RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

How to Implement a Mail Security Program

Cody Martin
Director Mail Security Services
RaySecur Inc.

Objectives of this Course

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

KEY OBJECTIVES

- Design and implement a mailroom security program
- Develop standardized operating procedures

Disclaimer: RAYSECUR is a consultant and facilitator of this process. It is the client's responsibility to implement a mail security program. RAYSECUR is not responsible for any errors or omissions.

What is a mail security program?

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

- A mailroom security program is a component of physical security used to prevent or minimize the introduction of threats via the mail stream.

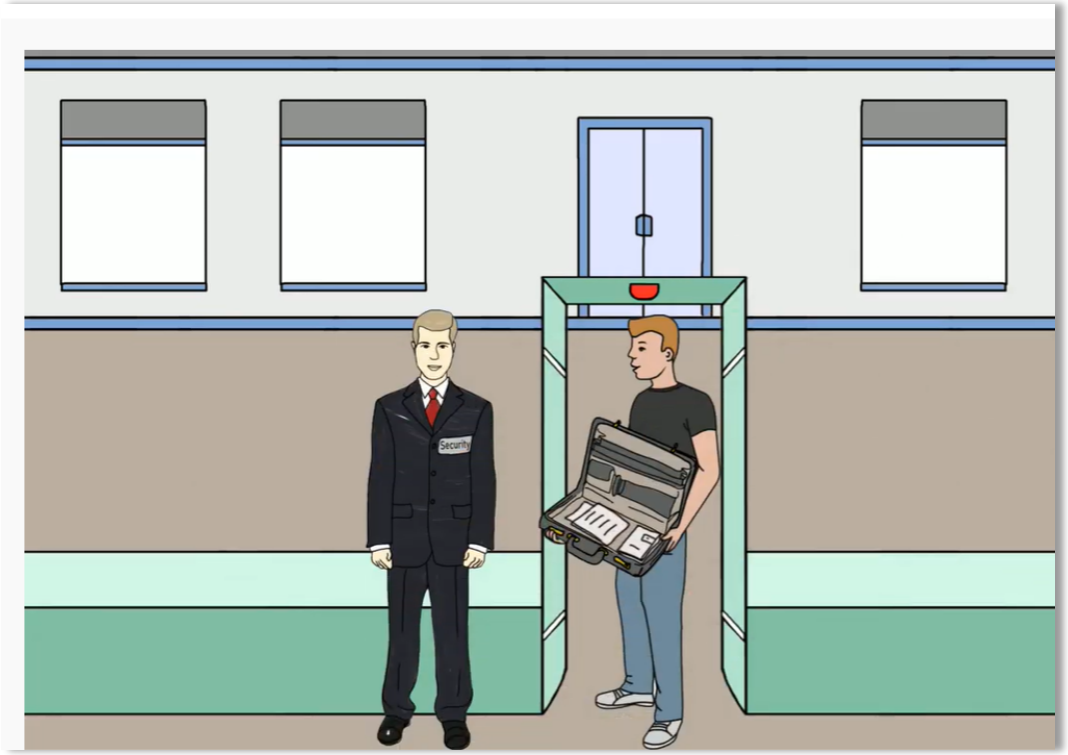
- It provides a systematic approach to protect people and assets from the point of acceptance through the final delivery or destruction of the mail piece.

- When effectively implemented, it closes a gap often found in physical security programs.

Why is a mail security program important?

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

The front door is well-protected.



The back door is wide open…

Most Major Companies Affected

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

1 in 3 **Fortune 500** Companies receive at least one mail threat per year*.

