



Government Facilities Tabletop Exercise

Situation Manual

[Insert Date]

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

EXERCISE AGENDA

Time	Activity
0745 – 0830	Registration
0830 – 0900	Welcome and Participant Briefing
0900 – 1015	Module One – Threat
1015 – 1030	Break
1030 – 1200	Module Two – Incident and Aftermath
1200 – 1230	Hot Wash

*All times are approximate

This page is intentionally left blank.

EXERCISE OVERVIEW

Exercise Name	Government Facilities Tabletop Exercise (TTX)
Exercise Dates	[Indicate the start and end dates of the exercise]
Scope	<p>This exercise is a TTX, planned for [exercise duration] at [exercise location]. Exercise play is limited to [exercise parameters].</p> <p>This exercise was developed using materials created by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP).</p>
Mission Area(s)	Prevention, Protection, Mitigation, Response, and Recovery [Select appropriate Mission Area(s)]
Core Capabilities	<p>Planning; Intelligence and Information Sharing; Risk Management for Protection Programs and Activities; and, Public Information and Warning</p> <p>[insert other core capabilities]</p>
Objectives	<ol style="list-style-type: none"> 1. Review intelligence and information sharing and dissemination processes in relation to a credible threat to domestic critical infrastructure owners / operators. 2. Assess information sharing capabilities with the public, sector partners, and Federal, State, local, tribal, and territorial government departments and agencies in accordance with applicable plans and procedures. 3. Discuss critical infrastructure stakeholders' emergency preparedness plans and response procedures to a threat-initiated incident and the coordination of activities under National Incident Management System (NIMS) with local, State, and Federal agencies. 4. [Insert additional exercise objectives as necessary]
Threat or Hazard	Improvised Explosive Device (IED)
Scenario	A domestic extremist group with nation-wide reach targets government facilities.
Sponsor	[Insert the name of the sponsor organization, as well as any grant programs being utilized, if applicable]

**Participating
Organizations**

[Insert a brief summary of the total number of participants and participation level (i.e., Federal, State, local, Tribal, non-governmental organizations [NGOs], and/or international agencies). Consider including the full list of participating agencies in Appendix B. Delete Appendix B if not required.]

**Points of
Contact**

[Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (e.g., exercise director or exercise sponsor)]

GENERAL INFORMATION

Exercise Objectives and Core Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to core capabilities, which are distinct critical elements necessary to achieve the specific mission area(s). The objectives and aligned core capabilities are guided by elected and appointed officials and selected by the Exercise Planning Team.

Exercise Objective	Core Capability
Review intelligence and information sharing and dissemination processes in relation to a credible threat to domestic critical infrastructure owners / operators.	✓ Intelligence and Information Sharing
Assess information sharing capabilities with the public, sector partners, and Federal, State, local, tribal, and territorial government departments and agencies in accordance with applicable plans and procedures.	✓ Intelligence and Information Sharing ✓ Public Information and Warning
Discuss critical infrastructure stakeholders' emergency preparedness plans and response procedures to a threat-initiated incident and the coordination of activities under NIMS with local, State, and Federal agencies.	✓ Planning ✓ Public Information and Warning ✓ Risk Management for Protection, Programs, and Activities
[Insert additional objectives as necessary]	✓ [Insert additional core capabilities as necessary]

Table 1. Exercise Objectives and Associated Core Capabilities

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players.** Players are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers.** 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.** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members also may assist with facilitation as subject matter experts (SMEs) during the exercise.

- **Evaluators.** Evaluators are assigned to observe and document certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

Exercise Structure

This TTX is comprised of two modules consisting of a domestic extremist threat followed by a domestic incident. Players will participate in the following two modules:

- Module One: Threat
- Module Two: Incident and Aftermath

Each module begins with a scenario update that summarizes key events occurring within that time period. A series of questions following the scenario summary will guide the facilitated discussion of critical issues in each of the modules. Based on exercise priorities, time dedicated to each module will be managed by the facilitator.

Exercise Guidelines

- This exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and 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 and possible solutions.
- The situation updates, written material, and resources provided are the basis for discussion. There are no hidden materials or scenarios.
- Issue identification is not as valuable as suggestions and recommended actions that could improve prevention, protection, and response efforts. Problem-solving efforts should be the focus.

Exercise Assumptions and Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted and/or account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise and should not allow these considerations to negatively impact their participation. During this exercise, the following apply:

- The scenario for this exercise is fictitious and does not represent any actual intelligence.
- The scenario is plausible, and events occur as they are presented.
- There are neither “hidden agendas” nor any “trick questions.”
- All players receive information at the same time.
- Assume cooperation and support from other responders, agencies, and organizational entities.

Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities, capability targets, and critical tasks. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and then compiled into the After-Action Report (AAR).

