INCREASE IN BOMB THREATS AND SUSPICIOUS PACKAGES

OVERVIEW

In 2023, the US Bomb Data Center (USBDC) Explosive Incident Report (EIR) recorded a significant increase in bomb threats and suspicious package reporting involving commercial, healthcare, transportation, government and other facilities. There were 3,203 reported bomb threat incidents reported in the USBDC Bomb Arson Tracking System (BATS) and the Cybersecurity and Infrastructure Security Agency (CISA) Office for Bombing Prevention's (OBP) Technical Resource for Incident Prevention (TRIPwire) during the 2023 calendar year. This was a 26 percent increase from the previous year. There were also 6,284 suspicious/unattended package incidents reported in BATS and TRIPwire in 2023. This was a 13 percent increase from the previous year.

PLANNING FOR BOMB THREATS

Planning and preparing for bomb threats may not influence the number of threats received but will significantly reduce the psychological and emotional stress and lessen the financial impact by shortening the duration of the threat response. Having a Bomb Threat Management (BTM) Plan may ensure that your organization is better prepared in the event of a bomb threat while also reducing risk should an actual explosive device be involved. The four primary goals of a BTM Plan are to: 1) mitigate vulnerabilities to bombing incidents, 2) make informed decisions during bomb threat assessments, 3) deter potential perpetrators of bombing incidents, and 4) minimize the consequences of a potential attack or threat on personnel and property. A proactive BTM Plan, in combination with training and exercising that plan, will allow stakeholders to manage threats more effectively. Additional information on roles, responsibilities, and what to do during an incident can be found in the Bomb Threat Guide.

WHAT TO DO DURING A BOMB THREAT

IF YOU RECEIVE A PHONED THREAT:

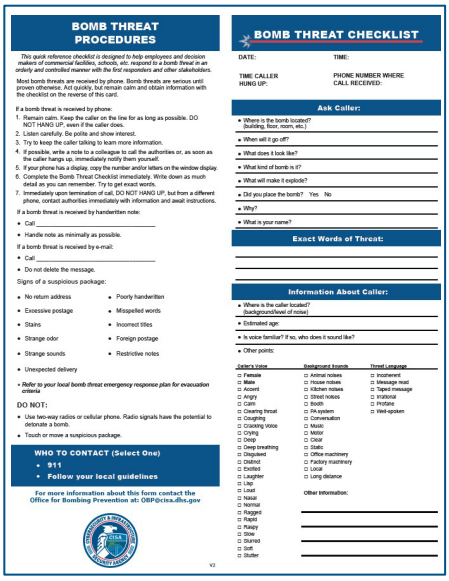
- Remain calm & do not hang up; keep the caller on the line for as long as possible.
- If possible, signal other staff members to listen & notify Site Decision Maker(s).
- If the phone has a display, copy the number and/or letters on the display.
- Write down the exact wording of the threat.
- Record the call if possible.
- Fill out the Bomb Threat Checklist immediately.

IF YOU RECEIVE A SOCIAL MEDIA OR EMAIL THREAT:

- Do not turn off or log out of the account.
- Leave the message open on the device.
- Take a screenshot, or copy the message and subject line.
- Note the date and time.
- Notify the organization Site Decision Maker(s).

IF YOU RECEIVE A WRITTEN THREAT:

- Handle the document as little as possible.
- Note date, time, and location the document was found.
- Secure the document and do not alter the item in any way.
- Notify the organization Site Decision Maker(s).



BOMB THREAT PROCEDURES

This quick reference checklist is designed to help employees and decision makers of commercial facilities, schools, etc. respond to a bomb threat in an orderly and controlled manner with the first responders and other stakeholders.

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the reverse of this card.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of call, DO NOT HANG UP, but from a different phone, contact authorities immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call _____
- Handle note as minimally as possible.

If a bomb threat is received by e-mail:

- Call _____
- Do not delete the message.

