

Mail Security

Standard Operating Procedure

- **Will Plummer** · Chief Security Officer
- **Cody Martin** · Director of Mail Security



Will Plummer
Chief Security Officer

25 Year U.S. Army EOD

- Master EOD Technician
- Special Operations Commands with multiple combat deployments
- Hundreds of full spectrum EOD responses
- Certified Multifunctional Logistician
- Hazardous Devices School Graduate, ATF Post Blast, Master Instructor



Cody Martin
Director of Mail Security

12 Year U.S. Postal Inspector

- USPIS Dangerous Mail Specialist & Instructor
- Co-created USPIS IED Program for National Headquarters
- Investigator on high-profile / VIP cases
- Screened mail for the NFL, NBA, President George W. Bush
- First responder to hundreds of incidents

- Mail Security Threats
 - Case Studies + Examples
- Mail Security Solutions
 - SOP Examples
- Questions + Answers

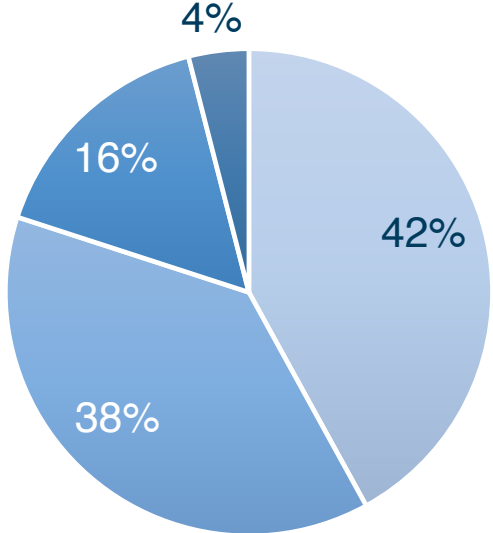
Mail Security Threats

Will Plummer, CSO

42%

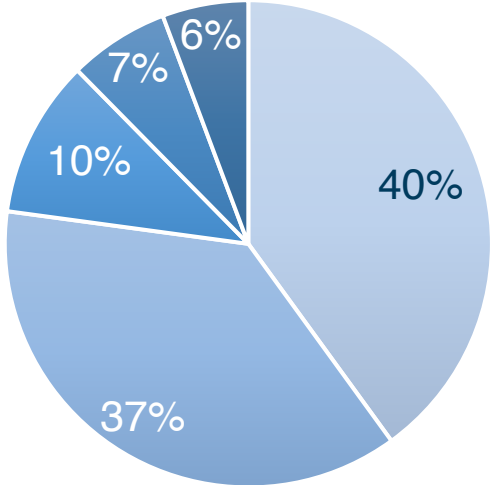
White Powders
and “Other”
Powders

Threat Types



- 42% ■ Drugs
- 38% ■ White Powder
- 16% ■ Other
- 4% ■ Other Powders

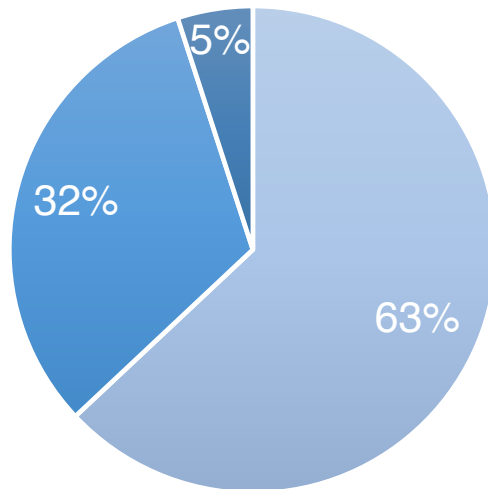
Targets



- 42% ■ Government
- 37% ■ Business / Residence
- 11% ■ Post Office
- 7% ■ Corrections
- 6% ■ Courts

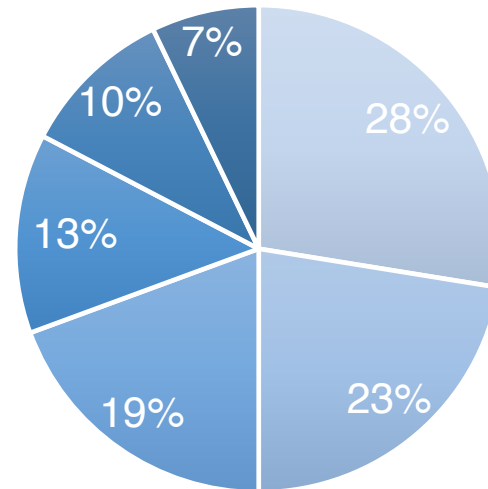
95% of Mail Threats in Small Packages

Container



- 63% ■ Parcels
- 32% ■ Letters
- 5% ■ Unreported

Response



- 27% ■ Hazmat
- 22% ■ EOD/Bomb Squad
- 19% ■ Sheriff
- 13% ■ FBI
- 10% ■ Local police
- 7% ■ USPIS

95%
Small Packages

32% of known threats arrived in a letter envelope, and 63% via parcel — which could be mailed via USPS “blue box.”