This page is intentionally left blank.

MODULE ONE: THREAT

Date: [Insert Event Date - 45 days]

Based on recent incidents in the United States and Europe, and increased chatter regarding similar incidents being called for, the Secretary of Homeland Security, through the National Terrorism Advisory System (NTAS), and in coordination with other Federal entities, issues an “Elevated” Threat Alert, warning of a credible terrorist threat against an organization in the United States. At this time, there is no specific information, which would warrant the release of an “Imminent” Threat Alert.



Photo courtesy of DHS

The alert follows a period of heightened domestic conflict and states that the threat is from domestic terrorist groups in the United States with ties to anti-government extremist organizations, which are focused on government facilities. In addition, the alert indicates these terrorists are using IEDs concealed in backpacks and duffle bags. The alert is to remain in place for three months, ending on [insert date].

DHS has passed on the alert to its partners in the Government Facilities Sector.

Additional information about the alert can be found in **Appendix A**.

Date: [Insert Event Date-14 days]

Time: [Insert]

A state trooper in [insert location] notices suspicious items in a vehicle during a routine traffic stop. Upon searching the vehicle, the trooper uncovers a variety of bomb making materials as well as anti-government paraphernalia. After executing a search warrant at the vehicle occupant’s place of residence, local law enforcement discovers surveillance materials, including maps and photographs, as well as documentation that suggests planned attacks at several local government buildings.

Following an extensive interview process with the suspect, local law enforcement determines that there are multiple other planned attacks targeting communities throughout the country, including confirmed locations in Montana, New York, and Texas.

Discussion Questions

1. What is the process by which your organization would receive intelligence and protective measure information given an emergent threat?

- a. What security organizations would you communicate with (e.g., Federal Protective Service (FPS), other agency-specific or local law enforcement, security agencies, your Joint Terrorism Task Force [JTTF], Federal Bureau of Investigation [FBI])?
 - b. What is the role of the Facility Security Committee (FSC) or Federal Executive Board in sharing threat and protective measure information?
 - c. Does your organization maintain a relationship with your Interagency Security Committee (ISC) Regional Advisor, Protective Security Advisor (PSA) or other members of the DHS CISA Regional Office? If so, do you have a rapid means of contacting them?
 - d. Does your organization use Homeland Security Information Network – Critical Infrastructure (HSIN-CI)?
2. What internal information sharing and dissemination processes does your organization currently have in place?
 3. How does your organization triage the information you receive (e.g., formal reporting, rumors, social media) for further dissemination within your organization and to your personnel?
 4. What resources are utilized to disseminate information?
 - a. What notification capabilities (e.g., alerts, email, telecom, text message, special tools) do you utilize to share information and communicate protective measures implementation appropriately with tenants, security organizations, etc.?
 - b. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing, such as religious customs that prohibit use of electronic communication during specific times?
 - i. If so, how will threat-based alerts and notifications be distributed to community members who follow religious customs that prohibit use of electronic communication during specific times?
 5. Given current and established information sharing procedures, what types of official information are the most useful (immediate information versus analyzed information) to your organization?
 - a. Does your organization perform independent analysis on information provided and, if so, describe the process?
 6. If your organization receives information related to potential threats against your facilities and personnel, how would you communicate this information to appropriate security entities (FPS, local law enforcement agencies, JTTF, FBI, your ISC Regional Advisor, PSA or other members of the CISA Regional Office, etc.)?
 7. If there is identified “suspicious behavior” observed at government facilities, how do the facilities report this information locally and within the sector?
 - a. Are trends of suspicious behaviors tracked across government facilities nationwide?
 - b. Is your organization aware of the “If You See Something, Say Something™” campaign or the National Suspicious Activity Reporting (SAR) Initiative?

8. Given evidence of a credible threat to government facilities, does your organization review your emergency response plans (e.g., Facility Security Plans, Occupant Emergency Plans, Emergency Action Plans, continuity of operations plans (COOP), or other appropriate plans or documents)?
9. What protective security measures or recommendations, if any, will be employed at your organization based on this threat?
 - a. Does your facility have a Facility Security Committee or similar organization responsible for making security and risk decisions for the facility?
 - b. Do you coordinate protective measure implementation with any other organization within government facilities, or with government entities, such as FPS, other agency specific or local law enforcement agencies, ISC Regional Advisor, PSA, or other members of the CISA Regional Office?
 - c. What are some procedural changes your facility could make to temporarily increase its protective posture?
 - d. How are the protective measures government facilities have put in place communicated back to the tenants and to the department/agency?
 - e. How useful are the information bulletins and advisories DHS provides (e.g., a Joint Intelligence Bulletin [JIB]) that recommend protective measures?

This page is intentionally left blank.

