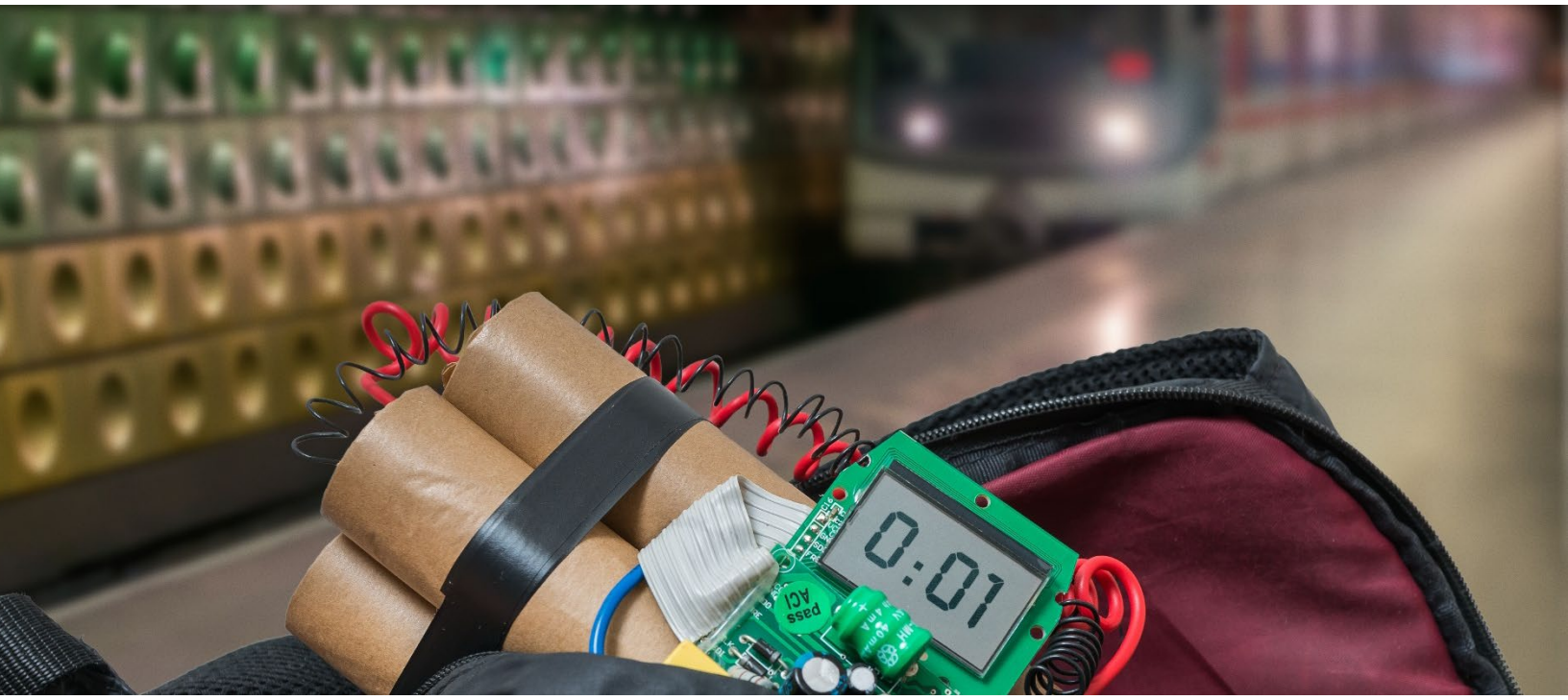


BOMB THREAT GUIDE

Version: 1.0

Disclaimer: This guide is intended for use as a reference for training and operations in preparing for and responding to potential criminal/terrorist activities. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. The opinions expressed in this Guide does necessarily reflect the positions or policies of DHS. Reference to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. DHS does not endorse any individual, enterprise, product, or service. DHS does not mandate or prescribe practices, models, or other activities described in this Guide. Implementation of the options for consideration identified is purely voluntary, and a decision not to implement these voluntary measures will not result in any enforcement action by DHS. Reference to any specific option for consideration does not constitute endorsement of that option. This Guide is not intended to, and does not, create any legal rights. Incidents or threats should be reported directly to your local law enforcement agency or by dialing 911. The information contained in this document is not all inclusive and should be applied in conjunction with previous training, experience, and standard procedures and policies. Be aware that each situation presents its own unique circumstances. In all cases, use common sense and do not conduct any operations that would place personnel, equipment, or facilities at risk. Not all methods will be appropriate for use in all situations. Leaders, mangers, and legal counsel should work together to ensure that these methods are employed in a manner consistent with legal requirements, the current threat level, and the facility's security policy. Users of this Guide should not substitute their judgment for a State, local, Tribal, or territorial law enforcement's laws. This Guide should not and does not replace law enforcement officer training for behavior indicators.

Contents

01

SECTION 1 - INTRODUCTION TO THIS GUIDE

These guidelines, provided by the Cybersecurity and Infrastructure Security Agency's (CISA) Office for Bombing Prevention (OBP), are developed to assist Decision Makers in responding to bomb threats in an orderly and controlled manner.

OBP leads the Department of Homeland Security's (DHS) efforts to implement the National Policy for Countering Improvised Explosive Devices (National Counter-IED policy) and enhance the nation's ability to prevent, protect against, respond to, and mitigate the use of explosives against critical infrastructure; the private sector; and federal, state, local, tribal, and territorial entities. **For more information, visit** cisa.gov/obp

BOMBING INCIDENTS

Before getting into the logistics of managing a bomb threat, it is important to understand common components and trends related to bombing incidents. While every incident is unique, each of the following plays a role in the development, delivery, and execution of a bombing attack:

- **Perpetrators:** bombs can be used by anyone, from everyday criminals to religious or political extremists. The intent of a bombing is oftentimes to inflict mass casualties.

- **Targets:** commercial and religious facilities have long been attractive targets for criminals and terrorists, both domestically and abroad, as they are usually easily accessible and heavily populated.

- **Devices:** Improvised Explosive Devices (IEDs) are readily accessible to terrorists and criminals due to the availability of common everyday items that can be repurposed as bomb-making materials. IED design and employment has become increasingly sophisticated and transnational, as terrorist organizations adapt their tactics to suit today's global security situation. Pipe bombs and over-pressure devices (such as bottles filled with volatile chemicals or pressure cookers containing explosive materials) are commonly encountered in the United States. Fragmentation from the container or enhancements, such as the addition of nuts and bolts, may be present to increase the damage of the device. Regardless of the type of device, they can cause substantial damage to property and a significant loss of life.

PRIOR TO THREAT:

- ✓ Plan and prepare
- ✓ Develop a Bomb Threat Management (BTM) Plan
- ✓ Provide BTM Plan training to all personnel

IF THREAT IS RECEIVED:

- ▪ Conduct threat assessment
- ▪ Execute appropriate actions outlined in BTM Plan

BOMB THREATS

While bombing incidents pose an obvious danger to people and organizations, threats themselves can impose significant impacts as well. **A bomb threat is any communication that indicates the presence of, or intent to detonate, an explosive device.** The impact that bomb threats alone can have on a site location, an organization, events, and the personnel within can be dangerous and costly, even if no explosive device is present.