Signs of a suspicious package:

- No return address
- Poorly handwritten
- Excessive postage
- Misspelled words
- Stains
- Incorrect titles
- Strange odor
- Foreign postage
- Strange sounds
- Restrictive notes
- Unexpected delivery

Refer to your local bomb threat emergency response plan for evacuation criteria

DO NOT:

- Use two-way radios or cellular phone. Radio signals have the potential to detonate a bomb.
- Touch or move a suspicious package.

WHO TO CONTACT (Select One)

- 911
- Follow your local guidelines

For more information about this form contact the Office for Bombing Prevention at: OBP@cisa.dhs.gov

BOMB THREAT CHECKLIST

DATE: TIME:

TIME CALLER HUNG UP: PHONE NUMBER WHERE CALL RECEIVED:

Ask Caller:

- Where is the bomb located? (building, floor, room, etc.)
- When will it go off?
- What does it look like?
- What kind of bomb is it?
- What will make it explode?
- Did you place the bomb? Yes No
- Why?
- What is your name?

Exact Words of Threat:

Information About Caller:

- Where is the caller located? (background/level of noise)
- Estimated age:
- Is voice familiar? If so, who does it sound like?
- Other points:

Caller's Voice	Background Sounds	Threat Language
□ Female	□ Animal noises	□ Incoherent
□ Male	□ House noises	□ Message read
□ Accent	□ Kitchen noises	□ Taped message
□ Angry	□ Street noises	□ Irrational
□ Calm	□ Booth	□ Profane
□ Clearing throat	□ PA system	□ Well-spoken
□ Coughing	□ Conversation	
□ Crackling Voice	□ Music	
□ Crying	□ Motor	
□ Deep	□ Clear	
□ Deep breathing	□ Static	
□ Disguised	□ Office machinery	
□ Distinct	□ Factory machinery	
□ Excited	□ Local	
□ Laughter	□ Long distance	
□ Lisp		
□ Loud	Other Information:	
□ Nasal		
□ Normal		
□ Ragged		
□ Rapid		
□ Raspy		
□ Slow		
□ Slurred		
□ Soft		
□ Stutter		

V2

Bomb Threat Checklist

IDENTIFYING SUSPICIOUS MAIL AND PACKAGES

Below are some common external characteristics of suspicious mail associated with criminal activity. Some of these indicators, such as unusual markings, excessive tape, and excessive postage, are also typical characteristics of legitimate mail received from uniformed service members, overseas citizens, and other sources. You can also refer to the Suspicious Mail or Packages Poster which provides tips to determine whether a piece of mail or package seems suspicious. The poster also outlines steps you should follow in the event you receive a suspicious package.

- No return address
- Restrictive markings (e.g., fragile, confidential, etc.)
- Poorly wrapped, excessive tape
- Improper spelling
- Badly typed or conspicuously written addresses
- Unknown powder or suspicious substances outside envelope (e.g., oily stains, package/letter discoloration, strange odor, protruding wires)
- Unexpected mail from a foreign country
- Excessive postage, no postage, not canceled

Suspicious Mail or Packages Poster

BE PREPARED FOR WHATEVER ARRIVES IN THE MAIL – SAFE PACKAGE HANDLING

Handling packages safely is crucial to protect yourself and others from potential dangers. Because of the increased sophistication of letter or package bombs and placed devices, fewer bombs can be readily identified by examining the exterior of a mail piece. If you're not expecting a letter or package, be suspicious. Whether you receive mail at home, work, or elsewhere, following these steps can help ensure your safety if you receive an unexpected mail piece:

- First, check the return address.
- If you don't recognize the return address, attempt to contact the sender.
- Don't open the mail piece until verification proves it's harmless.

ESTABLISH LETTER AND PACKAGE BOMB-SCREENING PROTOCOL AT ORGANIZATIONS OR BUSINESSES:

- Evaluate your organization to determine if your business or an employee is a potential target.
- Appoint a person and an alternate to be responsible for your screening plan and to ensure compliance.
- Understand screening procedures for all incoming letter and package deliveries. Train employees in the procedures.
- Develop handling procedures for items identified as suspicious and dangerous.
- Develop procedures for confirming the contents of suspicious letters and packages identified through screening.
- Establish procedures for isolating suspicious letters and packages.
- Conduct unannounced tests of contingency plans.