MODULE TWO: INCIDENT AND AFTERMATH

Date: [Insert]
Time: [Insert]
[Insert Location]

It is approaching mid-morning and [Insert Name of Service Facility] is already packed with citizens conducting their business. An individual approaches the Federal facility and casually places an Improvised Explosive Device (IED) concealed in a backpack behind a flower pot at the public entrance to the facility, where security personnel are tied up screening the public. Nobody notices the backpack. Subsequently, an explosion rips through the lobby of the building, instantly killing multiple people inside. The blast propels shrapnel and debris into the parking lot causing further injury. In the resulting confusion, survivors attempt to flee the area, resulting in additional injuries from slips and falls.



First responders quickly arrive on scene and attempt to identify the source of the blast. They estimate at least [insert number] killed and many more injured.

Local 911 dispatch is quickly overwhelmed by calls from concerned loved ones, and social media has exploded with images and live-streaming videos from bystanders.

Scenario Update

Date: [Insert]
Time: [Insert Initial Incident + 20 minutes]
[Insert local High Security Facility]

Shortly after the incident at [insert Name of Service Facility], an employee of [insert name of High Security Facility] approaches the security checkpoint in an unmarked white van. The security guard recognizes the employee but is suspicious because he has never seen the man in a similar vehicle. Now on heightened alert based on radio reports of an explosion that has just occurred elsewhere in town, he asks the employee to step out of the vehicle so it can be searched. The security guard discovers a large quantity of explosives in the rear of the van and alerts the head of security onsite, who then notifies 9-1-1.

Word of the [insert Name of Service Facility] bombing spreads quickly through the city, though knowledge of the possible vehicle borne improvised explosive device (VBIED) discovered at [insert name of High Security Facility] has not yet spread beyond the first responder / emergency management community. Most businesses and buildings in the area surrounding the [insert Name of Service Facility] comply with the advice of emergency management officials and shelter-in-place. Despite these measures, however, the streets are filled with concerned citizens looking to reach their loved ones and get home safely.

Scenario Update

Date: [Insert]

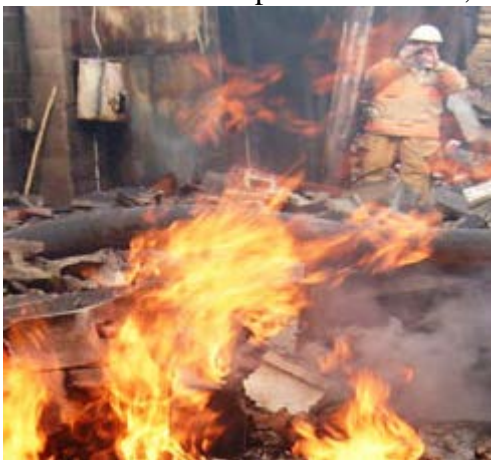
Time: [Insert Initial Incident + 40 minutes]

[Insert local Government Office Building]

The morning's events have significantly raised the activity level of the employees at the [insert name of Government Office Building]. Some employees heed the warnings of security officials and remain in the building, while others decide to take action and leave the premises. Security personnel prevent anyone currently outside the building from entering as they attempt to maintain a secure perimeter.

A car pulls up next to the main entrance of [insert name of Government Office Building]. As a police officer approaches the vehicle to direct it away from the building, the driver of the car detonates a VBIED. The explosion creates a massive fireball and throws glass, metal, and asphalt into the air. The blast carves a large hole in the side of the building by the front entrance and shatters windows in surrounding buildings.

Local 9-1-1 dispatch, already operating at peak capacity following the first detonation, is now overwhelmed with calls. Cellular phone service is limited as networks are receiving more traffic than they can handle. People begin pouring out into the streets trying to escape the mayhem, and descend in droves upon mass transit, looking to leave the area as quickly as possible.



There are untold casualties resulting from the massive VBIED, which has also generated significant infrastructure damage in the area, including ruptured gas and water mains, and area power outages.


Discussion Questions

1. What are your organization's information sharing responsibilities during the response to the incident?
2. What formal information sharing processes would your organization use at this point?
3. Do your organization's emergency response plans (e.g., Facility Security Plans, Occupant Emergency Plans, Emergency Action Plans, COOP, or other appropriate plans or documents) contain protocol for properly responding to the incidents described in this module?
4. Do your existing plans, policies, and procedures address counter-IED (C-IED) considerations?
 - a. If not, are you familiar with the resources available through the DHS Office of Bombing Prevention to assist in incorporating C-IED measures into planning efforts?
5. What resources are utilized to disseminate information?
 - a. What notification capabilities (e.g., alerts, email, telecom, text message, special tools) do you utilize to share information and communicate protective measures implementation appropriately with tenants, with security organizations, etc.?
 - b. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing, such as religious customs that prohibit use of electronic communication during specific times?
 - i. If so, how will threat-based alerts and notifications be distributed to community members who follow religious customs that prohibit use of electronic communication during specific times?
6. Who is the onsite security organization? What other security or law enforcement entities might also be onsite and how have the plans and exercises developed to date coordinated their activities in an event such as this?
7. What protective security measures will be employed at your organization following these domestic attacks?
 - a. Do you coordinate protective measure implementation with any other organization within the government facilities sector, or with government entities, such as FPS, other agency specific or local law enforcement or security agencies, your ISC Regional Advisor, PSA, or other members of the CISA Regional Office?
 - b. How are the protective measures government facilities have put in place communicated back to the tenants and to their parent headquarters?
 - c. How useful are the information bulletins and advisories DHS provides (e.g., a JIB) that recommend protective measures?
8. What measures would security or local law enforcement take at this time to protect your organization (e.g., outreach, increased vigilance, etc.)?
9. Who is responsible for coordinating the risk communications message for your organization?
10. What are the key messages concerning the continuing credible threat to your organization and stakeholders?

- a. Is the message coordinated with the tenants and their department or agency?
 - b. If so, what is the process for coordinating this message?
11. Would your organization review and update your emergency response plans (e.g., Facility Security Plans, Occupant Emergency Plans, Emergency Action Plans, COOP, or other appropriate plans or documents) after the response to these incidents was completed?
 12. What COOP plans are in place to continue operations in the aftermath of the attacks (telework, etc.)?
 13. What post-incident recovery activities might be needed for employees, their families and operations (e.g. reunification, psychological first aid, etc.)?

This page is intentionally left blank.

APPENDIX A: SAMPLE NTAS



National Terrorism Advisory System
Alert
www.dhs.gov/alerts

DATE & TIME ISSUED: Month XX,
XXXX 12:00 PM

SUMMARY

Based on recent intelligence gathering efforts, the Department of Homeland Security is issuing an Imminent Threat alert for the Government Facilities Sector.

DURATION

This alert will expire 30 days after the release date.

DETAILS

- Recent activity by individuals associated with domestic extremist groups suggest the presence of multiple operational cells capable of conducting bombings in locations throughout the United States.
- Recent documents and public statements by the leadership of these groups have called for the bombings of government buildings.
- Multiple members and associates of these groups were apprehended prior to conducting a bombing on government buildings in Tallahassee, Florida, and claimed to be one of several operational cells across the United States.
- The American public can expect to see a greater security presence at government buildings across the country for the next several weeks.

AFFECTED AREAS

- Albany, New York
- Houston, Texas
- Billings, Montana
- Exercise Location

HOW YOU CAN HELP

The public can assist authorities by reporting any suspicious activity they see. To report suspicious activity, the public should contact their local law enforcement agency and described specifically what was observed:

- Who or what you saw
- When you saw it
- Where it occurred; and
- Why its suspicious

BE PREPARED

The public should ensure they are aware of their surroundings during events and activities at large stadiums and/or arenas.

STAY INFORMED

DHS NTAS website:
<http://www.dhs.gov/alerts> and
<http://twitter.com/NTASAlerts>
<http://dhs.gov/see-something-say-something>

If You See Something, Say Something™. Report suspicious activity to local law enforcement or call 911.

The National Terrorism Advisory System provides Americans with alert information on homeland security threats. It is distributed by the Department of Homeland Security. More information is available at: www.dhs.gov/alerts. To receive mobile updates: www.twitter.com/NTASAlerts
If You See Something Say Something™ used with permission of the NY Metropolitan Transportation Authority.

This page is intentionally left blank.

APPENDIX B: EXERCISE PARTICIPANTS

Participating Organizations
Private Sector
[Private sector participants]
Federal
[Federal participants]
State
[State participants]
Local
[Local participants]
Other
[Insert additional participants]

This page is intentionally left blank.

APPENDIX C: RELEVANT PLANS

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

APPENDIX D: ACRONYMS

Acronym	Definition
AAR	After Action Report
C-IED	Counter-Improvised Explosive Device
CISA	Cybersecurity and Infrastructure Security Agency
CTEP	CISA Tabletop Exercise Package
COOP	Continuity of Operations Plan
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FPS	Federal Protective Service
FSC	Facility Security Committee
HSIN-CI	Homeland Security Information Network – Critical Infrastructure
IED	Improvised Explosive Device
ISC	Interagency Security Committee
JIB	Joint Intelligence Bulletin
JTTF	Joint Terrorism Task Force
NIMS	National Incident Management System
NTAS	National Terrorism Advisory System
PSA	Protective Security Advisor
SAR	Suspicious Activity Reporting
SitMan	Situation Manual
SME	Subject Matter Expert
TTX	Tabletop Exercise
VBIED	Vehicle Borne Improvised Explosive Device