INTENT

Depending on the motivation of the perpetrator, the intent behind any bomb threat can differ.

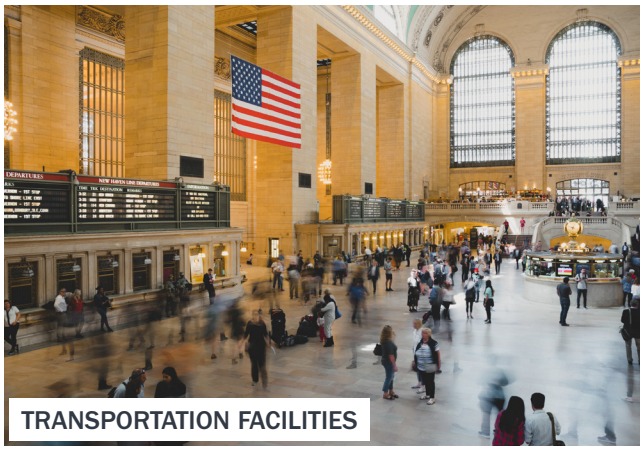
- **Disruption:** This is the most common cause of a bomb threat. Whether to disrupt, distract, or harass, they can be an effective way to interfere with an organization's operations.
- **Extortion:** Less common are bomb threats that serve to extort something, especially money, through force or threat.
- **Warn:** The least common are bomb threats that serve to warn people of an explosive device.

RECIPIENTS

In the United States, the most common targets of bomb threats include:

- **Schools:** including K-12 and institutions of higher education.
- **Commercial businesses:** including financial institutions, chemical facilities, and commercial department stores.
- **Courthouses.**
- **Government facilities:** including federal and state offices as well as election and polling places.
- **Medical facilities:** including hospitals, abortion clinics, urgent cares, etc.
- **Private residences.**
- **Transportation facilities:** including airports, railways, etc.
- **Faith-based organizations:** including churches and community centers.

SCHOOLS



TRANSPORTATION FACILITIES

While each of these may vary in rank order, they are common recipients of bomb threats year after year.

COMMERCIAL BUSINESSES

IMPACT

Bomb threats can severely impact organizations and personnel regardless of the perpetrator's intent. They can have a detrimental effect on morale and employee safety, and strain first responder resources. Perpetrators generally want to disrupt normal operations, and 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. Having a BTM Plan can reduce panic and ensure your organization is prepared to respond to a potentially dangerous situation. Some cascading impacts include, but are not limited to:

- **Operational impacts:** halting activities, shutting down and subsequently restarting operations, customers may not receive their products, supply chain disruption, loss of timely production or services, loss of instructional time (for schools), life-saving medical treatments delayed, property damages and cost to repair or replace.
- **Financial strains:** not just to a site location, but to public safety and first responders, and the community at large.
- **Community strains:** on first responders, and emergency management resources halting activities, and draining public resources.
- **Psychological impacts:** longer-term effects may disrupt lives, create fear, and uncertainty. May also include a decline in public trust, productivity, and morale.
- **Panic:** caused by fear of the known or the unknown and is one of the most contagious human emotions. Panic can be considered the ultimate achievement of a bomb threat caller.

Once a state of panic has been reached, the potential for personal injury and property damage is dramatically increased.

SECTION 2 - PLANNING AND PREPARATION

Having a BTM Plan may ensure that your organization is better protected from the worst effects of a bomb threat, while also increasing safety 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.
4. Minimize the consequences of a potential attack or threat on personnel and property.

DEVELOP A BOMB THREAT MANAGEMENT (BTM) PLAN AND TRAIN

A site location's Emergency Response Plan outlines mitigation efforts to counter threats or identified risks. It also outlines precautionary measures and predefined guidance to deal with all threats. It is essential to include bomb threat management as one of the components of that overall emergency response planning.

PLANNING CONSIDERATIONS

Always coordinate with local law enforcement and first responders where possible to ensure efficient and effective handling of a bomb threat.

DESIGNATION OF TEAM MEMBER RESPONSIBILITIES

The number of members and responsibilities assigned to the team can vary by organization, depending on the size and complexity of the site location. These circumstances may call for the Decision Maker to perform the duties of each role, or delegate as the situation demands. It is recommended to identify team members in advance, but some may become involved at the time of the incident. In addition, multiple roles can be assigned for specific incidents or situations. Regardless of the team makeup, the BTM plan should clearly outline roles and responsibilities. The more knowledgeable individuals are during an event, the better prepared the team will be to implement an effective and efficient response. Alternates should be assigned to team members to address personnel turnover, vacation, or illness.

DESIGNATE TEAM MEMBER RESPONSIBILITIES

- ✓ Develop clear-cut primary and alternate levels of authority (referred to in this document as “Decision Makers”).
- ✓ Identify Evacuation Teams and Search Teams.

Common team member roles include:

- **Receiving party:** the person who first receives or becomes aware of the threat.
- **Decision Maker:** the person who oversees the plan’s activation and makes the decisions on how to manage the incident.
- **Law enforcement liaison:** the person who bridges the Decision Maker and any law enforcement response.
- **Search team leader:** the person who oversees the search team members.
- **Search team:** the individuals who conduct the search for the threat as directed by the Decision Maker.
- **Evacuation team leader:** the person who oversees the evacuation team members.
- **Evacuation team:** those individuals who lead people to assembly areas.
- **Evacuees:** those individuals who are being evacuated from a site location (e.g., employees, customers, visitors, etc).
- **Runners:** those individuals who transport equipment or messages between teams, leaders, and the Decision Maker.

THE BOMB THREAT MANAGEMENT PLAN

This plan assists in determining appropriate courses of action on a case-by-case basis in light of all available information. BTM Plans will vary in length and detail depending on the nature, size of the site location, and the assessed risk, but there are core elements that should be included in every BTM Plan including:

- **A procedure for handling a bomb threat**
  Most bomb threats are answered by a recipient on the phone with a publicly listed number.
  [REFERENCE PAGE 15]

- **A procedure for assessing the threat level**
  The person who received the threat briefs the Decision Maker. The Decision Maker considers the information provided by the person receiving the threat when assessing the threat.
  [REFERENCE PAGE 18]

- **A procedure for response: a search and evacuation plan**
  A plan for search and evacuation is critical to ensure the safety of all individuals.
  [REFERENCE PAGE 22]

- **Instructions for restoring normal operations after an incident or threat**
  Every organization should have a continuity of operations plan following a bomb threat/incident. Extended disruption of operations can have severe impacts to an organization.
  [REFERENCE PAGE 13 & 26]

STEP 1— GATHER THE TEAM

Management typically designates the planning team. This team should be composed of personnel specializing in security and emergency planning to include any local responders who may interact with response teams in case of an incident. The planning team should bring together various expertise to develop a comprehensive plan.

STEP 2— UNDERSTAND THE SITUATION

Plan to understand your specific environment and situation. Keep in mind that this is an ongoing process. Most information related to the environment and its specific risks will be gathered through the vulnerability assessment/risk management process. Once information on your situation is collected, you must analyze how it affects your developing plan. OBP's TRIP*wire* can be a valuable online resource for staying current on threats in your region or business sector.

