POSTAL AND SHIPPING: IDENTIFICATION AND MITIGATION OF SUSPICIOUS MAIL AND PACKAGES

SCOPE: This product is intended for those who might be required to handle mail and packages in the course of their work in order to promote awareness and coordination among public safety and private sector entities, and to improve their ability to identify, report, and mitigate the effects of suspicious mail and packages. For specific suspicious package indicator information, refer to the products in the Resources section. None of the information in this document is intended to replace existing standard operating procedures or policies. This product was developed in coordination with the US Postal Service and postal/shipping private sector partners.

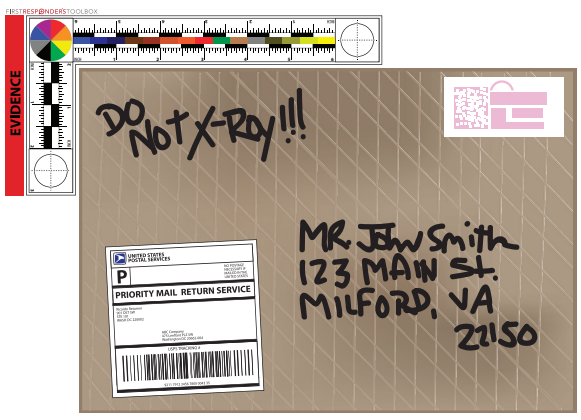
WHAT IS SUSPICIOUS? With no single list of all possible indicators, suspicious encounters can be anything that cannot easily be dismissed at that time, and should be reported.

- Incidents involving suspicious mail and packages should be reported immediately to the appropriate manager, security personnel, public safety official, first responder, or other responsible party. If the facility is a multi-tenant facility, appropriate building management should also be notified.
- Suspicious mail response procedures will vary by organization and will be based on a combination of factors such as the type and location of the item discovered (CBRNE, dangerous items, hoaxes, and threatening content), personnel, and specific organization emergency response protocols.
- Early notification of appropriate federal partners (US Postal Inspection Service, FBI, ATF), regional fusion center, closest medical facility(s), and private shipping or courier company will assist in incident stabilization and investigation.
- First responder agencies, including 911 emergency call and dispatch centers, should familiarize themselves with updated policies, procedures, and resources within their area of responsibility to notify and inform appropriate response personnel effectively.

UPON DISCOVERY: If a suspicious letter or package is discovered:

1) Follow established policies and procedures;
2) **DO NOT** disturb, handle or open;
3) Evacuate the premise/area;
4) **Notify 911** and remain in contact with call taker or provide with a call back number; and
5) List persons in the immediate discovery area for potential medical treatment and follow up questioning.

PROVIDE A DETAILED DESCRIPTION OF THE ITEM, INCLUDING PHYSICAL APPEARANCE, ORIGIN, AND INTENDED DESTINATION:



Label

- Computer generated
- Handwritten/postage
- Courier/hand delivered

Expecting the letter/package?

- Recognize the sender?

Early engagement

- Federal law enforcement partners
- US Postal Inspection Service
- Private shipping company
- Courier/hand delivered

Suspicious circumstances

- **W**ho, **W**hat, **W**hen, **W**here, **W**hy, and **H**ow
- Detailed Physical Description

Pictures

- **IF SAFE** and without moving item
- Each visible side of suspicious letter/package
- Size and color reference
- Visible names, addresses, labels, declarations, and postage
- **Do NOT** send or upload images in vicinity of package

CHARACTERISTICS AND IMPORTANT CONSIDERATIONS FOR SUSPECTED **CBRNE** OR **HOAX** DEVICE LETTER OR PACKAGE:

EXPLOSIVE: Parcel bomb attacks may be placed into the parcel system in clusters or over a period of time, so the presence of one device requires an immediate investigation to determine if additional parcel bombs remain within the shipping system. The origin, components, and intended destination of the package will be important clues in identifying the bomber and a possible motive.

- Evacuate to a safe distance without using cell phone or radios in the line of sight or vicinity of the potential device, because doing so could cause the explosive device to detonate.
- Explosive devices may be intentionally disguised to provide a false sense that the device is a "dud" and, therefore, safe to handle. However, no device should be handled until rendered safe by qualified experts.