2019 Industry Mail Security Survey

- **34%** of surveyed companies had at least one mail threat detected in the previous year
- **16%** had more than 3 threats in that same time period
- Threatening letters **doubled**
- Drugs and illegal substances **quadrupled**

https://www.uspis.gov/wp-content/uploads/2020/02/FY-2019-annual-report-508-web.pdf

*Government Technology & Services Coalition, "Third of Companies Got Mail Threats in Past Year While Biological Screening Doubled," May 19, 2019

Many Threats Go Unreported

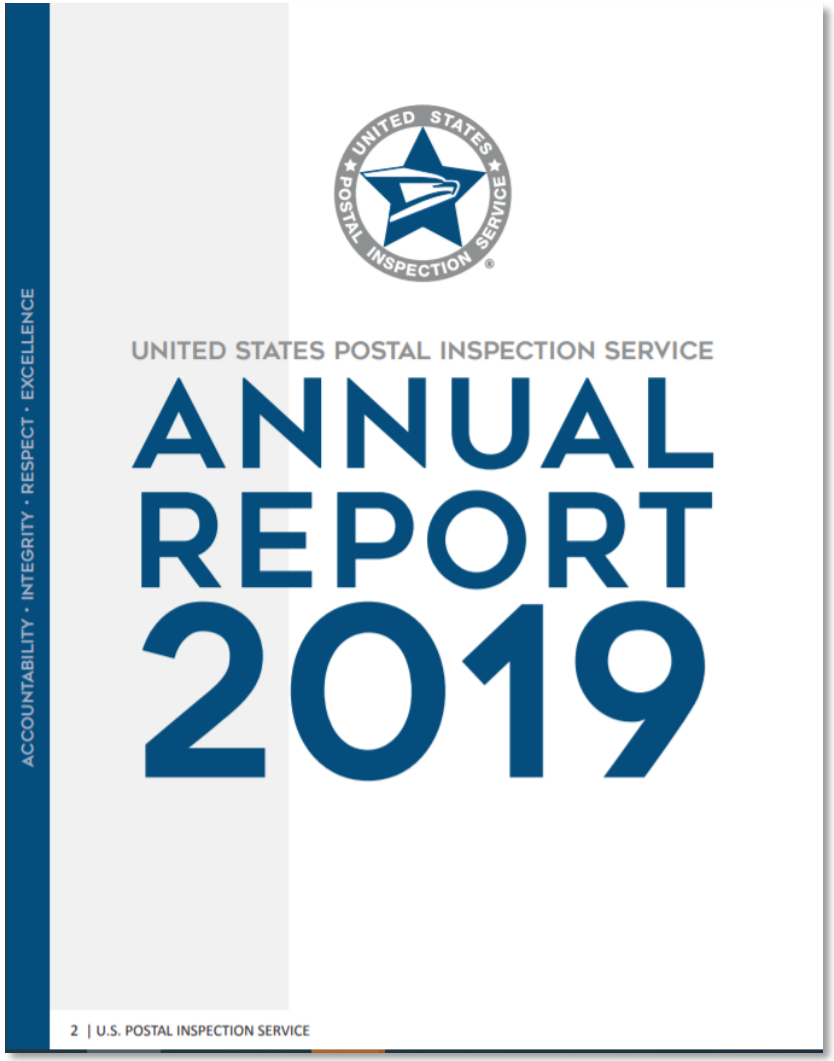
RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

USPIS 2019 Annual Report

- Dangerous Mail Investigations (DMI) Unit
- 400 specially-trained inspectors
- 3,289 suspicious incidents (powders, liquids)
- 125,000 suspicious mail items subject to forensics exam

US Bomb Data Center

- 7,404 suspicious packages in 2018
- 2,261 incidents involving letters or parcels



https://www.uspis.gov/wp-content/uploads/2020/02/FY-2019-annual-report-508-web.pdf

Five Pillars of Mail Security

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

1. Leadership and Execution

- Internal security team
- External support resources

2. Standard Process

- Best practices
- Effective and actionable
- Disciplined

3. Education and Intelligence

- Reinforce SOPs
- Continually updated

4. Advanced Screening

- Right tools for the job
- Simple and easy to use

5. Response Plan

- Internal procedures
- External coordination

FIVE PILLARS – 1. People

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

Internal Teams

- Executive Support
- Global Security
- Facilities Management
  - Outsourced Service Providers
- Mail Handlers

External Teams

- Subject Matter Experts
- On-Demand Support
- Incident Response

FIVE PILLARS – 2. Procedures

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

- Global Mailroom Security Policy Statement
- Global Mailroom Mail Screening Process
- SOP-001: Mail Security Screening
- SOP-002: Suspicious Item Screening
- SOP-003: Emergency Response

Broad Corporate Guidelines to Define Global Mail Screening Standards

- Appendix: Site-Specific Information
  - Site #1
  - Site #2
  - Site #...
  - Site #...
  - Site #...