STEP 3—
DETERMINE GOALS AND OBJECTIVES

With your team gathered and your specific situation understood, you are now ready to determine your search and risk mitigation priorities. The Decision Maker and planning team can then use these priorities to identify goals and objectives for the BTM Plan.

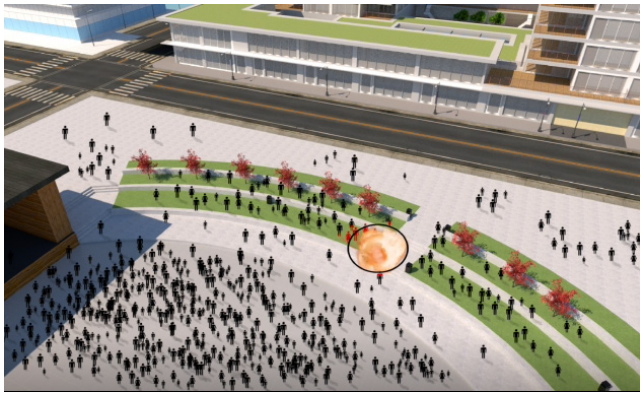
- **Goal:** a statement that describes the overall intended outcome. An example of a goal is to, "Safely manage and resolve an incident."

- **Objective:** define the actions needed to accomplish the goal. They must support achieving the plan's priorities. Objectives must be specific and include identifiable actions. An example of an objective is to, "Maintain an effective perimeter."

STEP 4—
PLAN DEVELOPMENT

With goals and objectives in place, you are ready to develop your plan. It should be a comprehensive plan, including topics not limited to:

- Protection of visitors and employees.
- Reporting of suspicious activities, items, or people.
- Access and screening procedures, to include any mail and vehicle inspection.
- Special event procedures.
- Employee training and awareness.



STEP 5—
PREPARE, REVIEW, AND GAIN APPROVAL FOR THE PLAN

The draft plan should be reviewed for discrepancies and presented to management for approval. Once approved, the plan should be circulated to the entire response team and all personnel should be educated on their role in an incident response.

STEP 6—
IMPLEMENT, MAINTAIN, AND TRAIN

Once a plan has been written, reviewed, and exercised, it is essential that the planning team continue ongoing evaluations and make adjustments where necessary. Revisions should be circulated to all personnel involved in the BTM Plan. Having a viable and exercised BTM Plan will help ensure its effectiveness.

DETERMINE OTHER PROCEDURES

PORTABLE COMMAND POST

The Decision Maker should move control operations to the command post once the BTM plan is initiated. Locations of the command post need to be flexible and consider standoff distances.

To maintain a functioning command post if it needs to be relocated, a portable command post kit should include:

- ✓ Copies of all emergency response plans.
- ✓ Names and numbers for all team members.
- ✓ Numbers for law enforcement and emergency response liaisons.
- ✓ Names and numbers of department/ adjacent site location points of contact if relevant.
- ✓ Internal extension numbers.
- ✓ Utility and service numbers.
- ✓ Complete set of master keys, coded to rooms with printed key list.
- ✓ A copy of the site location layout and floor plans marked with evacuation routes and search zones.
- ✓ Cell phones with fresh batteries and and a charging station for devices.
- ✓ Flashlights.

COMMUNICATION PLANS

Determine how communications will be handled within and outside of your team, including how the Decision Maker will be reached and how law enforcement will be contacted.

Determine how runners will be utilized, and how their safety will be ensured.

PROCEDURES FOR ACCESSING, SHUTTING OFF, AND REACTIVATING UTILITIES

Identify situations in which utilities will need to be accessed or shut off, depending on the industry and type of building your organization is dealing with.

Determine how these utilities will be reactivated safely after the threat is resolved.

RE-ENTRY PROCEDURES

Every organization should have a plan in place following a bomb threat/incident.

- Determine when the building will be reentered, and what parameters need to be met to ensure that the site location is safe.
- Identify how the site location will be reoccupied while avoiding any safety hazards. This is especially important in larger organizations where re-entry may present crowding hazards.
- Initiate action to recall evacuees using a phased approach if necessary (e.g., security should be back in place before operations are restored; employees should enter before the public, etc.).

SPECIAL CONSIDERATIONS

An organization may need to consider other aspects in their BTM plan specific to their needs. As an example, some organizations can't fully stop essential operations and will have to consider who and what remains behind. Some considerations can include to:

- Address any hazards resulting from disruption of safe process operations, such as those needing to be shut down in stages before all employees can evacuate to the greatest extent.
- Contact utility companies to shut down or restore these services if preventative measures were taken to minimize site location hazards or impact to operations.

PROTECTIVE MEASURE PREPARATIONS AND CONSIDERATIONS

ACCESS CONTROL AND IDENTITY VERIFICATION

Specific protective measures can be put in place to protect from IED threats by controlling entry into designated areas and detecting unauthorized individuals trying to gain access to a site location or event. Effective access control can prevent an IED from being placed in critical areas. Entry control points and access control measures should address vehicles and pedestrians, including visitors, deliveries, public transportation, and off-facility emergency response vehicles.

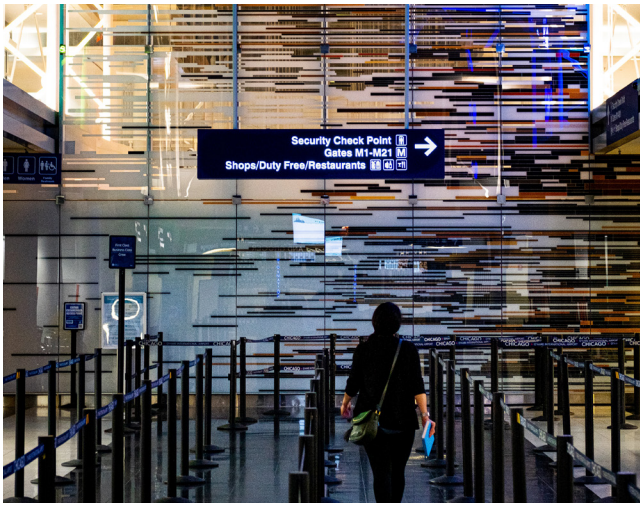
PHYSICAL PROTECTIVE MEASURES

Physical protective measures describe objects, structures, and tools you may use to mitigate risk and damage from IED explosions.

The distance from an IED is a significant factor in determining potential damages and injuries from the explosion. The primary strategy for preventing, protecting, mitigating, and responding to explosive threats is to maximize standoff distance.
[REFERENCE PAGE 35]

Remember to:

- Keep exits unobstructed.
- Ensure stocked emergency toolkits are available.
- Ensure adequate internal and external emergency lighting is present.



ACCESS CONTROL CONSIDERATIONS

CONTROL ACCESS:

- ✓ Implement strict master key control.
- ✓ Utilize electronic surveillance to verify personnel identity to control access, perform surveillance, and assess alarms.
- ✓ Inspect incoming parcels: There are a range of potential threats that can be introduced to a site location by way of the mail center. The mail center screening process must be able to identify threats and eliminate or reduce the risk they pose to personnel and property.

RISK MANAGEMENT PROGRAMS AND ACTIVITIES

Protective measures include more than just physical resources and systems. You can undertake several programs and activities within your area of responsibility that can lower risk from bomb threats, suspicious items and behaviors.