WHAT IS THE IMPORTANCE OF TESTING CONTINGENCY PLANS?

Test contingency plans with mock suspicious parcels placed in the mail center or elsewhere in the facility. The tests should be conducted in a manner that does not alarm employees. Dress rehearsals help ensure your lines of communication function as planned, and each person who has a role to play knows his or her part. Test the efficiency of your emergency contingency plan by conducting scheduled tests. Hold post-test meetings to address problems and resolve them before the next test.

WHAT TO DO – HANDLING SUSPICIOUS MAIL OR PACKAGES

If you believe the mail piece might be hazardous, take the following steps:

- INSPECT: Using the points of recognition or identifiers listed above, inspect the item to determine whether it is suspicious.
- ISOLATE: Avoid unnecessary movement or shaking of the package. Isolate the area where the mail piece was found—do not touch it. If the package was handled, avoid touching your face or any part of your body.
- ALERT: If received by a business, alert employees that a suspicious letter or package has been found, what the points of recognition are, and to remain clear of the isolation area.
- NOTIFY: Inform management and security that a suspicious item has been detected by the screening process.
- DOCUMENT: Without touching the mail piece, record from each visible side of the item all available information (name and address of addressee and of sender, postmark, cancellation date, types of stamps, and any other markings or labels found on the item). Copy information with exact spelling and location given on item.
- INFORM: Inform the proper authorities of all information recorded from the suspect item.

RESOURCES

- Refer to the U.S. Postal Inspection Service Guide to Mail Center Security for guidance on how to assess risk level, establish sound security protocols, and how to handle suspicious mail.
- Refer to the U.S. Postal Service Poster 84 to download and post a visual guide to suspicious mail indicators in the room where mail is handled. The poster can be found at: Suspicious Mail or Packages Poster | CISA
- OBP Response to Suspicious Behaviors and Items for Bombing Prevention Course (AWR-335) | CISA. This course is an introduction to the response to suspicious behaviors and items and provides participants with a foundation of potential suspicious behaviors and activities related to terrorist or criminal activities. This course also highlights what to do when encountering an unattended or suspicious item and who to report it to.
- OBP Introduction to Bomb Threat Management Course (AWR-939) | CISA. This course provides learners foundational knowledge on domestic bomb threat data, the OBP BTM Plan process, elements of a bomb threat plan, and the overall impact of bomb threats.
- Whether the bomb threat is made via phone, handwritten note, email, social media, or other means, the Bomb Threat Checklist provides instructions on how to respond to a bomb threat and a comprehensive list of information that will assist law enforcement in a bomb threat investigation.
- The Bomb Threat Guide provides awareness and guidance in preparing for and reacting to a bomb threat. It assists decision makers with assessment of received bomb threats, providing response guidance to save lives and protect critical infrastructure. This guide is also dual sealed with the Federal Bureau of Investigation (FBI).
- Developed in partnership with the FBI, the Department of Homeland Security (DHS)-Department of Justice (DOJ) Bomb Threat Stand-Off Card is a quick reference guide providing recommended evacuation and shelter-in-place distances for various types and sizes of Improvised Explosive Devices (IED).
- Gain insight into how to plan for, assess, and respond to bomb threats at your facility with OBP's various resources found at Bomb Threats | CISA.
- The Interagency Security Committee's (ISC) mandate is to enhance the quality and effectiveness of security in and the protection of buildings and nonmilitary Federal facilities in the United States. The ISC standards apply to all buildings and facilities in the United States occupied by federal employees for nonmilitary activities. For more information, visit Interagency Security Committee Policies, Standards, Best Practices, Guidance Documents, and White Papers | CISA.
- STAY IN THE KNOW: Get to know CISA and its mission through our series of 30-minute, topical live events hosted on the LinkedIn Live platform. Each *CISA Live!* features experts from CISA, as well as occasional guests from other agencies, who examine current issues related to cyber and physical critical infrastructure security and resilience, offer related tools and resources, and answer live audience questions. To watch live and access past sessions visit CISA Live! | CISA.