Site-Specific Resources:
- Process Materials: Poster 84, RS Process Flow
- Trainings: LMS, On-Site Training, Quarterly Webinar
- Equipment: Screening Mat, MailSecur Scanner
- Support: EODSecur 24/7/365 Support

Site-Specific Information

Flexibility to Adapt as COVID Situation Evolves

FIVE PILLARS – 3. Training

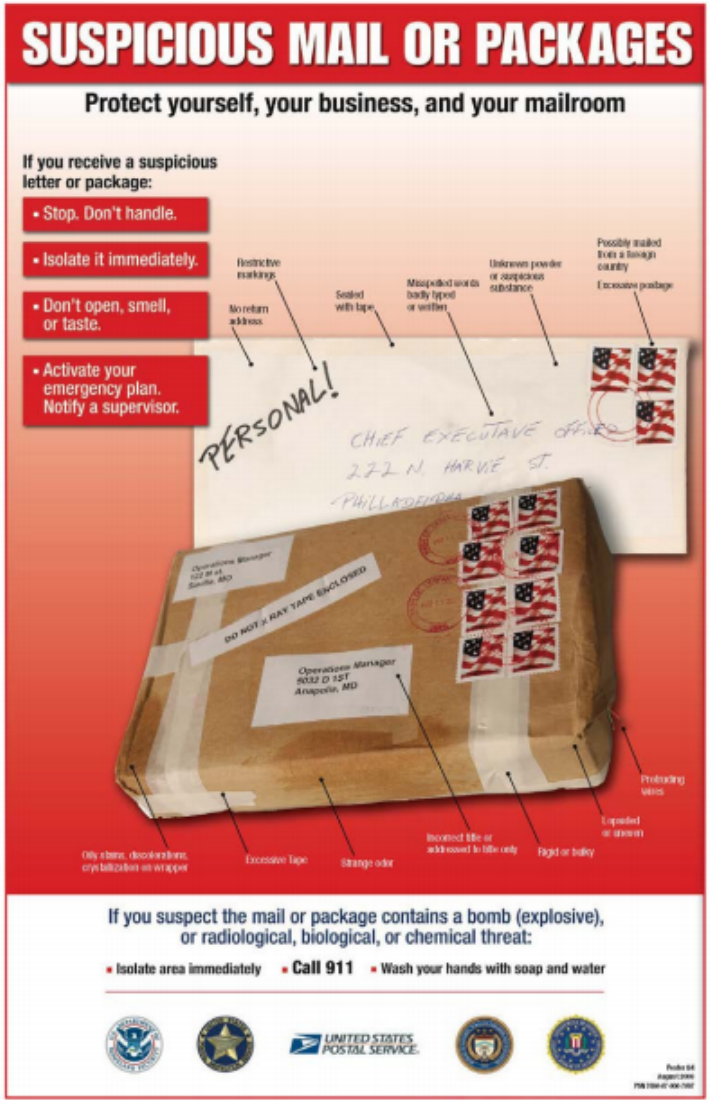
RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

Training – Internalize SOPs

- Spans all layers of the organization
- Objective is to educate
- Incorporate training aids into everyday routines
- Continually update

Certification

- Confirm required level of understanding
- Require periodic recertification for key employees