Remember to:

- Have replacement equipment on hand in case existing equipment fails.
- Safeguard confidential material.
- Train and communicate with personnel on their roles, responsibilities, and equipment assigned, as defined by the BTM plan.

[ADDITIONAL TRAINING IS AVAILABLE THROUGH THE CISA OFFICE FOR BOMBING PREVENTION.]

SECTION 3 - RECEIVING A THREAT

Because the threat itself can be a key piece of evidence for both the Decision Maker and local law enforcement, it is important that your response to received bomb threats follow specific procedures. Because anyone in your organization could be the recipient of a bomb threat, members of your organization must be trained on these procedures. These procedures will vary based on how the threat is received.

TELEPHONE

- ✓ Remain calm and DO NOT HANG UP.
- ✓ If possible, signal other staff members to listen and notify Decision Makers and authorities to enact the organization's BTM Plan.
- ✓ If the phone has a display, copy the number or letters on the window display.
- ✓ Pay close attention to the message, write down the exact wording of the threat.
- ✓ Keep the caller on the line for as long as possible and use the Bomb Threat Checklist [REFERENCE PAGE 34] to gather as much information as possible.
- ✓ Record, if possible.
- ✓ Attempt to listen for any background noises.
- ✓ Note the caller's voice/accent or use of any idioms.
- ✓ Fill out the Bomb Threat Checklist immediately.
- ✓ Be available for interviews with the emergency response team and law enforcement.

WRITTEN

- ✓ Handle the document as little as possible.
- ✓ Notify the Decision Maker and authorities.
- ✓ Rewrite the threat exactly as is on another sheet of paper and note the following:
  - Date, time, and location document was found.
  - Any situations or conditions surrounding the discovery/delivery.
  - Full names of any personnel who saw the threat.
- ✓ Secure the original threat; DO NOT alter the item in any way:
  - If small or removable, place in a bag or envelope.
  - If large or stationary, secure the location.

INTERNET, SOCIAL MEDIA MESSAGING, OR EMAIL

- ✓ Do not turn off or log out of the account.
- ✓ Leave the message open on the device.
- ✓ Print, photograph, take a screenshot, or copy the message and subject line.
  - Note the date and time.
- ✓ Notify the Decision Makers and authorities.

VERBAL OR IN PERSON

- ✓ Be aware of a psychologically distressed state in the person delivering the threat.
- ✓ Maintain distance from the individual.
- ✓ Contact the police immediately.
- ✓ If the perpetrator leaves, note which direction they went.
- ✓ Notify the Decision Makers and authorities.
- ✓ Write down the threat precisely as it was communicated.
- ✓ Note the description of the person who made the threat:
  - Name (if known).
  - Race.
  - Gender.
  - Type and color of clothing.
  - Body size (height/weight).
  - Hair and eye color.
  - Voice (loud, deep, accent, etc).
  - Any other distinguishing features.

OTHER METHODS

Other less common methods of receiving a threat include drawings or through a third party such as the police or the news media.

A NOTE ON MASS BOMB THREATS

Increasingly, bad actors are conducting strategic campaigns where multiple bomb threats sometimes simultaneously target infrastructure. Whether these mass bomb threats are made at multiple locations, or to one location over a length of time, **mass bomb threat campaigns can have significant impacts.** [REFERENCE PAGE 37]

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 (i.e. “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 explosive devices are involved.

04

SECTION 4 - THREAT ASSESSMENT

A crucial component of bomb threat management is the ability to assess a threat for risk. Because most threats prove to be false, a Decision Maker must be able to determine how serious a threat should be taken.

While it is difficult to decide on authenticity, consideration should be given to the following contributing factors:

- Level of realism.
- Plausibility.
- Directness.
- Immediacy of the threat as it was received.
- Exact wording of the threat (e.g., descriptions that show knowledge of the site location or employees and repetitive or motivating statements). If the threat shows knowledge of the site location, it is more likely that an explosive device is present.
- 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.
- Advice of local law enforcement.

CONSIDERATIONS FOR DECISION MAKERS

All threats should be carefully assessed. One must consider the facts and the context and then conclude whether there is a possible threat.

While there is no absolute method of determining the credibility of a threat, below are some parameters for helping Decision Makers conduct an informed assessment:

CONSIDERATIONS FOR DECISION MAKERS

LOW RISK

- Lacks realism
- Ability to carry out threat is questionable

MODERATE RISK

- Feasible and sufficiently detailed
- Includes time and place

HIGH RISK

- Highly specific locations or names
- Threat is related to recent events

LOW RISK

The primary indication that a bomb threat is low risk is if it lacks realism. Ask yourself how likely is it that the threat being presented could actually be carried out? Other indications that a threat is a low risk include:

- The threat poses a minimum risk to personnel and property.
- There is an obvious reason to believe the motive is disruption.
- The threat is vague and indirect, and information is inconsistent, implausible, or lacks detail.
- The threat was indirectly delivered (located on the wall or by email).
- The caller has made numerous, previous threats or is known.

LOW RISK

LACKS REALISM

A threat that poses a minimum risk. Probable motive is to cause disruption.

- **Vague and indirect**
- **Inconsistent, implausible, lacks detail**
- **Known or repeat caller**
- **Discovered**

CONSIDERATIONS FOR DECISION MAKERS

LOW RISK

- Lacks realism
- Ability to carry out threat is questionable

MODERATE RISK

- Feasible and sufficiently detailed
- Includes time and place

HIGH RISK

- Highly specific locations or names
- Threat is related to recent events

MODERATE RISK

The more realistic or specific a threat is, the more seriously it should be taken. Moderate threats are feasible but unlikely, but they are more specific about methods and places than low risk threats. Other indications that a threat poses moderate risk include:

- The threat is direct and feasible.
- The wording of the threat suggests thoughtful planning as to how the act will be carried out.
- The threat may indicate possible place and time.
- The threat does not include strong indication of preparatory steps, although there may be some indirect reference pointing to that possibility.
- Indication the perpetrator has details regarding the availability of components needed to construct an explosive device.
- Increased specificity to the threat (e.g., “I’m serious!” or “I really mean this!”).

MODERATE RISK

INCREASED LEVEL OF REALISM

Threat that could be carried out, although it may not appear entirely realistic.

- **Direct and feasible**
- **Wording suggests some forethought**
- **Place and time**
- **No strong indication of preparatory steps**
- **Bomb-making knowledge**
- **Increased specificity**

CONSIDERATIONS FOR DECISION MAKERS

LOW RISK

- Lacks realism
- Ability to carry out threat is questionable

MODERATE RISK

- Feasible and sufficiently detailed
- Includes time and place

HIGH RISK

- Highly specific locations or names
- Threat is related to recent events

HIGH RISK

Specific and feasible threats present the most risk, especially if the threat is delivered in person. Other indications that a threat should be taken seriously include:

- The threat poses an immediate and significant danger to the safety of others.
- The threat is direct, specific, and realistic; it may include names, times, and/or location of the device.
- The perpetrator provides their identity and threat suggests concrete steps have been taken.
- The perpetrator indicates practice with a weapon or surveillance of the intended victim(s).
- The threat may be used as a warning by providing specific details of an explosive device or attempt to extort something, such as money.