CHEMICAL/BIOHAZARD: Because of the minuscule size and amount needed for biological agents, the threat may not be as immediately apparent, possibly delaying consequence management and causing further contamination. Chemical threats may be aerosols, liquids or solids, small in size, light in weight, and contained until opened, making detection problematic. Leaks or spills—including powders, stains and discoloration—may be indicators.

- **Do NOT** attempt to clean up leaks or spills.
- If possible, close windows and doors and shut off HVAC systems to prevent further contamination.
- Report any signs or symptoms of exposure.
- Isolate those potentially exposed for further triage.

RADIATION OR NUCLEAR: Radioactive materials are widely used in agriculture, medicine, industry, and research. The use of a radiological dispersion device (RDD), or "dirty bomb," requires minimal technical knowledge to build and deploy.

- Evacuate to a safe distance without using cell phones or radios in the line of sight or vicinity of the potential RDD, because doing so could cause a device to detonate.
- Isolate those potentially exposed for further triage.

HOAX: The use of a hoax package/letter may be designed to elicit a specific response, which may be used by terrorists to spread fear, divert, test, and/or determine response capabilities or assess security features, and may have the potential to develop complacency among screening and security staff or first responders. Hoax packages/letters may also be used to delay or cancel events.

SAFETY REMINDER: ONLY QUALIFIED EXPERTS SHOULD ATTEMPT TO RENDER WOULD-BE CBRNE DEVICES OR COMPONENTS SAFE, AS IMPROPER HANDLING MAY CAUSE INJURIES OR FATALITIES, OR CONTAMINATE FORENSIC EVIDENCE.

RESPONDING PERSONNEL should note the details of anything out of the ordinary and follow up with the reporting party to help guide or determine additional response needs. This may include screening the area for potential secondary attacks, establishing a unified command post to ensure efficient response, incident stabilization—including possible requests for EOD or HazMat, as exposure may result in numerous types of traumatic injures (blast pressure, internal, burns, and shrapnel)—and the smooth transition to the investigation phase. It is important to note that evidence collection drives the need for complete and accurate reporting to assist with a follow-on investigation.

NCTC 034215 ID 11-18
15 NOV 2018
AUTHORED BY NCTC

POSTAL AND SHIPPING: IDENTIFICATION AND MITIGATION OF SUSPICIOUS MAIL AND PACKAGES *Continued*

OUTLOOK: In the near- to mid-term, terrorists and criminals will likely attempt to circumvent security measures by taking advantage of new technologies and adapting existing services. As the postal and shipping sector continues to expand and evolve to meet business and consumer needs, public safety and private sector entities will need to update their policies and procedures periodically. Policies and procedures should take into account ways in which terrorists may leverage emerging technologies such as Unmanned Aerial Systems, or online retailers or pop-up shippers to "rebag" hazardous materials,

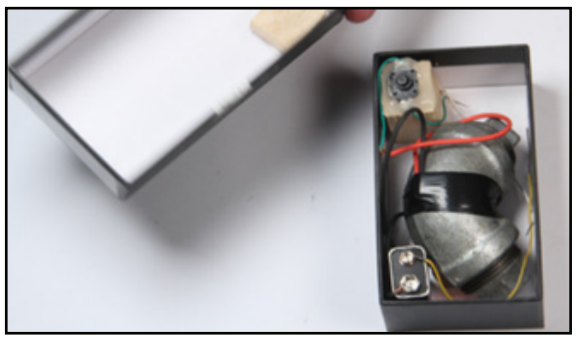


IMAGE TAKEN FROM AN ONLINE ENGLISH-LANGUAGE TERRORIST PUBLICATION ESPOUSING THE USE OF EXPLOSIVE PACKAGES

including explosives, or radiological, biological or chemical materials. Actionable intelligence often results from information sharing between partners at all levels, as each may be aware of potentially related bits of information that will help develop a greater understanding of a threat and identify trends in terrorist and criminal tactics. First responders and private sector entities are encouraged to establish a rapport before an incident. Regular information sharing/tracking and participation in preparedness exercises among the Intelligence Community, other government agencies, first responders, public safety officials, and private sector partners will help to ensure a rapid response, medical countermeasures, and investigation.