FIVE PILLARS – 4. Technology

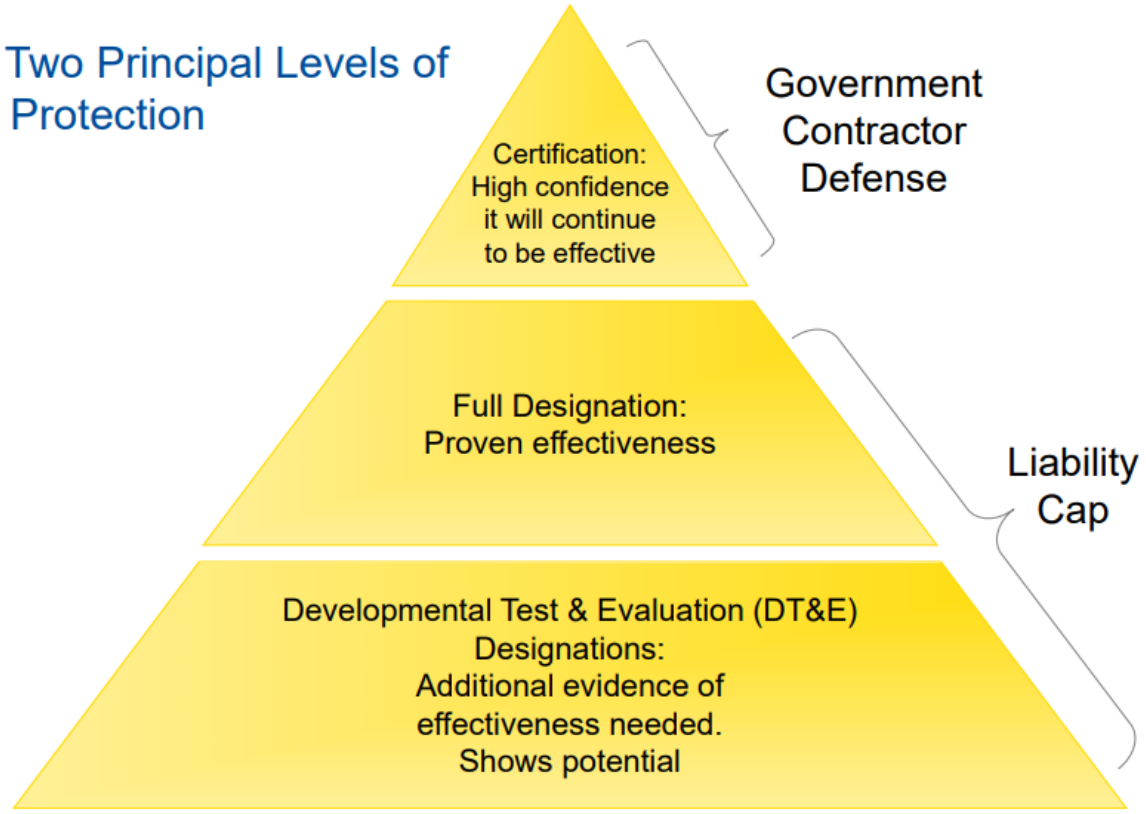
RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

Adhere to validated standards.

Homeland Security
Science and Technology

Essential Concepts

1. Two Principal Levels of Protection



https://www.safetyact.gov/externalRes/refDoc/refGroup/8/SAFETY%20Act%20101%20Briefing.pdf

FIVE PILLARS – 5. Response Plans

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

USPIS Response

- Within 4 hours
- Unmarked SUV
- Dangerous Mail Specialist
- Screen up Through Identification
- Resolve or Escalate

Local (911) Response

- More Immediate Response Times
- Numerous Personnel
- Evacuations
- Very Similar Mail Screening Equipment

Overview of Mail Security Program

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

Assessing Risk

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

Guidelines are based on:

- Site risk profile
- Physical layout of the facility
- Other unique requirements.

Site -specific considerations:

- Internal mail transport routes
- Mailroom location and access
- Available technology

KEY RISK FACTORS	
• Public Posture	• Symbolism
• Location	• Population
• Intangibles	• Volume of Mail

Mail Transport Route

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

Utilize the shortest route to minimize exposure.