HIGH RISK

SPECIFIC AND REALISTIC

Threat appears to pose an immediate and serious danger to the safety of others.

- **Direct, specific, realistic**
- **Provides identity**
- **Concrete steps taken**
- **Indication of practice or surveillance**

04

As you assess the risk of a bomb threat, take comfort that most threats prove to be false. However, you always want to be sure to look for signs and follow your BTM Plan closely to avoid a tragic outcome.

05

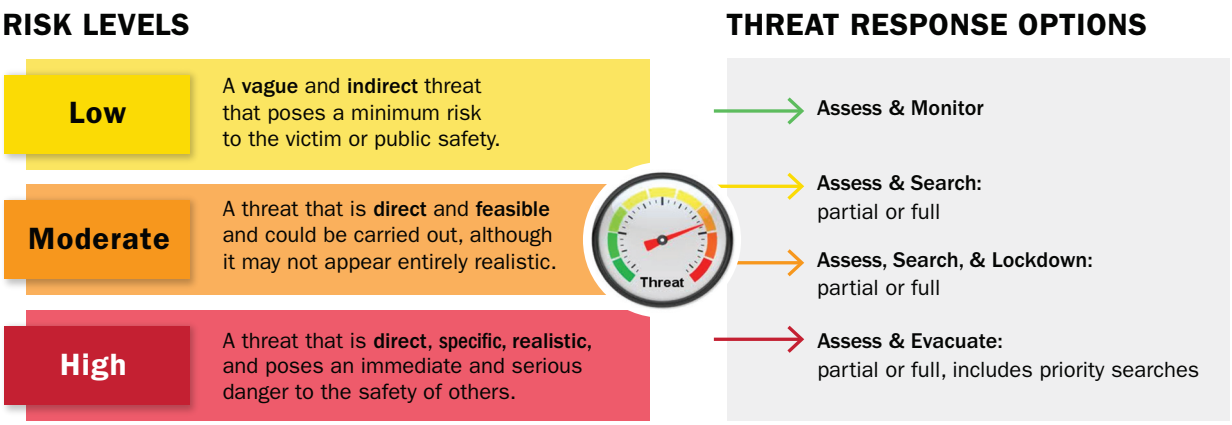
SECTION 5 - RESPONSES

Assess the threat by determining whether it is low risk, moderate risk, or high risk.
[REFERENCE PAGE 18]
Different threat levels correspond to different courses of action. For example:

- **Minimal threat:** assess the threat and discount it based on experience (caller has made multiple baseless threats and threat does not contain new or specific details).
- **Low threat:** assess the threat, 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.
- **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.
- **High threat:** assess that the threat is specific and realistic and conduct a partial or full evacuation of the site location.

CONSIDERATIONS FOR DECISION MAKERS

- Limit access to site location.
- Review BTM Plan.
- Conduct Threat Assessment.
- Determine course of action warranted based on Threat Assessment.
- Immediately contact local law enforcement if required.



RESPONSE OPTIONS

ASSESS AND MONITOR

The Decision Maker determines that the information received does not indicate that the threat is sufficiently credible. Although a discounted threat means no action is taken, it is important to continue monitoring the threat and inform all relevant planning team members should new information indicate the threat is credible.

ASSESS & SEARCH

The Decision Maker may elect to conduct a partial or full search without a lockdown, garnering more time to assess whether the threat is credible. This determination should be based on the credibility of the threat and its corresponding course of action.

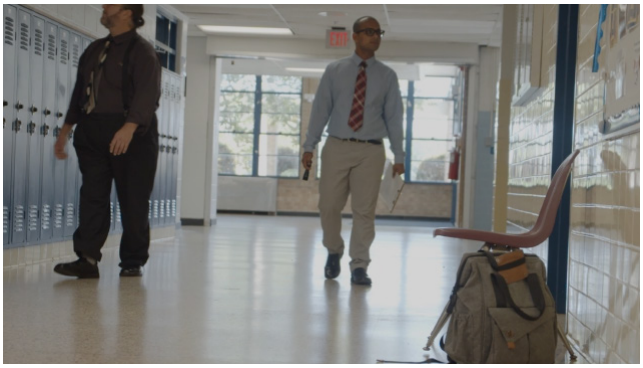
ASSESS, SEARCH, & LOCKDOWN

The Decision Maker determines that more time and information are needed to assess whether the threat is credible. They can elect to conduct a search which may include a partial or full lockdown by restricting entrance to the site location. This determination should be based on the credibility of the threat and its corresponding course of action.

ASSESS AND EVACUATE

The Decision Maker determines the threat is credible and the best approach is to evacuate after conducting priority searches. Even if a threat seems adequately credible, do not automatically evacuate. This could place evacuees in greater danger of an attack. Hostile actors have used bomb threats in the past to better target personnel.

Like lockdowns, they may elect to conduct a partial or full evacuation. A hospital, for example, may not be able to safely evacuate all patients and select to only evacuate high risk areas.



Lockdowns
Keep in mind that there are two types of lockdowns:

- Partial: a partial lockdown only affects a specific site location section. This prevents people from entering or exiting this area.

- Full: a complete lockdown prevents anyone from leaving or entering the site location.

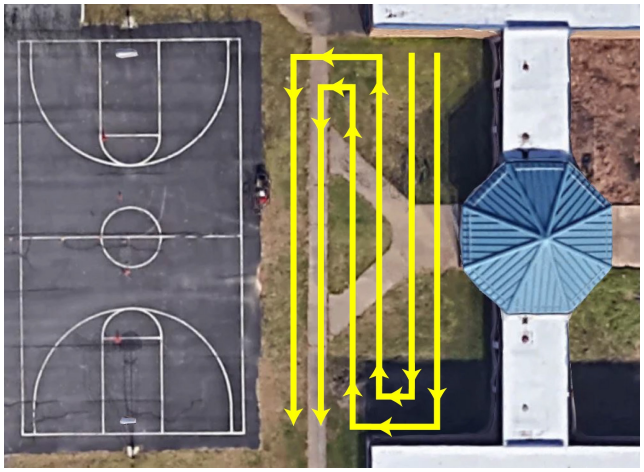
The type of lockdown you elect to use depends on the nature and credibility of the threat, whether you are conducting a search during the lockdown, and the specifics of your site location and environment. Keep in mind that it is wise to lockdown areas with high foot traffic during a search, so that devices are not placed in the area after the search is complete.

Searches
It is essential to have a predetermined approach and parameters for conducting a search in your BTM Plan.
[REFERENCE PAGE 10]

Identify or develop the following:

- ✓ Factors that determine if the search is conducted before or after evacuation.
- ✓ Search priorities.
- ✓ Roles and tasks to complete during search.
- ✓ Floorplans and outside area layout.
- ✓ Critical or vulnerable areas to search.
- ✓ Areas to search if evacuation is initiated.
- ✓ Tools and equipment needed for search team members.
- ✓ Basic procedures for a systematic and thorough search.
- ✓ Items to use for marking or securing cleared areas.
- ✓ Additional search resources that may be available offsite.