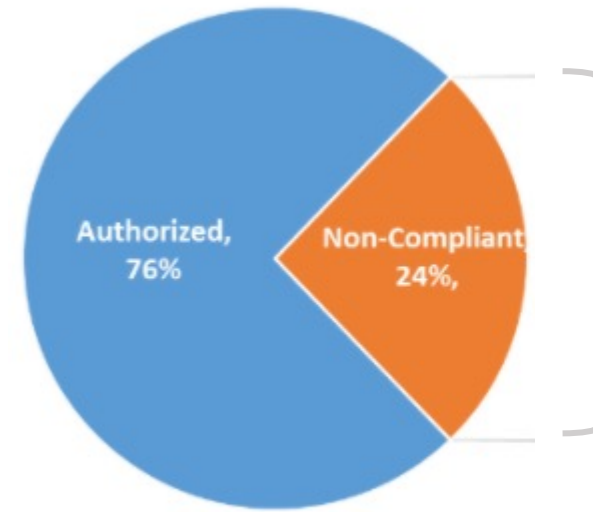


Most Mail Threats

1. Small to fit anonymous drop box
2. Lack chain of custody
3. Exhibit unusual characteristics

Chain of Custody More Frequently Broken

Competition at the Last Mile



Multi-Mode Last Mile Delivery

Potential for risk and complacency

- Crowdsourced providers
- Local carrier services
- Automated technologies



Case Studies

Motives + Mechanics of
Dangerous Mail

1 in 3

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



2020 Shutdown Example

- ~200 Employees Work in HQ
- Approximately 20 on Site
- News outlets tied it to “Firings”
- Recent “problems” like Jared Fogel
- News agencies blamed Corporate



Example: Politician + Ricin (Poison)

