TRIPwire
tripwire.dhs.gov

TAB TRIP*wire* Awareness Bulletin

Responding to Mass Bomb Threat Campaigns

This TRIP*wire* Awareness Bulletin (TAB) provides resources for a managed response to bomb threat campaigns; information on previous mass bomb threat campaigns; and statistics on devices discovered following bomb threats. There are best practices for responding to bomb threats and making informed risk management decisions that address each risk level appropriately and are optimal for personnel and facilities. The Cybersecurity and Infrastructure Security Agency (CISA) focuses on implementing measures to keep people safe and mitigating the impacts of events.

Mass bomb threat campaigns are a reminder that bomb threats pose a serious disruption within local communities, as well as to public and private sectors across the United States.

- They have a psychological impact, disrupting lives and creating fear, uncertainty, and sometimes panic. With multiple threats to similar targets, the psychological and operational impact can be increased.
- They have an operational impact—causing activities to halt, harming commerce, and draining the resources of law enforcement and other first responders.
- Electronically disseminated mass bomb threats can target specific types of infrastructure on a national level (election polling locations, institutions of higher education, medical facilities, etc.) to enhance the impact and create cascading consequences.
- Mass bomb threats typically lack specificity or make grand claims (e.g., “there is a bomb in every major city.” Threats are typically sent by email or phone and calls may use an automated voice.
- Unsubstantiated bomb threats may also create complacency that can lead to increased vulnerability when actual devices are present.

Mass Bomb Threat Campaigns

- **Bomb Threats Targeting Historically Black Colleges and Universities (HBCUs) – 2022:** In January and February 2022, a total of 65 bomb threats were reported against HBCUs nationwide, resulting in campus evacuations and lockdowns. The FBI has identified persons of interests and has ongoing investigations in the bomb threats.
- **Bitcoin Bomb Threat Campaign – 2018:** On 13 December 2018, multiple infrastructure sites in the U.S., Canada, Australia, and New Zealand received over 3,000 bomb threats via emails from an unknown sender, which claimed that an unspecified explosive device had been emplaced in the recipient’s location and would function if the recipient failed to send $20,000 in Bitcoin to a designated web address.
- **Jewish Community Bomb Threat Campaign – 2017:** In early 2017, a wave of more than 2,000 bomb threats were made against Jewish Community Centers in the U.S., UK, Australia, New Zealand, Norway, and Denmark. In March 2017, two individuals were arrested on separate charges of making a number of the bomb threats and were later convicted and sentenced.

Assessment

Data from past bomb threat campaigns shows that virtually all such threats are unsubstantiated. The vast majority of the reported bomb threats referenced above were harmless, and many were perpetrated by students without the intent to physically harm others. Numerous studies show direct bomb threats rarely involve an actual device. Open source data shows that from 2017 – 2021, of the 6,071 identified bomb threat incidents, only 3 (0.05%) resulted in an actual device found. However, the time and resources allocated to the threat responses have been a major burden in bomb threat campaigns. This product seeks to raise awareness and provide resources to law enforcement and Federal, State, Local, Tribal, and Territorial security officials, so that they might properly assess and respond to any future bomb threat campaigns. All threats should be carefully evaluated. One must consider the facts and context, and then conclude whether there is a possible threat.

- **Low Risk**: A vague and indirect threat that poses a minimum risk to the victim or public safety.
- **Medium Risk**: A threat that is direct and feasible and could be carried out, although it may not appear entirely realistic.
- **High Risk**: A threat that is direct, specific and realistic and poses an immediate and serious danger to the safety of others.

Important: Every bomb threat requires professional judgment and should be handled in accordance with the facility's needs. Site Decision Maker(s) and administrators should periodically review Federal guidance and work with local first responders to establish a Bomb Threat Response Plan that addresses each risk level appropriately and is optimal for their building(s) and personnel.