Searching for a potential explosive device is inherently dangerous. Whether or not an explosive device is found, the safety of your personnel is paramount. All search team members should have the floor plan of your site location with evacuation routes marked. They should prioritize evacuation areas, hazardous areas, and the identified target locations of the threat. Look for items that look out of place or suspicious. To ensure their safety, ensure the following guidelines are followed:



Bird's eye view of venue depicting systematic search.

- ✓ Minimize the use of wireless communications.
- ✓ Minimize the number of people participating in zone searches.
- ✓ Ensure all areas searched are marked and recorded.
- ✓ Thoroughly search all public areas, assembly locations, and exterior evacuation routes before evacuation.
- ✓ If an object is found, isolate it. If anyone can see the object, they are too close.
- ✓ Use safe and timely communication techniques with all individuals.
- ✓ Report accurate information to the search team leader.
- ✓ NEVER assume only one device is present.
- ✓ NEVER assume the time of detonation stated in the threat is accurate.
- ✓ NEVER touch, move, or cover a suspicious object.
- ✓ NEVER spend more time near a suspicious object than necessary.

Regardless of the threat assessment, your designated Decision Maker or the appropriate on-site supervisor is responsible for determining what action to take.

[ADDITIONAL TRAINING IS AVAILABLE THROUGH THE CISA OFFICE FOR BOMBING PREVENTION.]

Evacuations

If you determine that it is safe and necessary to evacuate, contact first responders and do the following:

- ✓ Use alternate evacuation routes only for those near a suspicious item.
- ✓ Select evacuation routes and assembly areas not in the vicinity of the suspicious item and ensure that these routes and assembly areas have been searched and cleared.
- ✓ Announce the need to evacuate AFTER evacuation routes and assembly areas have been searched and nothing is found.
- ✓ Notify police/fire/EMS of evacuation and request assistance.
- ✓ Advise all evacuees to remove all personal items (e.g., purses or backpacks).
- ✓ Account for all personnel and patients.
- ✓ Have the Evacuation Team confirm the site location is empty.
- ✓ Bring emergency kits and trauma kits, if available.

Re-entry

After evacuation, the Decision Maker must determine when re-entry can be safely conducted. These parameters should be outlined in your BTM Plan. When re-entry is conducted, consider how the site location can be safely entered, especially when crowding may occur. Likewise, the site Decision Maker should determine whether staff should search their work areas upon their return.

REMEMBER Your organization may need to consider other aspects of your BTM Plan that are specific to your needs. Some organizations can't entirely stop operations, and determinations will need to be made about who and what remains inside. Depending on these considerations, evacuations and restoring operations after an evacuation will need to be tailored to an organization's specific needs.

06

SECTION 6 - SUSPICIOUS ITEMS

Just as with the need to assess bomb threats, it is essential to assess all items (examples include bags, packages, and vehicles) within your site locations to determine whether they are suspicious or simply unattended. When deciding whether an item is suspicious, use the acronym **H.O.T.**:

[REFERENCE PAGE 36]

Is it HOT?

H: Is the item intentionally **Hidden**?

O: Is the item **Obviously** suspicious?

T: Is the item not **Typical** for your environment?

Unattended Items are anything that:

- Are not in someone's possession.
- Have no obvious signs of being suspicious.
- Do not correlate to any received threat.

CONSIDERATIONS FOR DECISION MAKERS

- Not all items are suspicious.
- An unattended item is anything not in someone's possession and where there are no obvious signs of being suspicious, especially if no threat was received.

06

A suspicious item is anything that is reasonably believed to contain explosives, an IED, or other hazardous material that requires a bomb technician to further evaluate it.

- Potential indicators can be threats, placement, or proximity of the item to people and valuable assets.
- Examples include unexplainable wires or electronics, other visible bomb-like components, unusual sounds, vapors, mists, or odors.

IF A SUSPICIOUS ITEM IS FOUND

- DO NOT touch, tamper with, or move the item.
- Immediately report item to the Decision Makers and local law enforcement/first responders.
- Decision Makers must:
  - ✓ Ensure area is secured. and cleared of personnel.
  - ✓ Notify Search Teams.
  - ✓ Ensure emergency responders are briefed.
- Evacuation & Search Teams should remain available to assist and inform evacuees, staff, and others.

ADDRESSING A SUSPICIOUS ITEM

Once an item has been identified as suspicious, you can use the acronym RAIN to recall the recommended steps involved in responding and neutralizing the threat of this item. RAIN stands for:

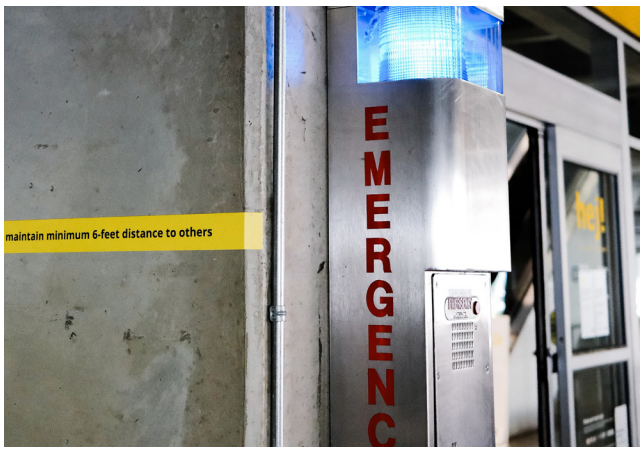
R: Recognize the Indicators of a Suspected Explosive Device: remember that Suspicious Devices are HOT (Hidden, Obviously suspicious, not Typical).

A: Avoid the Device or Item: do not touch the device. Move away from the suspected device or item immediately.

I: Isolate the Area: secure the perimeter of the area surrounding the device. If possible, wear protective equipment or use frontal and overhead cover in case of detonation.

N: Notify appropriate emergency services.

[REFERENCE PAGE 36]



07

SECTION 7 - CONCLUSION

When it comes to the threat of IEDs and bomb threats, having a clear, specific, and well-known plan in place can save lives and reduce disruptions. Take the time ahead of a threat to form a plan for your site location that contains all the details that you'll need when the time comes.

Every bomb threat should be individually assessed for risk factors based on a site location's needs. Decision Makers and administrators should periodically review federal guidance and work with local first responders to establish a BTM Plan that addresses each risk level appropriately and is optimal for their site location(s) and personnel.

08

SECTION 8 - GLOSSARY, REFERENCES, AND RESOURCES

BOMB THREAT GUIDE ACRONYM LIST

CISA Cybersecurity and Infrastructure Security Agency

IED Improvised Explosive Devices

BTM Bomb Threat Management

OBP Office for Bombing Prevention

TRIP*wire* Technical Resource for Incident Prevention wire

REFERENCES

Cybersecurity and Infrastructure Security Agency, Office for Bombing Prevention. (2022). Bomb Threat Management Planning Course, V3.

Cybersecurity and Infrastructure Security Agency, Office for Bombing Prevention. (2022). Bomb Threat Assessment for Decision Makers Course, V1.

Cybersecurity and Infrastructure Security Agency, Office for Bombing Prevention. (2022). Mass Bomb Threats Card, V1.

Cybersecurity and Infrastructure Security Agency, Office for Bombing Prevention. (n.d.). Bomb Threat Guidance, V2.

Department of Homeland Security. (2017, September). DHS Risk Lexicon.