Washington DC, Sep 2020

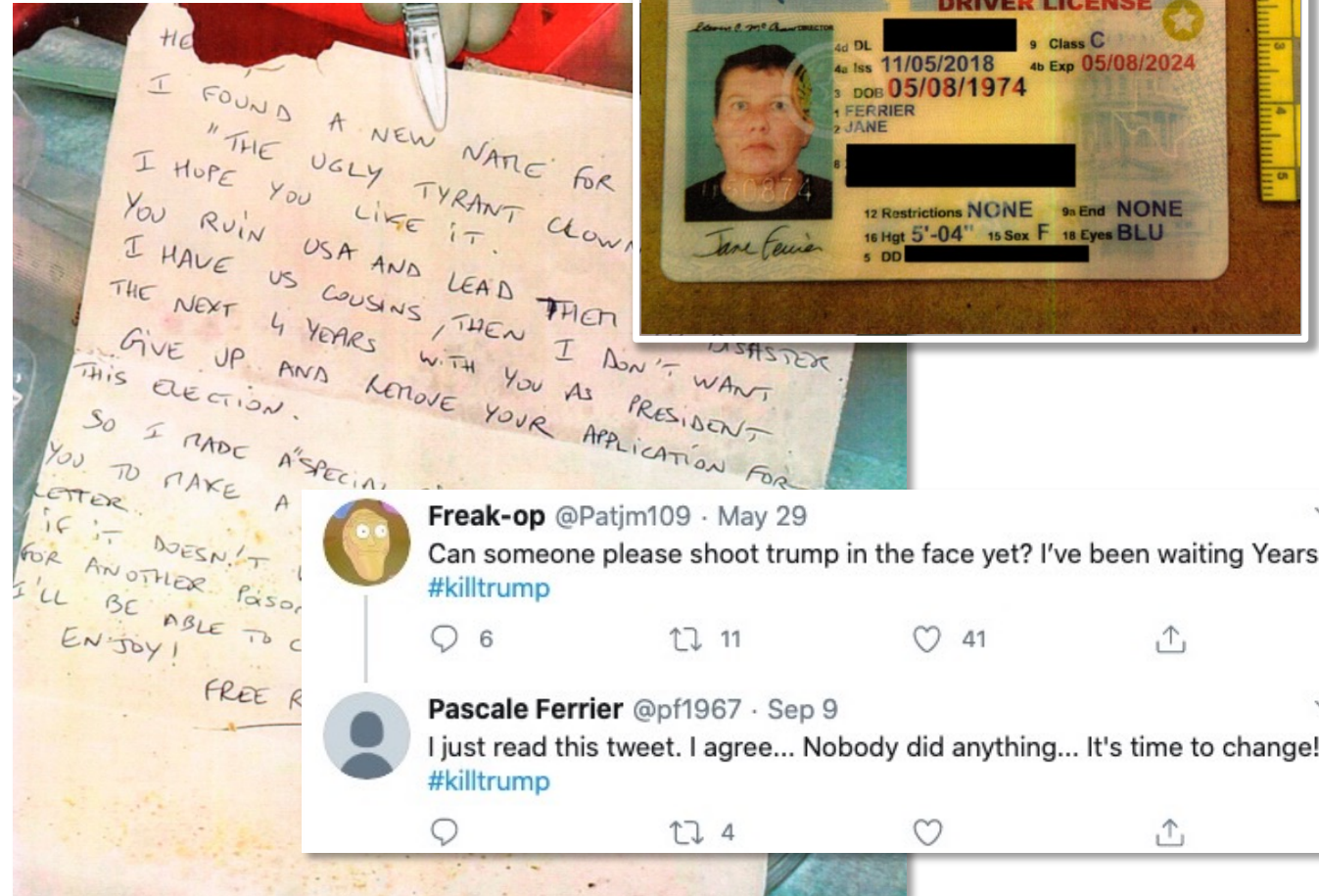
White House – 1 letter

Texas – 6 Letters

- Detention Centers
- Law Enforcement HQs

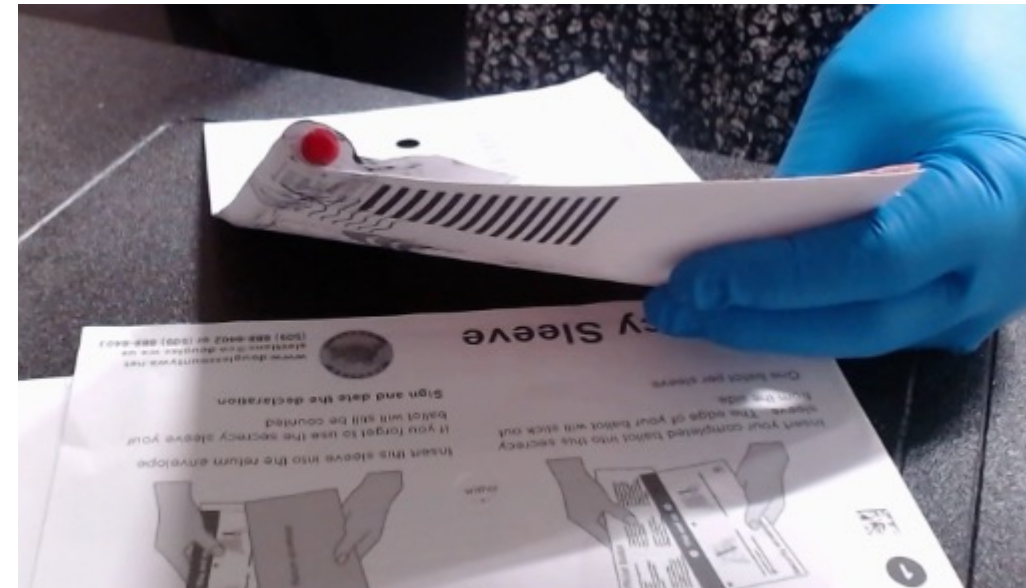
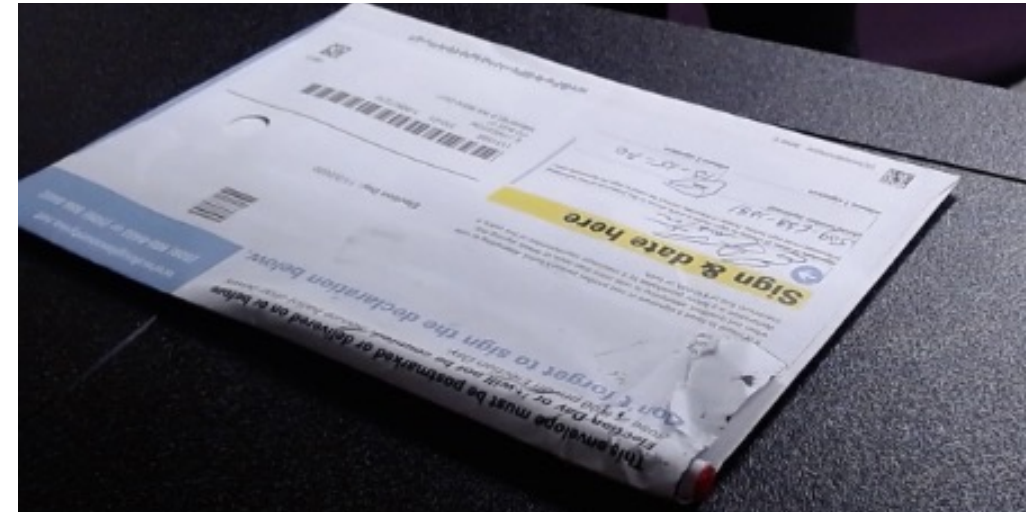
Federal Charges

- Making Interstate Threats
- Violating Prohibitions on Biological Weapons
- USPS



Multiple Cities

1. Las Vegas, NV – Board of Elections
 - White Powder
2. Baltimore, MD – NAACP
 - White powder & racist note
3. Erie County, NY – Board of Elections
 - White Powder
4. Grand Island, NE – Election Commission
 - 24" x 3" tube, blue liquid & electric pump
 - “F___ off, NWO” in reference to the “New World Order” on voter registration form



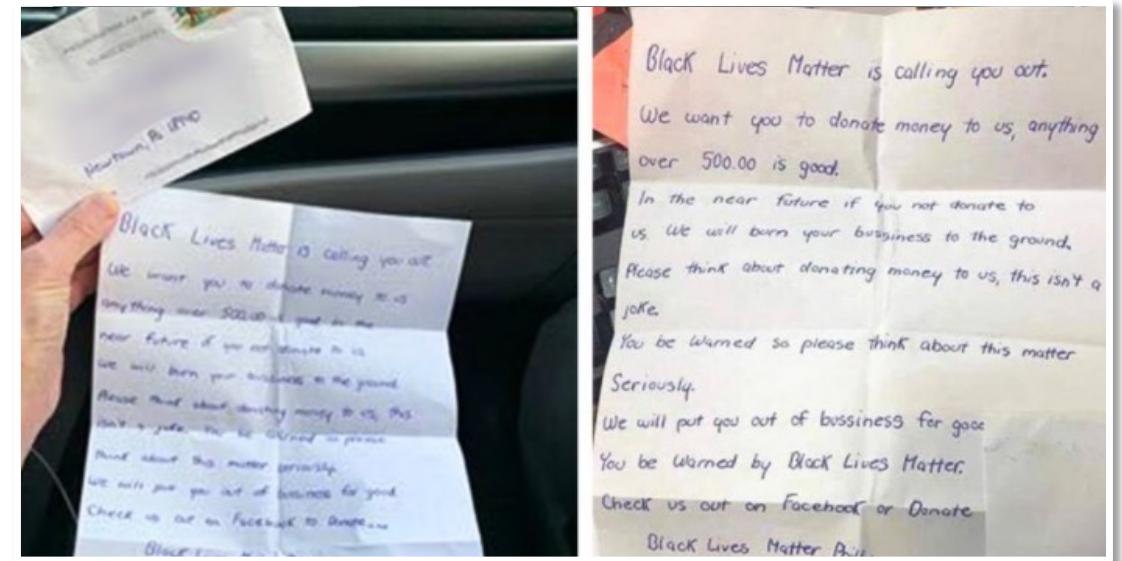
Baltimore

- Last mile threat
 - Allows for safe separation
 - Control of delivery
- Moved into building by occupant 8AM
- Moved to a bedroom 5PM
- Victim emplaced and operated
 - Anti-tamper/Tilt/movement



Suspect Package

- Hoax IED
- In-person church services
- Aimed to force church to close
- Actual outcome:
 - IED Response, Federal Charges
 - State Mandated Shutdown
- Last mile



Illegal Activities

- Hoaxes
- Drugs
- Weapons
- Corporate Espionage
- Counterfeiting
- Smuggling



Wish.com + Others

- You can buy anything you want online



Dangerous Mail Attacks – Global

Date	Location	Target	Incident
2021 - Feb	Germany	LiDL (HQ) and other food manufacturers	Mail bomb, 3 injured
2021 – Jan	UK	AstraZeneca Covid Vaccine Plant	Suspect package
2021- Jan	Canada	Private Residences (Bitcoin Scam)	Multiple white powder letters
2020- Sept.	UK	Individual Consumers (Amazon/PayPal Fraud)	Multiple explosive devices
2020 – May	United States	Subway (HQ)	White powder letter
2020 – April	Hong Kong	HK Chief of Police	White powder letters, followed by letter bomb
2020 – Feb	Netherlands	Ricoh, UNISYS ING Bank, ABN Amro	20+ Mail bombs, several detonations
2019 – Jan	Japan	12+ Drug Companies, Newspapers, Food Mfg.	12+ White powder letters containing cyanide



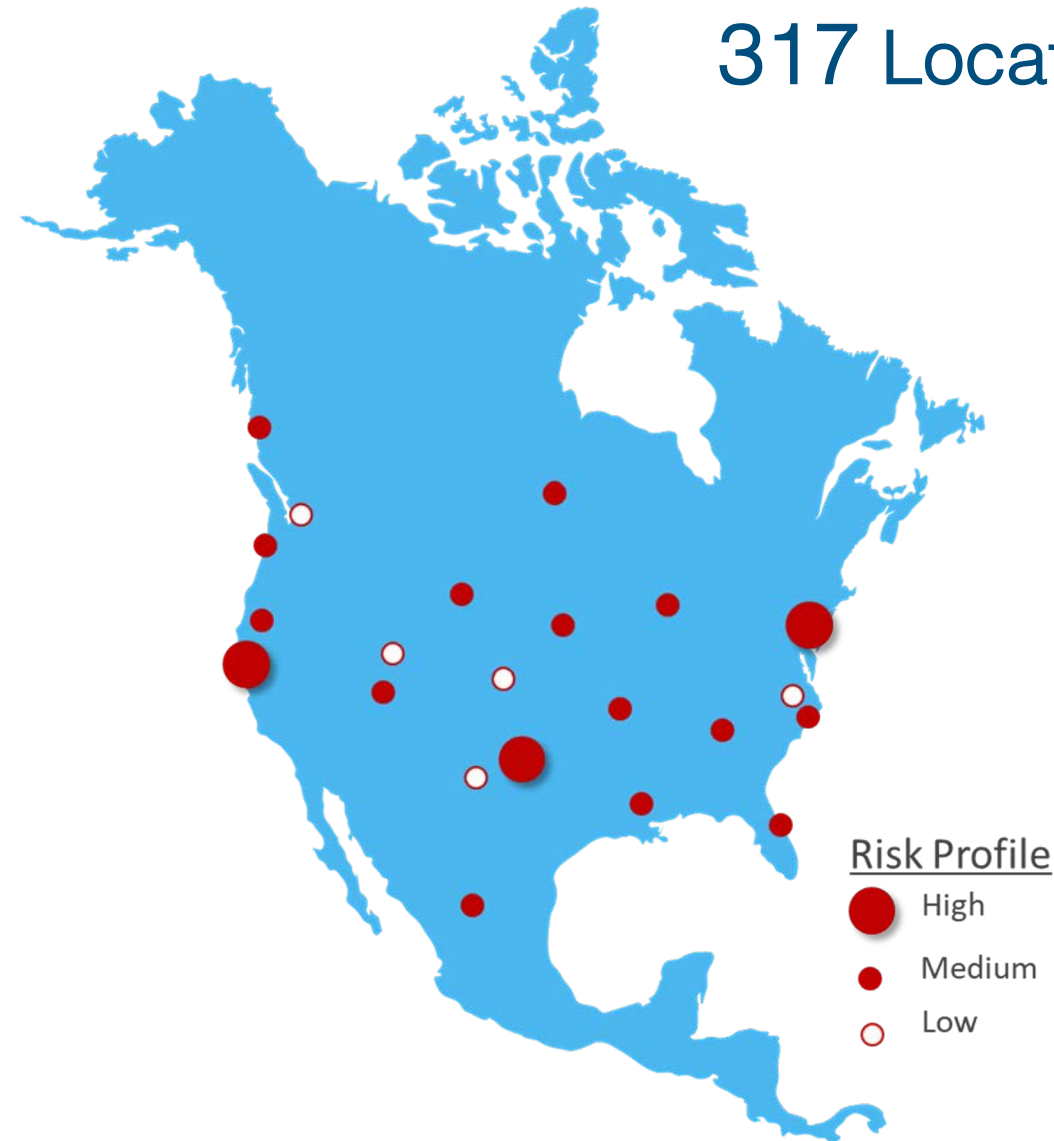


