WHAT TO DO: BOMB THREATS

OVERVIEW

Bomb threats involve any communication that indicates the presence of, or intent to detonate an explosive device. While these threats can be connected to actual acts of violence in which explosives are used, these threats are increasingly used as a tactic to disrupt, distract, or harass locations or organizations. The operational, financial, and psychological impacts that bomb threats can have on a location, an organization, an event, a community, and personnel can be dangerous and costly, even if no explosive device is present. Although not a new tactic, recent statistics reveal a disturbing increase in bomb threats across the nation. Bomb threat activities increased by 35% from 2021 (1,876) to 2022 (2,538), and by an additional 25% from 2022 to 2023 (3,164).[1] This guidance document provides an overview of bomb threats and some recommended practices to mitigate the impacts associated with these threats.

UNDERSTANDING BOMB THREATS

The primary reason for employing bomb threats when no explosive device is present, is to disrupt, distract, and harass. Perpetrators generally want to disrupt normal operations, and threats of violence that generate panic can be an effective method. Once in a state of anxiety, an organization is at much higher risk for personal injury, property damage, and operational disruption. The most common targets of bomb threats include schools, government facilities, commercial businesses, healthcare facilities, and faith-based organizations. Bomb threats also have cascading impacts on communities by placing strains on first responders and emergency management activities draining public resources. Bomb threats are mostly received via phone, but are also made in person, via email, social media, written note, or other means. Every bomb threat is unique and should be handled in the context of the facility or environment in which it occurs.

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

Bomb Threat Checklist

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)

ASSESSING THE BOMB THREAT

A crucial component of bomb threat management is the ability to assess the risk level of the threat. Because most threats prove to be false, a Decision Maker must be able to determine how serious a threat should be taken. All threats should be carefully assessed. One must consider the facts and context to conclude whether there is a possible threat. While it is difficult to decide on authenticity, consideration should be given to the following contributing factors.

- *Level of realism.*
- *Plausibility.*
- *Directness.*
- *Amount of time between threat notification and reported timing of the event.*
- *Exact wording of the threat (e.g., descriptions that show knowledge of the site location or employees and repetitive or motivating statements).*
- *Prior acts or threats against this or similar facilities.*
- *Current events regarding this or similar facilities.*
- *Individuals or actions at the site.*
- *Accessibility of the site.*
- *Occupants of the site.*
- *Danger in evacuation areas.*

Different threat levels correspond to different courses of action. These actions may include monitoring the situation, lockdown and search, or evacuations as determined during the evaluation. For example:

- **Minimal threat:** assess the threat and discount it based on experience (e.g., the caller has made multiple baseless threats and threat does not contain new or specific details).
- **Low threat:** assess and determine that the threat of an existing device is low and lock down the site location to ensure no suspicious items enter the site location. If a suspicious item is discovered, the threat is elevated, and an evacuation may be needed.

- **Moderate threat:** assess the threat, determine the realistic potential of a suspicious device, lockdown the site location and conduct a full or partial search for a device. If a suspicious item is discovered, the threat is elevated, and an evacuation may be needed.
- **High threat:** assess that the threat is specific/realistic and conduct a partial or full evacuation of the site location.

REPORTING THE BOMB THREAT

- Retain all information regarding the incident (such as usernames, email addresses, websites, phone numbers, or names of platforms, etc.) and report it to local law enforcement.
- If a suspicious item is discovered or the threat is elevated, it should be treated as an emergency by contacting 911.

RESOURCES AVAILABLE

- **CISA.GOV Bomb Threat Resources and Tools** (Bomb Threats | CISA) – Online resource for bomb threat products, training offerings, and resources that help with preparation and response options in the event of a bomb threat.
- **The Technical Resource for Incident Prevention** (TRIPwire) – A collaborative, online information-sharing and resource portal for the nation's security and emergency services professionals. It combines expert analyses and reports with relevant documents, images, and videos to help users anticipate, identify, and prevent IED incidents.