Reception

Sorting and scanning

Delivery

Mailroom Location and Access

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

Evaluate the location within the building and access control.

Questions to Ask:

- If a dangerous item is identified within the mailroom, what kind of impact will it have on building operations?
- Are critical assets or personnel located immediately near or above the mailroom?
- If a mail threat is discovered what type of concern does that raise?

Review Current Procedures

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

1. Centralize all mail handling.

   A fragmented footprint not only allows for multiple entry points but also creates an environment where standards often vary from place to place.

2. Locate the mail center in a stand-alone location, if possible.
   - Maintain appropriate standoff from the main facility.
   - If it is not possible, provisions need to be made to accommodate these scenarios.

3. Assign a mailroom coordinator.

Additional Considerations for Key Processes

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

- How is the mail processed?
- Is a visual inspection occurring at the area where mail is received?
- Is the mail then introduced to a more thorough visual and tactile inspection in the mailroom?
- Is technology available for more advanced screening?
- What are the roles of mailroom personnel?
- Do personnel know the key indicators of a suspicious mail piece?
- Do personnel know what emergency procedures to take to mitigate the various types of incidents they may be exposed to?

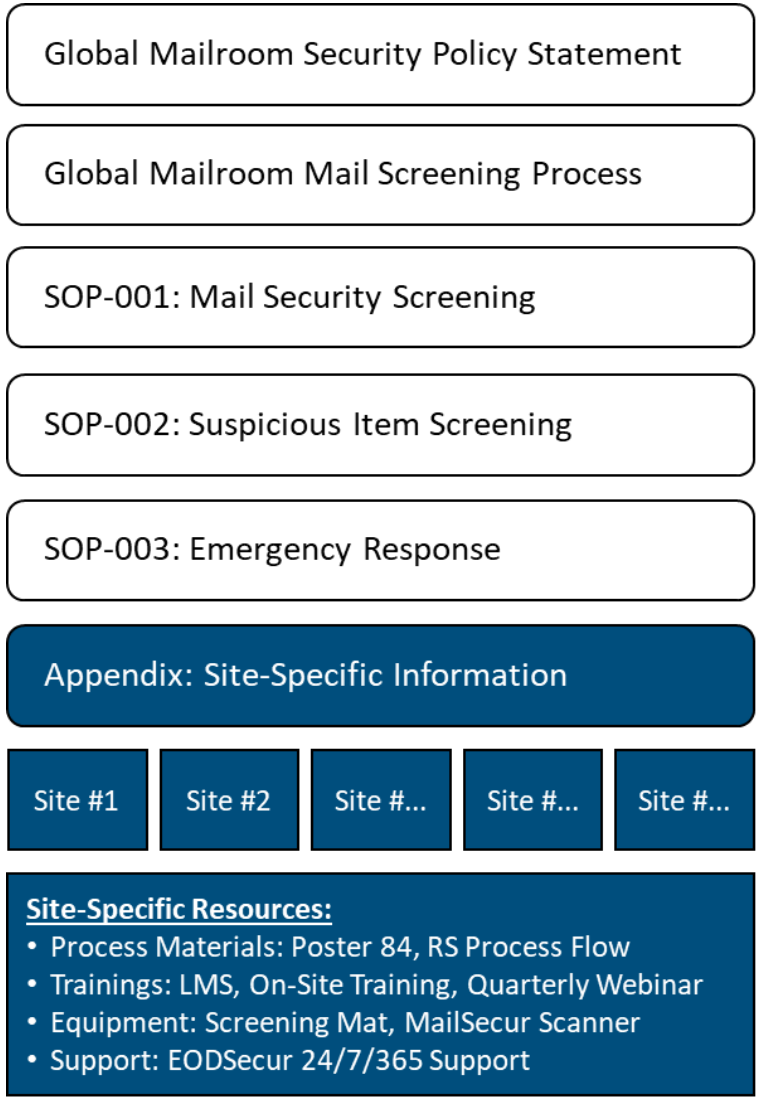
Standard Operating Procedures (SOPs)

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

SOPs define roles and responsibilities within the mail security program for all personnel.