The identification and mitigation of suspicious mail and packages remains a complex, resource-intensive issue which may be effectively addressed through intergovernmental and private sector partnerships. Terrorists will continue to exploit the postal and shipping sectors in various ways, including mailing and shipping explosives, hazardous chemicals, and their precursors; carrying out attacks; delivering threats; propagating hoaxes; performing financing and support activities; and testing security. The accessibility of the postal and shipping sector, combined with English-language media encouraging related terrorist attacks and the publicity surrounding incidents involving suspicious packages may spur ongoing or increased interest by nefarious actors.

UNDERSTANDING THE INDICATORS: Basic "indicators" of suspicious mail and packages are readily available. The challenge is ensuring the appropriate training and reporting mechanisms are in place so that indicators are communicated to relevant stakeholders. Any parcel can be deemed "suspicious" depending on the expectations of the handler, recipient, or any other individual reporting the package. The package, its delivery mechanism, and the person delivering the package may all display suspicious indicators and behaviors. Terrorists and criminals will likely use seemingly innocuous methods and are only limited by their creativity, access to materials, and knowledge; therefore, it is important that stakeholders maintain a low threshold for suspicion. Indicators of suspicious mail or packages may be observed by any individual involved in any part of the shipping and handling process from initial order to final delivery.

- **Who:** Vendor, packager, shipper, driver, handler, inspector, law enforcement, the general public, or the recipient.
- **Where:** Shipping and packing facility, shipping and delivery vehicle, cargo screening facility, mailroom, and business or residence to which mail or package is delivered.

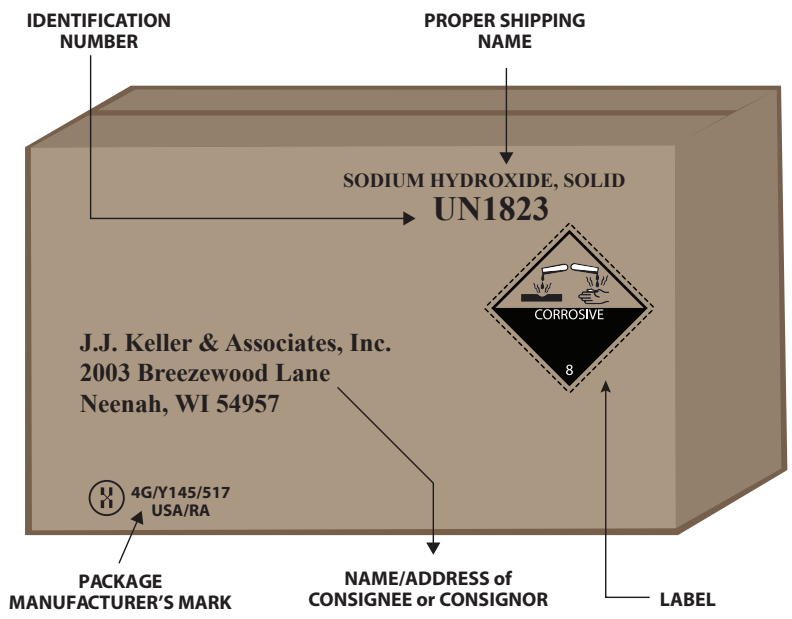
ORGANIZATIONAL ROLES: The postal and shipping sector plays an important role for investigative officials to identify individuals purchasing and selling illicit materials (precursor materials, weapons, toxins, narcotics, etc.) through Darknet marketplaces, as these items can be intercepted in transit and may contain important identifiers regarding origin, proxy, and mailing address of the perpetrators.