Mail Security Risk Assessment

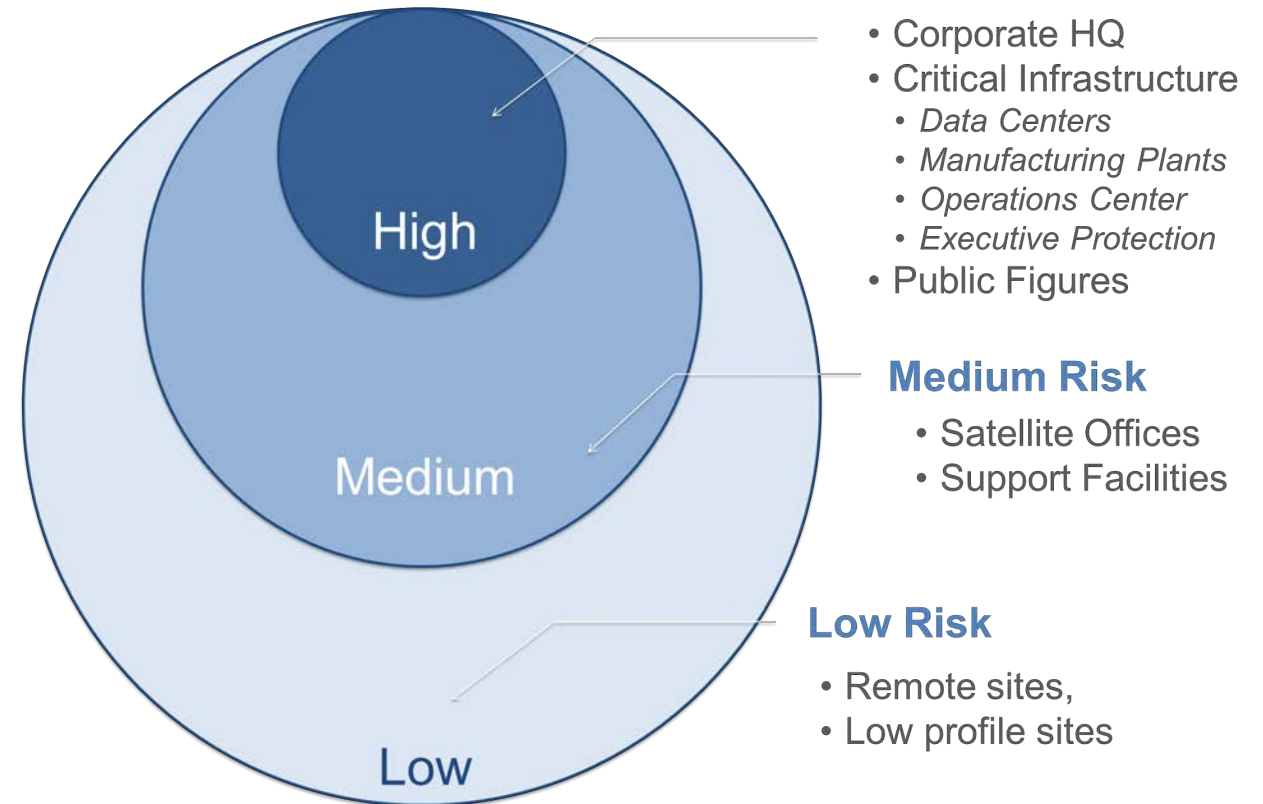
Cody Martin

Director of Mail Security

317 Locations for the Average Fortune 500 Company



Site Risk Profile Varies



US DHS High Risk Areas

- Banking
- Energy / Power
- Defense
- Legal
- Chemical / Pharmaceutical
- Nuclear Facilities
- Transportation
- Health & Medical
- Telecommunications
- Construction
- Bio-Medical Research
- “Military Industrial Complex”



1.43	902.98	UK	UK	UK	UK	UK
03	-21.03	10879	10605	1762	2711	
	3.40	-11	+0	-24	-87	
	5.96	2519/T	66/T	9/T	2614/T	2
		CN	CN	N	CN	

Risk Assessment Considerations

- Symbolism
- Location
- Population



Risk Assessment “Intangibles”

- Previous attacks
- Negative press
- Demonstrations, boycotts, labor disputes
- Disgruntled employees
- Facility layout
- Facility tenants
- Controlled vs. public access
- Loading dock
- Visibility (signage, lighting, advertising)
- Visitors



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

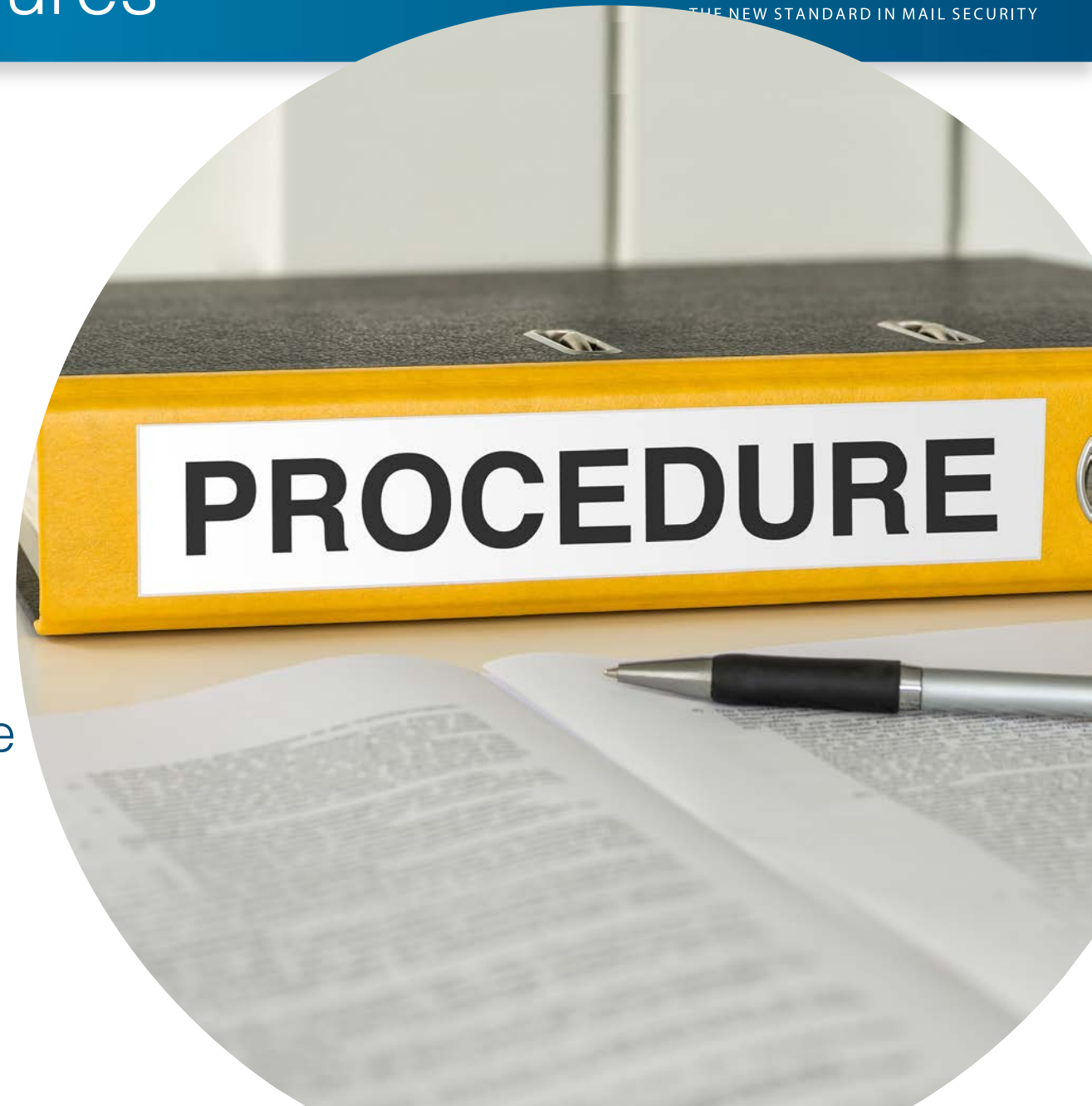


Mail Security SOPs

Solutions + Examples

Standard Operating Procedures

- Specify company-wide
- Global, not site-specific
- Individual sites added case-by-case
- All sites use global standards
- Site-specific SOPs based on risk profile



Global Mail Screening Standards

Global Mailroom Security Policy Statement

Global Mailroom Mail Screening Process

SOP-001: Mail Security Screening

SOP-001A: Executive Protection Screening
Standard Operating Procedure

SOP-002: Suspicious Item Screening

SOP-003: Emergency Response

Site-specific Appendix

Appendix: Site-Specific Information

Site 1

Site 2

Site 3

Site 4

Site 5

Site 6

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

DHS Mail Center Classification & Rating

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

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

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

Best Practices in Anti-Terrorism Security

- Mail room or loading dock only
- Verify registration before accepting
 - Hold courier ID
 - Monitor critical areas
- Electronic surveillance
- Reduce accessories
- Independent HVAC zones