SOP's should include the following:

1. Global Mailroom Security Policy Statement
2. Global Mailroom Mail Screening Process
3. Mail Security Screening Procedure
4. Suspicious Item Screening Procedure
5. Emergency Response Procedure



Importance of Well-Trained Personnel

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

- Well trained personnel are key to mitigating mail-borne threats.
  - They are also able to more easily recognize trusted senders to expedite screening and have a better understanding of emergency procedures.
  - They understand what is “normal” for your mail.

- All mail handlers should be trained in the fundamentals of mail security covering the types of mail threats, identification of suspicious items, and the basics of visual and tactile inspection.

- Operators of mail security screening technology should be trained in all aspects of their screening technology operation and threat detection including annual recertification.

Securing your Facility

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

- Key pieces of an enterprise mail screening program:
  - ✓ Risk analysis
  - ✓ Reviewed current policies and procedures
  - ✓ Integrated standardized operating procedures
  - ✓ Trained personnel
- Continuing education, training, and certification.
- Develop a security-first mindset that works from the top down.

Mail Security Guidelines

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

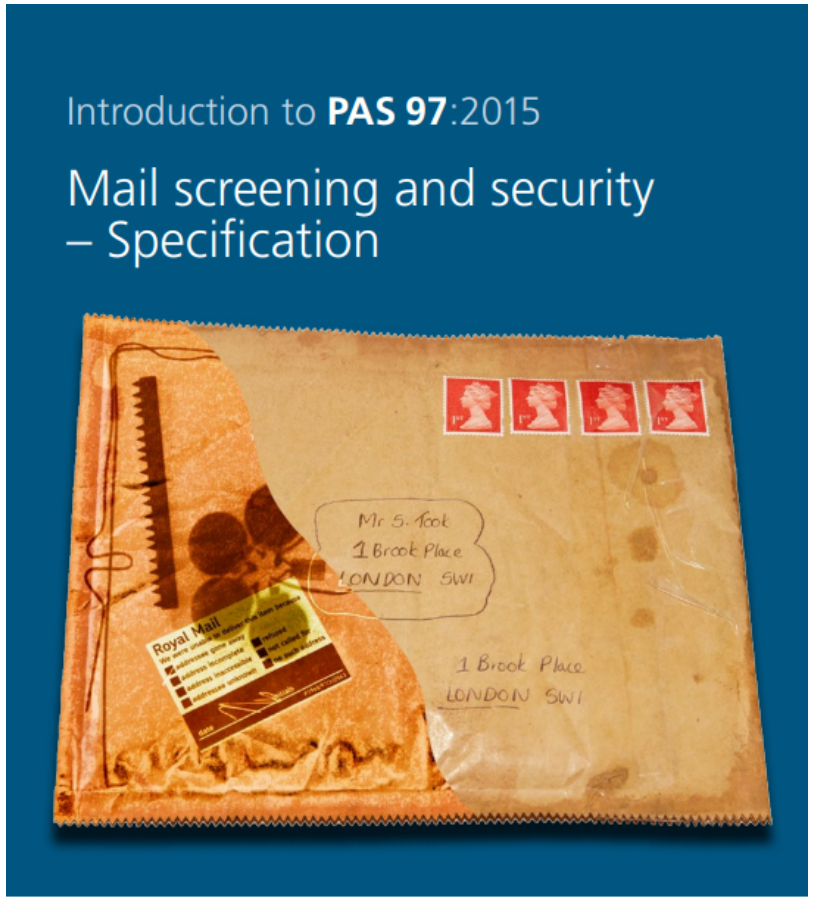
Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors

September 27, 2012

1st Edition

Homeland Security

Interagency Security Committee



CPNI
Centre for the Protection of National Infrastructure

bsi.