- **US Postal Service:** When a suspicious mail incident occurs on USPS property, US Postal Inspection Service (USPIS) conducts an internal response and investigation. Based on their assessment of the incident, USPIS may request specific support such as bomb squads or HAZMAT teams. If the incident occurs off USPS property, USPIS may liaise with first responders, potentially utilizing standing relationships with JTTFs. It is illegal for anyone other than the recipient to open a piece of US domestic mail once it has entered the postal system—including for Postal Inspectors—without a federal search warrant.
- **Private Sector:** Private sector shipping and delivery companies maintain their own individual response procedures, which may vary from one location to another. Companies typically notify both local law enforcement and onsite security in the event of an incident, and in general, will clear the incident internally if deemed appropriate, based on internal policies and resources. Shipping and delivery companies maintain internal security practices which include the ability to open suspicious packages, but reporting depends on employees, highlighting the importance of regular training.

SHIPPING AND HANDLING: All organizations that handle mail and packages should consider a defined screening element as an essential part of a complete security program. Developing and continually updating a comprehensive letter and package-screening program should consider:

- Screening all mail and packages when they first arrive;
- When possible, offsite mail screening has the potential to lessen exposure or damage;
- Training personnel who sort mail by hand or sign for packages to properly screen incoming items; and
- Verifying couriers and screening hand-delivered letters and packages.

NON-BULK PACKAGE:
Correctly Shipped Hazardous Material Packaging



RESOURCES:

- **US Postal Inspection Service Poster**—*https://about.usps.com/posters/pos84.pdf*
- **USPS—Guide to Mail Center Security**—*https://aboutUSPS.com/publications/pub166.pdf*
- **FBI/DHS—BOMB THREAT STAND-OFF CARD**—*https://tripwire.dhs.gov/IED/resources/docs/DHS-DOJ%20Bomb%20Threat%20Stand-off%20Card.pdf*
- **DHS—BEST PRACTICES FOR MAIL SCREENING AND HANDLING PROCESSES:** *A Guide for the Public and Private Sectors"*—1st Edition—*https://www.dhs.gov/sites/default/files/publications/Mail_Handling_Document_NonFOUO%209-27-2012.pdf*
- **DHS—National Protection & Program Directorate**—Hazardous Information Training Sheet "Safe Mail Handling Procedures"—*http://www.osec.doc.gov/osy/PDF/SafeMailing.pdf*
- **DHS—TripWire**—*"How to React Quickly and Safely to Suspicious Packages and Bomb Threats"*—*https://tripwire.dhs.gov/IED/resources/jsp/loginPopup2.jsp*
- **DHS—What To Do—Bomb Threat**—*https://www.dhs.gov/what-to-do-bomb-threat*
- **DHS—Bomb-Making Materials Awareness Program**—*https://dhs.gov/bmap*
- **DHS—Counter-IED Training and Resources Page**—*https://www.dhs.gov/bombing-prevention-training*#
- **National Explosive Task Force (NEFT)**—*"Suspicious Package Indicators & Recommended Response Procedures"*—*https://www.fbi.gov/file-repository/suspicious-package-indicators.pdf/view*
- **Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)**—*https://nsi.ncire.gov*
- **CHEMTREC**—*1-800-424-9300*
- **National Poison Control Center**—*1-800-222-1222*

NCTC 034215 ID 11-18
15 NOV 2018
AUTHORED BY NCTC

JOINT COUNTERTERRORISM ASSESSMENT TEAM | JCAT

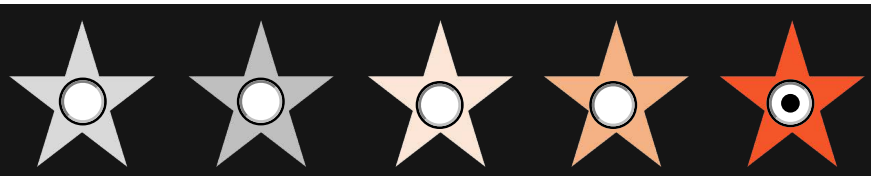
PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and/or ORG:

DISCIPLINE: ☐ LE ☐ FIRE ☐ EMS ☐ HEALTH ☐ ANALYSIS ☐ PRIVATE SECTOR DATE:

PRODUCT TITLE: NCTC-FBI-DHS (U) First Responder's Toolbox -Postal and Shipping- Identification and

POOR  GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS. HOW DOES JCAT MAKE PRODUCTS BETTER?

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT