**<Insert Cover Photo>**

**Bomb Threat Tabletop Exercise**

**CISA Tabletop Exercise Package**

**Situation Manual**

**<Sponsoring Organization>**

<Month, Day, Year>

Cybersecurity and Infrastructure Security Agency

Updated March 2025

Table of Contents

Exercise Agenda 3

Exercise Overview4

General Information6

Module 1: Intelligence and Information Sharing8

Module 1: Scenario Update10

Module 2: Incident Response12

Module 2: Scenario Update14

Module 3: Recovery and Continuity16

Appendix A: Exercise Participants18

Appendix B: Relevant Plans19

Appendix C: CISA OBP Resources for Bomb Threats20

Appendix D: Acronyms22

# Exercise Agenda

|  |  |
| --- | --- |
| Time | Activity |
| 20 Minutes | Introductions and Opening Remarks |
| 60 Minutes | Module 1: Intelligence and Information Sharing |
| 10 Minutes | Break |
| 60 Minutes | Module 2: Incident Response |
| 10 Minutes | Break |
| 60 Minutes | Module 3: Recovery and Continuity |
| 30 Minutes | Hotwash and Closing Remarks |

*All times are approximate.*

# Exercise Overview

|  |  |
| --- | --- |
| Exercise Name | Bomb Threat Tabletop Exercise |
| Exercise Date(s), Time, and Location | <Exercise Date(s)>  <Time (e.g., 9:00 a.m. – 12:00 p.m.)>  <Exercise Location> |
| Purpose | Assess the resilience of <organization name> and their ability to respond to a significant threat. |
| Mission Area(s) | Prevention, Protection, Mitigation, Response, and Recovery [Select as appropriate based on the discussion questions chosen.] |
| Core Capabilities | * Intelligence and Information Sharing * On-Scene Security, Protection, and Law Enforcement * Operational Communication * Operational Coordination * Planning * Public Information and Warning * Public Health, Healthcare, and Emergency Medical Services (EMS) * Situational Assessment   [modify as needed] |
| Objectives | 1. Review emergency preparedness plans and response procedures to a suspicious activity event and a follow-on bomb threat. 2. Examine threat and incident information sharing, notification, and communication procedures between [insert facility or organization] partners, focusing on intelligence community partners and law enforcement. 3. Examine public messaging and information plans and procedures related to an active threat. 4. Discuss recovery and continuity plans and procedures following suspicious activity events and a bomb threat.   [Insert additional exercise objectives as necessary] |
| Threat or Hazard | Suspicious Activity, Bomb Threat |
| Scenario | An interactive, discussion-based exercise focused on a suspicious activity, followed by a bomb threat. The scenario consists of three modules: Intelligence and Information Sharing, Incident Response, and Recovery and Continuity. |
| Sponsor(s) | <Exercise Sponsor(s)> |
| Participating Organizations | <Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.).>  Please see Appendix A for a complete list of participating organizations. |
| Points of Contact | **<Organization POC(s)>**  Contact Information  **CISA Exercises**  <cisa.exercises@mail.cisa.dhs.gov> |

# General Information

## Building Resilience

The purpose of CISA’s Tabletop Exercise Packages (CTEPs) is to increase your organization’s resilience by assessing and validating capabilities and identifying areas for improvement.

## Participant Roles and Responsibilities

**Players** have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario.

**Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.

**Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key EPT members may also assist with facilitation as subject matter experts during the exercise.

**Moderators** are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio. [Remove for in-person exercises.]

**Data Collectors** are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

## Exercise Structure

This exercise is intended to be a facilitated exercise. Players will participate in the following:

* Scenario modules:
  + **Module** **1:** Intelligence and Information Sharing
  + **Module** **2:** Incident Response
  + **Module** **3:** Recovery and Continuity
* Hotwash

***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired.*

## Exercise Guidelines

* This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.
* Respond to the scenario using your knowledge of existing plans and capabilities, along with the valuable insights derived from your training.
* Decisions are not precedent-setting and may not reflect your organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options, possible solutions, and suggested actions to resolve or mitigate a problem.
* There is no hidden agenda or trick questions. The resources and written materials provided are the basis for discussion.
* Issue identification is not as valuable as suggestions and recommended actions that could improve prevention, protection, mitigation, response, and recovery efforts. Problem-solving efforts should be the focus.
* In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors to negatively impact your participation in the exercise.

## Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions. Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and evaluator notes, will be used to evaluate the exercise, and then compiled into the After-Action Report (AAR) / Improvement Plan (IP).

# Module 1: Intelligence and Information Sharing

***Note: For consistency throughout this exercise, participants should have a clear meaning of the term Bomb Threat. A bomb threat is any communication that indicates the presence of or intent to detonate an explosive device.***

### <Incident Month, Day, Year: Time>

Over the past few years, there have been an increasing number of bomb threats directed at a wide spectrum of critical infrastructure facilities throughout the United States. Most of these threats consist of little information about the caller, and no groups or organizations have taken direct responsibility for them. While an actual explosive device is often not discovered as the result of a bomb threat, these threats create fear, anxiety, loss of productivity, and can significantly strain resources.

The Department of Homeland Security (DHS) 2025 Homeland Threat Assessment (HTA) states,

"[Domestic Violent Extremists] DVEs and criminal actors with a range of motivations—some unclear—likely will continue to call for and carry out physical attacks against US critical infrastructure. Violent extremists view such attacks as advancing their ideological and sociopolitical goals, a trend that is consistent with historic drivers."

Federal agencies such as CISA, ATF, and the FBI have increased their outreach, information sharing, and other resources with state, local, tribal, territorial, and private sector partners, as well as state and local fusion centers.

### Discussion Questions

*The following questions are designed to help Players engage in discussions regarding your operational response to the scenario. These questions may not be a definitive list of concerns to address, nor is it required to address every question. The questions may be altered, removed, or added to as desired.*

1. Does [insert facility or organization] have a Bomb Threat Management Plan?
   1. Who is responsible for reviewing and updating the Bomb Threat Management Plan?
   2. Is law enforcement involved in the planning and reviewing process?
   3. How often is the Bomb Threat Management Plan reviewed and updated?
   4. How is the Bomb Threat Management Plan communicated to staff?
   5. Is there any specific training associated with the Bomb Threat Management Plan?
   6. How often is the Bomb Threat Management Plan exercised, such as a drill or tabletop?
   7. Is there a predetermined point of contact at your facility for law enforcement / Bomb Squad?
2. How is your facility / organization coordinating information sharing among partners (e.g., federal, state, and local law enforcement; fusion centers; surrounding businesses; other state organizations; etc.)?
   1. What pre-existing relationship does law enforcement have with your facility / organization?
3. What security recommendations, if any, are local, state, and federal law enforcement or fusion centers making to stakeholders?
4. Does the fusion center currently track bomb threats or trends within its area of responsibility? If so, how do they receive and disseminate that information?
   1. Does the fusion center track regional or nationwide bomb threat trends? If so, how do they receive and disseminate that information?
   2. What is the fusion center’s process for sharing information about bomb threat trends with local, state, and federal law enforcement and public safety agencies?
5. What methods of intelligence gathering and information sharing do you have within [insert facility or organization?
6. Does [insert facility or organization] have a violence prevention program (e.g. – insider threat management program or a Behavioral Threat Assessment and Management Team)?
   1. How does [insert facility or organization] triage the information you receive (e.g., from formal reporting, hearsay, and open-source websites)?
   2. Who is empowered to make decisions based on a review of this information?
   3. How are decisions made on this threat information and who are these decisions communicated to?
7. What plans exist describing any protective measures that [insert facility or organization] needs to take?
   1. How would you adjust your security posture based on the information that you receive?
   2. At what point do you inform employees of a potential threat?

# Module 1: Scenario Update

### <Incident Month, Day, Year: Time>

The receptionist for your organization receives a call from an individual who says he is interested in a position with your organization. The receptionist offers to transfer him to the Human Resources Specialist, but he declines and starts a line of questioning about who the Chief Operating Officer is, what office he works from, and how he can be contacted directly. When asked to provide his contact information, he is reluctant but later gives the name of Joseph Smith. He then indicates he must go but will call back later. The employee reports this information to her manager.

Later that day, an employee notices an individual wearing a hooded sweatshirt, ball cap, sunglasses and jeans walking around the outside perimeter of your facility. The individual appears to be taking pictures of the building entrances and the parking lot. The employee reports this information to her manager.[[1]](#footnote-2)

### Discussion Questions

*The following questions are designed to help Players engage in discussions regarding your operational response to the scenario. These questions may not be a definitive list of concerns to address, nor is it required to address every question. The questions may be altered, removed, or added to as desired.*

1. What steps does [insert facility or organization] take once it receives notice of or observes suspicious activity?
2. Does [insert facility or organization] display or distribute any products, such as messaging, posters, etc., to promote suspicious activity awareness and reporting procedures?
   1. Where does your facility / organization source these products or posters?
3. Does [insert facility or organization] participate in Suspicious Activity Reporting (SAR) efforts?
   1. Does [insert facility or organization] conduct any specific training on suspicious activity awareness or SAR?
   2. If so, what kind of training?
   3. Are these trainings mandatory?
4. What individuals inside of [insert facility or organization] would you need to notify based on this suspicious activity?
5. What key stakeholders outside of [insert facility or organization] would you need to notify based on this suspicious activity?
6. What mechanisms are in place for [insert facility or organization] to report suspicious activity?
7. Who is responsible for assessing the threat? What criteria are used to do so?
8. Do you have a security team that patrols or monitors the interior / exterior of your facility?
9. What actions are local, state, and federal law enforcement agencies taking at this point?
10. What security recommendations, if any, are local, state, and federal law enforcement making to stakeholders at this point?
11. Is [insert facility or organization] aware of or does it interact with the local fusion center?
    1. How does the fusion center educate private and public sector partners about reporting suspicious activity, such as bomb threats?
12. What other agencies or organizations would you notify of this incident?

# Module 2: Incident Response

### <Incident Month, Day, Year: Time>

At approximately [insert time], the receptionist receives an anonymous phone call stating bombs have been placed at your facility / organization and [insert facility or organization] would “pay for their misdeeds.” The caller does not provide information about what time the bombs will detonate or the specific location(s), but they do state, “Don’t try to look for them. Get out now.”

The company’s public-facing email account also receives a message that states, “A bomb will go off in your facility in two hours. You’ve been warned!” The information technology department immediately provides this information to [insert facility or organization]’s security department.

### Discussion Questions

*The following questions are designed to help Players engage in discussions regarding your operational response to the scenario. These questions may not be a definitive list of concerns to address, nor is it required to address every question. The questions may be altered, removed, or added to as desired.*

1. Does the [insert facility or organization] staff receive any specific training on receiving a bomb threat?
2. How would [insert facility or organization] internally communicate information about a bomb threat?
3. What factors would be considered in assessing the bomb threat to aid an appropriate response?
4. According to your Bomb Threat Management plan, what actions would be taken at this time? In the absence of a plan, what are your priorities?
   1. Who is responsible for enacting your Bomb Threat Management Plan?
   2. Does [insert facility or organization] have and use job aids such as Bomb Threat Checklists to document information about the bomb threat?
      1. If so, where are these job aides located?
5. When would it be necessary for [insert facility or organization] to notify law enforcement?
6. Once notified, what type of response does [insert facility or organization] expect from the local or state law enforcement (patrol officer, Bomb Squad, or explosives detection canine)?
7. What actions or recommendations are local and / or state law enforcement agencies taking at this point?
8. Does the Bomb Threat Management Plan include specific actions to be taken when receiving via various modes of transmission such as phoned, written, e-mailed, verbal, etc.?
   1. If your facility or organization chooses to conduct its own search, does the Bomb Threat Management Plan designate team member responsibilities such as Decision Maker, Law Enforcement Liaison, Evacuation Team Leader, Evacuation Team, etc.?
   2. If your facility or organization chooses to conduct its own search, do the employee expectations of their roles mirror those of the law enforcement expectations?
9. If your facility or organization chooses to conduct its own search, does the Bomb Threat Management Plan identify actions to be taken if a suspicious item is found?
10. If your facility or organization conducts its own search, how often are IED search procedures exercised, such as a drill or tabletop?
    1. If your facility or organization chooses to conduct its own search of the premise, are tools and equipment such as flashlights, floorplans, or note pads available for use by Search Teams?
11. What protective measures are in place to protect against a bombing attack?
12. What level of security / law enforcement presence is at [insert facility or organization] daily?
    1. What role do they play in a bomb threat situation?
13. Who makes the decision to evacuate or not evacuate?
14. What factors are being considered when deciding to evacuate or not evacuate?
15. Does your facility / organization have an emergency evacuation plan?
    1. Does your evacuation plan have a pre-designated rally point(s)?
    2. How often do you rehearse your evacuation plan?
16. What other resources are available to assist with resolving the incident, and what are the triggers for their response?
17. What information is critical from your facility / organization to assist in the criminal investigation?
18. How is information being disseminated to other area law enforcement and emergency managers?
    1. How does law enforcement determine if this is part of a nationwide threat, such as a swatting campaign, or if it is isolated to your facility / organization / locality?
    2. What role does the fusion center play?
19. How is information of this incident communicated to employees both internal and external to your facility / organization?

# Module 2: Scenario Update

### <Incident Month, Day, Year: Time>

Based on the information gleaned from the bomb threat and the previous suspicious activity, the Site Manager has assessed the threat as a moderate risk. They decide to “shelter-in-place" or lockdown the facility. Appropriately trained and qualified on-site security personnel conduct a partial search of the exterior and public access areas for anything suspicious.

### Discussion Questions

*The following questions are designed to help Players engage in discussions regarding your operational response to the scenario. These questions may not be a definitive list of concerns to address, nor is it required to address every question. The questions may be altered, removed, or added to as desired.*

1. What shelter-in-place or lockdown procedures does [insert facility or organization] have?
   1. How often are they updated and practiced?
2. How are facility / organization employees trained to respond to an incident such as this?
   1. Is training conducted on a regular basis?
3. Are there protocols in place to alert nearby businesses and organizations of an emergency?
4. What additional notifications need to be made outside of [insert facility or organization]?
   1. How is this notification process conducted?
5. What actions are local and / or state law enforcement agencies taking at this point?
6. What security recommendations, if any, are local, state, and federal law enforcement making to stakeholders at this point?
7. Is there initial and ongoing training for security personnel and staff on IED recognition and bomb-making material awareness?
   1. Do site managers and staff have training on what to look for concerning suspicious items?
   2. If you have on-site security personnel, are they trained to know the difference between an “unattended item” and a “suspicious package?”
      1. If so, what are the different types of indicators the on-site security personnel will look for (i.e.: Hidden, obviously suspicious, and not Typical; Recognize indicators of a suspected explosive device, Avoid the area, Isolate the item, Notify 911 (HOT RAIN) principles)?
8. Are employees or your search and / or evacuation team trained in IED search procedures?
9. How would you handle staff who are worried about their safety and want to go home?
10. Does the Bomb Threat Management Plan identify evacuation and / or sheltering-in-place actions to be taken if a suspicious item is found?
    1. Do these procedures account for individuals with access and functional needs?
11. What other resources are available to assist with resolving the incident, and what are the triggers for their response?
12. What information is critical from your facility / organization to assist in the criminal investigation?
13. How is this information shared with law enforcement?
14. What resources or tools does the fusion center have to assist in resolving this incident?
15. Is the fusion center communicating information about similar incidents to on-site law enforcement?
16. Is the fusion center or law enforcement communicating information about this incident to other fusion centers / agencies? If so, how?
17. How are you determining whether this is an isolated event or part of a local, regional, or national campaign?
18. What other actions are you taking at this point?

# Module 3: Recovery and Continuity

### <Incident Month, Day, Year: Time>

Utilizing the Law Enforcement Liaison, Search Team Leader, and Search Teams, the results of the partial search of the exterior and public access areas for anything suspicious revealed nothing. After lifting the shelter-in-place / lockdown, your organization assists law enforcement with investigative follow-up activities.

Although there is no real threat to your organization at present, some employees are hesitant to return to work and want to know what your organization is doing to ensure their safety. Some local media outlets are sending inquiries regarding the incident and are seeking comments about the organization’s next steps.

### Discussion Questions

*The following questions are designed to help Players engage in discussions regarding your operational response to the scenario. These questions may not be a definitive list of concerns to address, nor is it required to address every question. The questions may be altered, removed, or added to as desired.*

1. Does your facility conduct an accountability check of your employees?
   1. What plans and procedures do you have in place to accomplish this?
2. How do you share the results of the search internally with employees?
   1. How do you address employee concerns about the threat and the reopening of your facility?
3. Does your facility have contingency plans for continuity of operations if it needed to be closed for an extended period due to the threat and search operations?
   1. Do you already have, or how would you identify, an alternate work site if needed?
4. Does [insert facility or organization] have a media plan?
5. Does your media plan cover scenarios such as this?
   1. Who is responsible for public messaging?
   2. How are you coordinating messaging with response agencies and other stakeholders to ensure that one consistent message is disseminated?
   3. How are these messages being released?
   4. Do you have plans and procedures for how this is accomplished?
6. What business continuity or rapid recovery plan does your organization have, if any?
   1. What type of messaging will your organization send to employees, vendors, and industry partners? How will you do this?
   2. What training do employees and / or industry partners receive regarding media relations and the release of sensitive information?
7. What are the short-term recovery objectives for your organization?
8. What, if any, of the organization’s interdependencies could have been affected because of any interruption to daily operations?
9. What actions would be taken to address security concerns at [insert facility or organization] following the incident?
   1. Is there any change in security posture for [insert facility or organization] following this event?
10. How would [insert facility or organization] prepare for any public backlash and criticism for the actions taken by the facility and law enforcement during the incident?
11. Does your facility maintain transaction logs or record telephone calls, e-mails, etc., to support any investigative activity?
12. What steps does your organization take during response and recovery to track gaps and best practices for continuous improvement in disaster response?

# Appendix A: Exercise Participants

|  |
| --- |
| Participating Private Sector Organizations |
|  |
|  |
|  |
|  |

|  |
| --- |
| Participating Local Organizations |
|  |
|  |
|  |
|  |

|  |
| --- |
| Participating State Organizations |
|  |
|  |
|  |
|  |

|  |
| --- |
| Participating Federal Organizations |
|  |
|  |
|  |
|  |

|  |
| --- |
| Other Participating Organizations |
|  |
|  |
|  |
|  |

# Appendix B: Relevant Plans

*Insert excerpts from relevant plans, policies, or procedures to be discussed during the exercise. Materials may include:*

* *Organizational Standard Operating Procedures*
* *Training or employee onboarding protocols*
* *Facility or community maps*
* *Emergency contact information of key organizations*

# Appendix C: CISA OBP Resources for Bomb Threats

CISA OBP builds nationwide counter-improvised explosive device (C-IED) core capabilities through multiple programs and a diverse curriculum of training and awareness products to enhance terrorist threat awareness. These resources are designed to aid communities and individuals in effectively addressing bombing incidents and threats.

**Training**

* + [Bomb Threat Assessment for Decision Makers Course (AWR-945) | CISA](https://www.cisa.gov/resources-tools/training/bomb-threat-assessment-decision-makers-course-awr-945) (virtual) – Introduction to types of threats, the threat assessment process, and the implementation of a BTM plan.
  + [Bomb Threat Preparedness and Response Course (AWR-903) | CISA](https://www.cisa.gov/resources-tools/training/bomb-threat-preparedness-and-response-course-awr-903) (online) – Interactive exercises and case histories of what happened during bombing incidents.
  + [Bomb Threat Management Planning Course (MGT-451) | CISA](https://www.cisa.gov/resources-tools/training/bomb-threat-management-planning-course-mgt-451) (in-person) – Mobile training team-led foundational knowledge on the DHS risk management process and bomb threat management planning.
  + [IED Search Procedures Course (PER-339) | CISA (in-person) - I](https://www.cisa.gov/resources-tools/training/ied-search-procedures-course-339)ntroduces participants to basic, low-risk search protocols. It provides participants the information needed to create a search plan for their facility or special event.
  + [Introduction to Bomb Threat Management Course (AWR-939) | CISA](https://www.cisa.gov/resources-tools/training/introduction-bomb-threat-management-course-awr-939) (virtual) – Provides an overview of domestic bomb threat data including the delivery, recipients, and impact of bomb threats historically and today.

**Resources**

* + [Bomb Threat Guide](https://www.cisa.gov/resources-tools/resources/bomb-threat-guide) – Walks decision-makers through planning for, assessing, and responding to bomb threats in an orderly and controlled manner.
  + [Bomb Threat Procedures & Checklist](https://www.cisa.gov/resources-tools/resources/dhs-bomb-threat-checklist) – Provides instructions on responding to a bomb threat in addition to a comprehensive list of information to assist law enforcement investigations.
  + [Suspicious or Unattended Item](https://www.cisa.gov/resources-tools/resources/unattended-vs-suspicious-item-postcard-and-poster) Postcard – Provides a process to determine if an item is a serious threat or an unattended item.
  + [Bomb Threat Stand-Off](https://www.cisa.gov/resources-tools/resources/dhs-doj-bomb-threat-stand-card) Postcard – Provides a quick reference on recommended evacuation and shelter-in- place distances for various IED types and sizes.
  + [Mass Bomb Threats](https://www.cisa.gov/resources-tools/resources/mass-bomb-threats-postcard) Postcard – Provides awareness on mass bomb threat campaigns.
  + [Bomb Threat Management Annex Template | CISA](https://www.cisa.gov/resources-tools/resources/bomb-threat-management-annex-template) – Assists college and university security officials in developing and implementing plans to manage bomb threat situations.
  + [What to Do: Bomb Threats | CISA](https://www.cisa.gov/resources-tools/resources/what-do-bomb-threats) - This guidance document provides an overview of bomb threats and some recommended practices to mitigate the impacts associated with these threats.

**Videos**

* [What to Do: Bomb Threat](https://www.youtube.com/watch?v=v7JUtb-YOdg) – Demonstrates procedures to follow when receiving a bomb threat to help individuals prepare and react appropriately.
* [Critical Resources for Handling Bomb Threats Video](https://www.youtube.com/watch?v=08_pG2hVtrI) – Provides a wide range of free tools and tips to help members of the public and others effectively respond to bomb threats.
* [Bomb Threat Awareness for College Students Video](https://www.cisa.gov/resources-tools/resources/bomb-threat-awareness-college-students-video) - Short video aims to mitigate the impact of bomb threats received by colleges and universities on a student population by showing them the importance of following directions and security procedures. Focus is placed on increasing vigilance to their surroundings and the importance of reporting suspicious activity, items, and packages

**Contact Us**

For more information about CISA OBP and our resources, visit us at [www.cisa.gov/obp](https://www.cisa.gov/topics/physical-security/bombing-prevention/products) or email [OBPOperations@cisa.dhs.gov.](mailto:OBPOperations@cisa.dhs.gov)

To request training and for resources specific to bomb threats, visit our Bomb Threats page at <https://www.cisa.gov/bomb-threats> or email us at [OBP@cisa.dhs.gov](https://ociocisa.sharepoint.com/sites/CISAExercisesInternal/ISEB/CTEP/3%20ISEB%20Situation%20Manuals/Non-Sector%20Specific/Bomb%20Threat/OBP@cisa.dhs.gov)

# Appendix D: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| AAR | After-Action Report |
| ATF | Bureau of Alcohol, Tobacco, and Firearms |
| C-IED | Counter-Improvised Explosive Device |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CTEP | CISA Tabletop Exercise Package |
| DHS | Department of Homeland Security |
| EMS | Emergency Medical Services |
| EPT | Exercise Planning Team |
| FBI | Federal Bureau of Investigation |
| HOT RAIN | HOT: Hidden, Obviously suspicious, and not Typical.  RAIN: Recognize indicators of a suspected explosive device, Avoid the area, Isolate the item, Notify 911. |
| HTA | Homeland Threat Assessment |
| IED | Improvised Explosive Device |
| IP | Improvement Plan |
| OBP | Office for Bombing Prevention |
| POC | Point of Contact |
| SAR | Suspicious Activity Reporting |
| SitMan | Situation Manual |

1. This Tabletop Exercise describes activities and behaviors that may concern or be indicative of criminal or malicious activity; however, certain federal, state, and local laws may legally protect these activities. One should only report these activities when sufficient facts exist to support a rational conclusion that they are indicative of criminal or malicious activity. One should not report activities solely on the basis of race, religion, gender, sexual orientation, age, disability, any other legally protected trait, or a combination of only such traits. [↑](#footnote-ref-2)