Department of Homeland Security. (2011, November 10). Domestic Terrorism and Homegrown Violent Extremism Lexicon.

Department of Homeland Security. (2011, April). Risk Management Fundamentals.

Department of Homeland Security, Office for Bombing Prevention (2018, December). Security and Resiliency Guide: Counter-Improvised Explosive Device Concepts, Common Goals, and Available Assistance (SRG C-IED). https://www.dhs.gov/publication/security-and-resiliency-guide-and-annexes.

Department of Homeland Security, Office for Bombing Prevention (2018, April). Instructional Video: Explosive Effects and Blast Considerations for Person-Borne and Vehicle-Borne IED Events. https://tripwire.dhs.gov/video-library.

Department of Homeland Security, Office of Infrastructure Protection (2013, September). Protective Measures Guide for U.S. Commercial Real Estate.

Gundry, C. (2002, March). Chemical Plant Bomb Threat Planning Handbook. Retrieved from https://www.cisworldservices.org/wp-content/uploads/2002/03/CP_BOMB.pdf

Joint Counterterrorism Assessment Team (JCAT) Counterterrorism Guide for Public Safety Personnel. https://www.dni.gov/nctc/jcat/index.html.

Nationwide SAR Initiative (NSI). (2015, March). Suspicious Activity Reporting: Indicators and Behaviors. Revised 02/16. http://nsi.ncirc.gov.

U.S. Bomb Data Center (USBDC). 2015. Explosives Incident Report (EIR) 2015. Washington, DC: U.S. Department of Justice.

U.S. Defense Threat Reduction Agency and U.S. Joint Improvised Threat Defeat Organization. 2017. Improvised Explosive Device (IED) Technical Exploitation Lexicon, 5th Edition. May.

U.S. Department of Justice, U.S. Department of Homeland Security, & Major Cities Chiefs Association. (2008, June). Finding and Recommendations of the Suspicious Activity Report (SAR): Support and Implementation Project. June 2008. https://bja.ojp.gov/library/publications/findings-and-recommendations-suspicious-activity-reporting-sar-support-and

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
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected delivery
- Poorly handwritten
- Misspelled words
- Incorrect titles
- Foreign postage
- Restrictive notes

**** 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

V2

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

- ☐ **Female**
- ☐ **Male**
- ☐ Accent
- ☐ Angry
- ☐ Calm
- ☐ Clearing throat
- ☐ Coughing
- ☐ Cracking Voice
- ☐ Crying
- ☐ Deep
- ☐ Deep breathing
- ☐ Disguised
- ☐ Distinct
- ☐ Excited
- ☐ Laughter
- ☐ Lisp
- ☐ Loud
- ☐ Nasal
- ☐ Normal
- ☐ Ragged
- ☐ Rapid
- ☐ Raspy
- ☐ Slow
- ☐ Slurred
- ☐ Soft
- ☐ Stutter

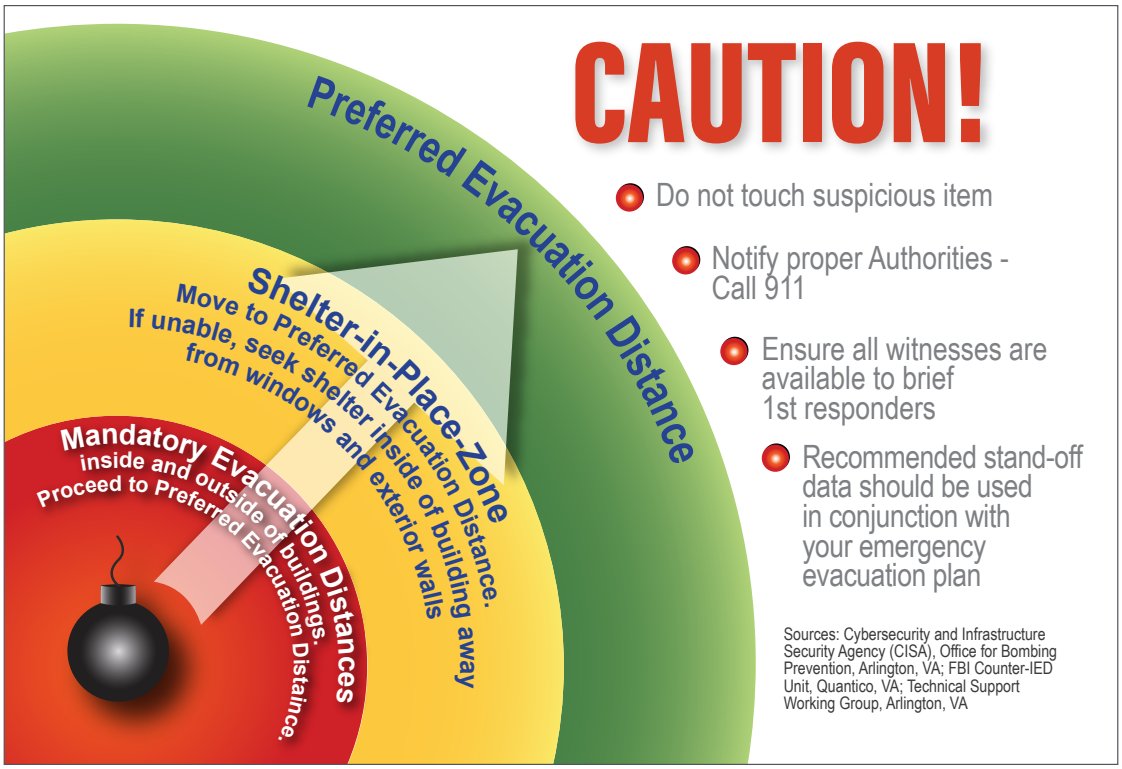
Background Sounds

- ☐ Animal noises
- ☐ House noises
- ☐ Kitchen noises
- ☐ Street noises
- ☐ Booth
- ☐ PA system
- ☐ Conversation
- ☐ Music
- ☐ Motor
- ☐ Clear
- ☐ Static
- ☐ Office machinery
- ☐ Factory machinery
- ☐ Local
- ☐ Long distance

Other Information:

Threat Language

- ☐ Incoherent
- ☐ Message read
- ☐ Taped message
- ☐ Irrational
- ☐ Profane
- ☐ Well-spoken



BOMB THREAT STAND-OFF CARD

OFFICE FOR BOMBING PREVENTION

Threat Description	Explosives Capacity	Mandatory Evacuation Distance	Shelter-in-Place Zone	Preferred Evacuation Distance
Pipe Bomb	5 lbs	70 ft	71-1199 ft	+1200 ft
Suicide Bomber	20 lbs	110 ft	111-1699 ft	+1700 ft
Briefcase/Suitcase	50 lbs	150 ft	151-1849 ft	+1850 ft
Car	500 lbs	320 ft	321-1899 ft	+1900 ft
SUV/Van	1,000 lbs	400 ft	401-2399 ft	+2400 ft
Small Delivery Truck	4,000 lbs	640 ft	641-3799 ft	+3800 ft
Container/Water Truck	10,000 lbs	860 ft	861-5099 ft	+5100 ft
Semi-Trailer	60,000 lbs	1570 ft	1571-9299 ft	+9300 ft

DEFEND TODAY, SECURE TOMORROW

Suspicious or Unattended?