U.S. DHS Guidelines

https://www.cisa.gov/sites/default/files/publications/isc-mail-handling-screening-nonfouo-sept-2012-508.pdf

UK CPNI Guidelines

https://www.cpni.gov.uk/system/files/documents/3f/b7/Introduction-to-PAS-97-2015.pdf

Mail Security Classification and Requirements

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

1. Classification of the Mail Center

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. Facility Risk Rating

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

3. Mail Screening Requirements

TABLE A5-2

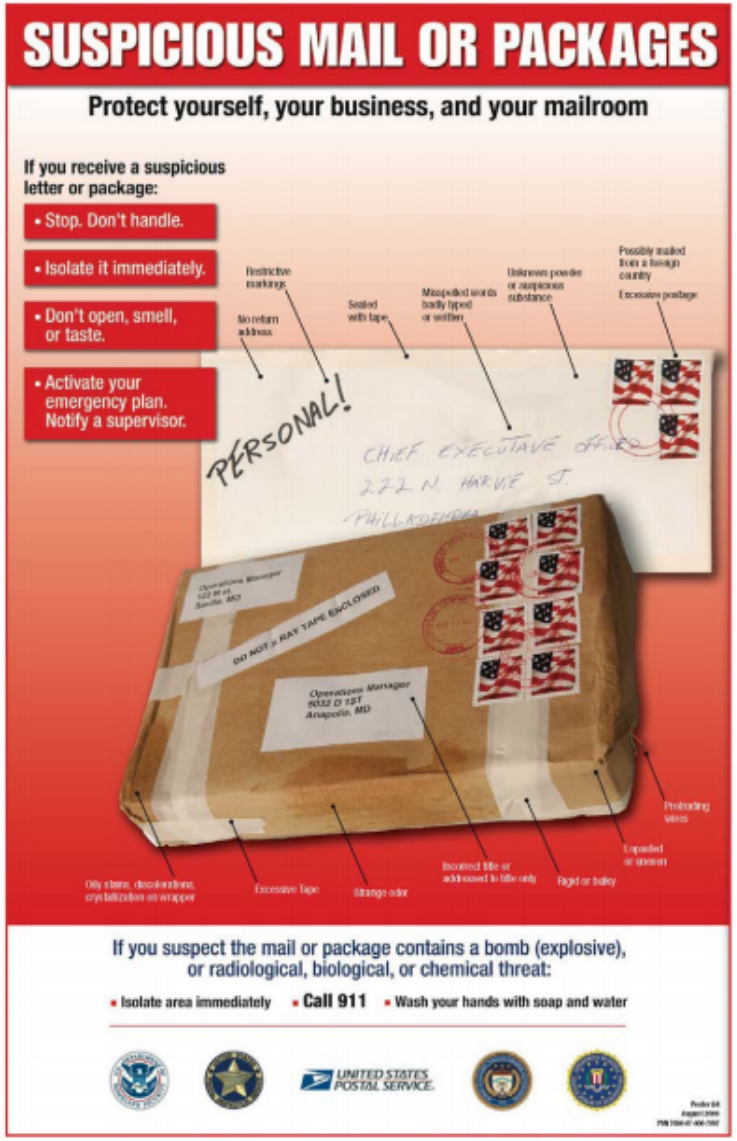
MAIL SCREENING BEST PRACTICES

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

Source: USDHS

Safe Mail Handling and Screening Resources

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY



Best Practices for Safe Mail Handling

Interagency Security Committee

Homeland Security

USPS Suspicious Mail

https://about.usps.com/postal-bulletin/2019/pb22529/html/info_002.htm

USDHS Best Practices

https://www.fbiic.gov/public/2010/nov/safe_Mail_Handling.pdf

Summary

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

- Implementing a mail security program is often the missing link in a comprehensive physical security program.
- It is unfamiliar to many and may present challenges to those who are new to the world of mail security.
- RaySecur can help implement a sound mail center security practice and bridge the gap in your facility's physical security.

Contact

RAYSECUR™
THE NEW STANDARD IN MAIL SECURITY

Cody Martin
Director of Mail Center Security

cmartin@raysecur.com

www.raysecur.com