CISA OBP Key Resources

CISA OBP offers the following **services, training courses, and information** to help facilities and the public prepare for bomb threats and take appropriate action:

- "What to Do: Bomb Threat Resources" webpage offers guidance and resources with in-depth procedures for either bomb threats or suspicious items to help you prepare and react appropriately during these events.
- We offer the public these free short videos that provide tips on reacting to bomb threats:
  - ◊ *CISA's Critical Resources for Handling Bomb Threats* describes the wide array of critical resources that OBP offers for free to help members of the public and others effectively respond to bomb threats.
  - ◊ What to Do: Bomb Threat video demonstrates the procedures you should follow during a bomb threat and helps you prepare and react appropriately.
  - ◊ What to Do: Suspicious or Unattended Item video demonstrates how you can determine whether an item is suspicious (i.e., a potential bomb) or simply unattended, and helps you prepare and react appropriately.
  - ◊ What to Do: Bomb Searches video describes basic bomb search procedures to use once the determination has been made that a search is warranted, and authorities have been notified. It demonstrates in detail the room, route and area search techniques that can be applied to any facility.

CISA OBP Key Resources

We also offer a wide variety of free online training courses on those specific subjects and more:

- Bomb Threat Preparedness and Response (AWR-903) – **1-hour Online**

  Web-Based Course. Description: Online independent study training that uses interactive exercises and case histories of what happened during bombing incidents to familiarize participants with the steps necessary to prepare for and respond to a bomb threat.

- Response to Suspicious Behaviors and Items (AWR-335) – **1-hour Virtual Instructor-Led Course. Description:** Provides participants with a foundational introduction to recognizing and responding to 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 to whom to report it.

- Bomb Threat Management (BTM) Planning (MGT-451) – **1-day In-Person Course. Description:** Provides participants foundational knowledge on the DHS risk management process and bomb threat management planning. It gives participants opportunity to apply this knowledge to develop a bomb threat management plan.

- Improvised Explosive Device (IED) Search Procedures (PER-339) – **1-day In-Person Course. Description:** Introduces participants to basic, low risk search protocols. It provides participants the information needed to create a search plan for their facility or special event and allows them to perform IED searches of a facility, an area and a route

- The DHS-DOJ Bomb Threat Guidance is a quick reference guide that provides site decision-makers with guidelines to react to a bomb threat in an orderly and controlled manner.

- The DHS-DOJ Bomb Threat Stand-Off Card provides standard distances for safety during a bomb threat if you must shelter in place or evacuate.

- OBP's Bomb Threat Procedures & Checklist helps employees at schools, commercial facilities and elsewhere respond to a bomb threat in an orderly and controlled manner with first responders and other stakeholders.

- The Suspicious or Unattended Item postcard helps you safely determine if an item is a serious threat, or just unattended.

- TRIP*wire* is OBP's free, online information and resource sharing portal that offers best practices; preparedness information; and reports about evolving improvised explosive device tactics.

Disclaimer

This product is based primarily on available open-source reporting and unclassified DHS reporting or finished products. Due to the nature of open-source intelligence (OSINT) collection, this data may not reflect all incidents during the stated period. The provided open-source data is derived from news, social media, and/or other media, including the deep/dark web, and is verified source material to the extent possible. It does not include classified or law enforcement sensitive information. It should be noted that incidents that received a response from law enforcement, first responders, or other authorities are frequently reported only through official channels, such as locally held police logs, because of the nature of criminal investigations. Therefore, some information may not be available and/or captured in the data used to compile this report. Nonetheless, the available records do provide a significant and representative sample of reported events in open-source reporting.

WARNING

Do not disturb suspected IEDs. Call your local explosives disposal unit and law enforcement.

This document was prepared by **DHS Office for Bombing Prevention's TRIP*wire* Team**. For source material and additional information please visit tripwire.dhs.gov.
For questions regarding this product please contact the **TRIP*wire* Help Desk**: tripwirehelp@dhs.gov