Criminals or terrorists sometimes conceal improvised explosive devices (IEDs) in backpacks, suitcases, or common items.

Use this process to safely determine if an item is a serious threat or just unattended.

Is it H O T ?

Hidden
- Placed out of sight
- Appears purposely concealed

Obviously suspicious
- Unexplainable wires or electronics
- Bomb-like components

not Typical
- Out of place for the location
- Potentially related to a threat

- Use **R. A. I. N.** (Continue to other side)

YES (Suspicious)

NO (Unattended)
- Treat with caution
- Try to determine the owner
- Report to an authority

If an item is suspicious you should:

R — **Recognize the Indicators of a Suspected Explosive Device**

Indicators can be related to the characteristics, events, location, or time, including whether the item is Hidden, Obviously suspicious, or not Typical (HOT).

A — **Avoid the Area**

Don't touch the suspected item. Instead, immediately move and direct others to move away immediately.

I — **Isolate the Suspected Item**

Establish a perimeter to secure the area and continue to direct people away. Use frontal and overhead cover and if available wear personal protective equipment.

N — **Notify Appropriate Emergency Services**

Describe the **S**uspicious items and persons, the person's **A**ctions, the **L**ocation of the item, the **T**ime of placement and discovery, and **Y**our actions to mitigate risk (SALTY).

If you **see** something, **say** something®

REPORT SUSPICIOUS ACTIVITY. Contact **local law enforcement** or **9-1-1** in case of emergency

DEFEND TODAY, SECURE TOMORROW

"If You See Something, Say Something®" used with permission of the NY Metropolitan Transportation Authority

Mass Bomb Threats

CISA OFFICE FOR BOMBING PREVENTION

Increasingly, bad actors are conducting strategic campaigns where multiple bomb threats sometimes simultaneously target infrastructure. Whether these mass bomb threats are made at multiple locations, or to one location over a length of time, **mass bomb threat campaigns can have significant impacts.**

INDICATORS

- Threats lack specificity and realism
- Often delivered via email, phone, or social media
- Phone threats are likely to have automated voices
- Media reports indicate similar and simultaneous threats

Cascading consequences and enhanced impact

Mass bomb threat campaigns target specific types of infrastructure on a national level such as:

- Election Polling Locations
- Medical Facilities
- Institutions of Higher Education
- Faith-Based Organizations

OPERATIONAL IMPACT

May halt activities, harm commerce, and drain resources

PSYCHOLOGICAL IMPACT

May disrupt lives, create fear, uncertainty, and panic

Each affected organization or facility should carefully evaluate the bomb threat

Consider the **facts, context,** and **totality of the circumstances,** then determine a response option.

Exact wording of the threat | **Prior threats** against this or similar facilities | **Current events** regarding this or similar facilities | **Accessibility** of the site | **Occupants** of the site

RISK LEVELS

Low — A **vague** and **indirect** threat that poses a minimum risk to the victim or public safety.

Medium — A threat that is **direct** and **feasible** and could be carried out, although it may not appear entirely realistic.

High — A threat that is **direct, specific, realistic,** and poses an immediate and serious danger to the safety of others.

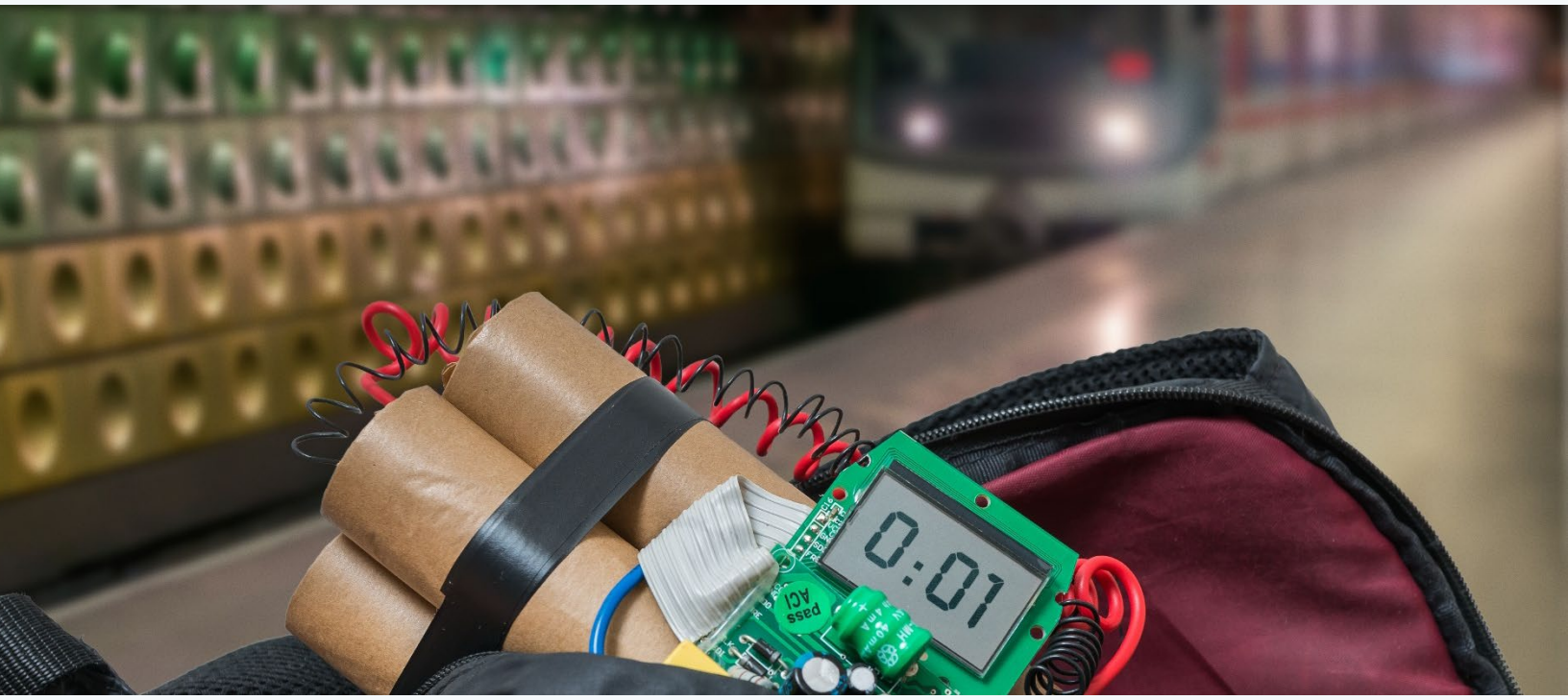
THREAT RESPONSE OPTIONS

- **Assess & Discount:** continue to monitor
- **Assess & Lockdown:** partial or full
- **Assess, Lockdown, & Search:** partial or full
- **Assess & Evacuate:** partial or full, includes priority searches

Every bomb threat requires professional judgment and should be handled in accordance with the facility's needs. 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.

For a full list of related CISA Office for Bombing Prevention trainings and resources, please visit: **cisa.gov/what-to-do-bomb-threat**

DEFEND TODAY, SECURE TOMORROW



Version: 1.0