	1. Mail center personnel have received, read, and been briefed on the suspicious mail and emergency response plan. 2. Mail center personnel and related organizations to include public health officials have conducted a tabletop exercise of the emergency response plan.

6.0 TRAINING	BEST PRACTICE	MINIMUM RECOMMENDED
6.1 Suspicious Mail and Package Characteristics	1. All mail center personnel have received initial training on identification and handling of suspicious mail and packages prior to beginning work at the mail center. 2. All mail center personnel have received annual training on identifying suspicious items.	1. All mail center personnel have received initial training on identification and handling of suspicious mail and packages prior to beginning work at the mail center. 2. All mail center personnel have received annual training on identifying suspicious mail and packages.
6.2 Screening Technology and Procedures	1. Mail center personnel have received initial training on specialized mail screening equipment from the vendor. 2. Mail center personnel have received annual training from the vendor or local supervisors.	1. Mail center personnel have received initial training on specialized mail screening equipment from the vendor. 2. Mail center personnel have received annual training from the vendor or local supervisors.

Acknowledgements

The following organizations participated in, contributed to, and/or were instrumental in the creation of this document:

- United States Department of State
- United States Department of Defense
- United States Department of Homeland Security
- Interagency Security Committee
- United States Postal Service
- United States Postal Inspection Service
- Centers for Disease Control and Prevention
- Pitney Bowes Government Solutions
- Serco