Mail Room Security Practices

- Away from main entrances & infrastructure
- Off-site or at perimeter
- No deliveries during peak business hours
- Screen all packages
- Separate mail room ventilation
- CBRN detection & isolation equipment
- Train on suspicious mail & deliveries
- Provide PPE



PROCEDURE

SOP

Examples

Enhanced Security Mail Screening

PURPOSE

The purpose of this standard operating procedure (SOP) is to define and outline safe and approved enhanced mail security screening procedures that serve as standards for the organization to follow.

This SOP is covered in four sections critical to maintaining a high level of mail security for the organization: (I) receiving area, (II) transfer route, (III) mailroom operation, and (IV) delivery.

IMPLEMENTATION

The following four sections cover critical aspects of the screening process required to maintain a high level of mail security for the organization, including the mail receiving area, transfer route, mailroom operation, and delivery.

Section I: Receiving area

Section II: Transfer Route

Section III: Mailroom Security Operations

Section IV: Distribution

Suspicious Package Screening

Section I: Validate Suspicious Item

- Best judgment & intuition
- USPS Poster 84 examples
- Look for suspicious characteristics
- Confirm legitimate addressee or sender

Section II: Render Situation Safer

- Minimize risk to people & property
- Place item down — no one else exposed

Section III: De-escalate Situation

- Reach out for support
- Follow emergency response card

Section IV: Escalate to ERP

- Additional review with support
- Corporate security may initiate ERP

Emergency Response

Step 1: Evacuation

- Physical reaction
- Smoke, vapors, fumes
- Any threatening substance

Step 2: Communicate to Security Team

- Chain of command (emergency response card)
- Relay pertinent data
- Discuss why item not rendered safe

Step 3: Risk Mitigation

- Good-faith effort to reduce risk
- Minimize exposure to employees & facilities

Step 4: Call First Responders

- Local hazmat team
- Police + Fire department
- US Postal Inspection Service
- Any applicable jurisdiction

Questions & Discussion

State of Mail Security – Annual Report

- ATF & USPSIS data
- Case studies & analysis

[RaySecur.com/Report](https://www.raysecur.com/Report)





Will Plummer
will@raysecur.com



Cody Martin
cmartin@raysecur.com



TJ Kelly
tjkelly@raysecur.com

RaySecur.com/Report

Appendix

USPS Poster 84

SUSPICIOUS MAIL OR PACKAGES

Protect yourself, your business, and your mailroom

If you receive a suspicious letter or package:

- Stop. Don't handle.
- Isolate it immediately.
- Don't open, smell, or taste.
- Activate your emergency plan. Notify a supervisor.

Warning Signs:

- Restrictive markings
- No return address
- Sealed with tape
- Misprinted words, body typed or written
- Unknown powder or suspicious substance
- Possibly mailed from a foreign country
- Excessive postage
- Handwritten: **PERSONAL!**
- Address: CHIEF EXECUTIVE OFFICE, 272 N. HARVE ST., PHILADELPHIA
- Labels: Operations Manager, 100 Mt. Sohier, MD; Operations Manager, 9832 D. ST, Annapolis, MD
- DO NOT - RAY TAPE ENCLOSED
- Protruding wires
- Excessive tape
- Strange odor
- Incorrect title or addressed to title only
- Faded or bulky
- Liquid or unusual
- Only stains, discolorations, crystallization on wrapper

If you suspect the mail or package contains a bomb (explosive), or radiological, biological, or chemical threat:

- Isolate area immediately
- Call 911
- Wash your hands with soap and water

Logos: FBI, DHS, UNITED STATES POSTAL SERVICE, FBI, DHS

Poster 84 August 2016
PSN 2006-01 606-2007

Emergency Response Card

EMERGENCY RESPONSE INFORMATION

Manager

Police

Fire

USPIS

Fire Extinguishers

Medical Kit

Decontamination Kit

Eye Wash Station

RAYSECUR™
SAFE ACCESSIBLE DETECTION

press1 1-844-RAY-SECUR (729-7328)

Note: This information is intended to help in design and implementation of an Emergency Response Plan or Emergency Action Plan in mailrooms. It is not intended to be used without modification to the unique needs of a facility or mailroom.

Poster06.19

- Official and open-source data
- More case studies
- Deep-dive analysis

RaySecur.com/Report

