[Insert Cover Picture]

Healthcare and Public Health Suspicious Package Tabletop Exercise

Situation Manual

[Date]

This Situation Manual (SitMan) provides exercise participants with all 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.

Photo Courtesy of [insert source]

This page is intentionally left blank.

EXERCISE AGENDA

Start Time	End Time	Activity
7:45 a.m.	8:30 a.m.	Registration
8:30 a.m.	8:45 a.m.	Welcome and Participant Briefing
8:45 a.m.	9:45 a.m.	Module One: Pre-Incident
9:45 a.m.	9:55 a.m.	Break
9:55 a.m.	10:55 a.m.	Module Two: Incident
10:55 a.m.	11:05 a.m.	Break
11:05 a.m.	12:05 p.m.	Module Three: Recovery
12:05 p.m.	12:30 p.m.	Hot Wash
**All times are approximate*		

This page is intentionally left blank.

EXERCISE OVERVIEW

Exercise Name	Healthcare and Public Health (HPH) Suspicious Package Tabletop Exercise (TTX)
Exercise Dates	[Indicate the start and end dates of the exercise]
Scope	This exercise is a TTX planned for [exercise duration] at [exercise location]. Exercise play is limited to [exercise parameters]. This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP).
Mission Area(s)	Prevention, Protection, Mitigation, Response, and Recovery [Select appropriate Mission Areas]
Capabilities	• Economic Recovery • Fatality Management Services • Intelligence and Information Sharing • Logistics and Supply Chain Management • Operational Communications • Operational Coordination • Physical Protective Measures • Planning • Public Health, Healthcare, and Emergency Medical Services (EMS) • Public Information and Warning • Situational Assessment • [Insert other capabilities, as necessary]

Objectives	1. Examine information sharing between HPH owners / operators and various stakeholders, including the public, other HPH owners / operators, and federal, state, and local government departments and agencies when dealing with a credible threat. 2. Assess your facility's plans, policies, and procedures related to an adversarial threat, including incident management, evacuation, and personnel accountability. 3. Assess the ability of existing recovery plans and business continuity / continuity of operations plans to address facility and stakeholder needs following an active threat incident. 4. Enhance the ability of healthcare facilities to provide care during all-hazards incidents and mitigate the threat of disruptions to healthcare services. 5. Discuss and validate internal incident management communication processes in accordance with existing plans and procedures. 6. [Insert additional exercise objectives as necessary.]
Threat or Hazard	Suspicious Package / Improvised Explosive Device (IED)
Scenario	An interactive, discussion-based exercise focused on a potential IED attack. The scenario consists of three modules: Pre-Incident, Incident, and Recovery.
Sponsor	[Insert the name of the sponsor organization, as well as any grant programs being used, if applicable]
Participating Organizations	[Please see Appendix A.]
Point of Contact	[Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (POC) (e.g., exercise director or exercise sponsor).]

GENERAL INFORMATION

Exercise Objectives and Capabilities

The exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

Exercise Objectives	Capability
Examine information sharing between HPH owners / operators and various stakeholders, including the public, other HPH owners / operators, and federal, state, and local government departments and agencies when dealing with a credible threat.	✓ Intelligence and Information Sharing ✓ Operational Coordination ✓ Planning ✓ Public Information and Warning
Assess your facility's plans, policies, and procedures related to an adversarial threat, including incident management, evacuation, and personnel accountability.	✓ Fatality Management Services ✓ Operational Coordination ✓ Physical Protective Measures ✓ Planning ✓ Public Health and Medical Services ✓ Public Information & Warning
Assess the ability of existing recovery plans and business continuity / continuity of operations plans to address facility and stakeholder needs following an active threat incident.	✓ Economic Recovery ✓ Operational Coordination ✓ Planning
Enhance the ability of healthcare facilities to provide care during all-hazards incidents and mitigate the threat of disruptions to healthcare services.	✓ Logistics and Supply Chain Management ✓ Operational Coordination ✓ Planning ✓ Public Health, Healthcare, and EMS
Discuss and validate internal incident management communication processes in accordance with existing plans and procedures.	✓ Intelligence and Information Sharing ✓ Operational Communications ✓ Operational Coordination ✓ Planning ✓ Situational Assessment
[Insert additional objectives as necessary].	✓ [Insert additional core capabilities as necessary].

Table 1. Exercise Objectives and Associated 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.
- **Facilitator:** The facilitator provides situation updates and moderates discussions. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
- **Moderators:** 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.
- **Evaluators:** Evaluators are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

- Module One: Pre-Incident
- Module Two: Incident
- Module Three: Recovery

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [mission area] issues.

Exercise Guidelines

- This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. 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 jurisdiction's / organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommended actions that could improve [mission area] efforts. Problem-solving efforts should be the focus.
- The assumption is the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

Exercise Evaluation

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 AAR / Improvement Plan (IP).

This page is intentionally left blank

MODULE ONE: PRE-INCIDENT

Scenario

[Location]

[Month, Day, Year]

[Insert Your State / Highway Police] receives several calls regarding a suspect running from the scene of a hit-and-run accident. When an officer arrives to investigate, the suspect's vehicle is found abandoned on the side of the highway. A search of the car reveals weapons and explosive manufacturing materials. Police obtain a warrant to search the vehicle owner's home and find instructions for developing homemade bombs, as well as photographs of several medical facilities and badge-making equipment. Police notify the Federal Bureau of Investigation (FBI) field office.

Date: [Insert Date + Four Days]

After investigating the evidence police collected and reviewing recent online activity calling for an attack on healthcare-related activities, the FBI identifies a credible threat in [insert your region]. Based on the investigation, the Secretary of Homeland Security, in coordination with other federal entities, issues an "Elevated" Threat Alert through the National Terrorism Advisory System (NTAS). The alert warns of an extremist group that is planning several attacks on healthcare-related facilities including medical research laboratories, local health departments, and retail pharmacies [edit list if your type of facility is not included]. The alert is to remain in place for three months, ending on [insert date + three months].

Date: [Insert Date + Two Weeks]

During the early morning shift, a [insert your facility name] staff member informs their supervisor that on their way in, they saw an unknown person wandering in front of the facility, acting nervous and evasive while carefully surveying the grounds. The supervisor receives a similar report later that afternoon, with another employee noting they saw an individual roaming the premises and taking pictures. The supervisor notifies building security of both accounts.

Discussion Questions

1. How would your agency or organization expect to receive information about a credible threat?
2. Does your agency or organization receive NTAS alerts from the Department of Homeland Security (DHS)? If so, how? If not, is your organization signed up?
3. How would law enforcement / fusion centers disseminate this information?
4. How does your organization communicate this type of alert, or any suspicious activity alert, to departments within your organization?
    a. What do the department heads do with this information?
    b. How does your organization protect suspicious activity information?
5. How does your organization share this information with the customers / stakeholders that use your facility?

6. What information does your organization's leadership need or expect from local, state, and / or federal agencies regarding this threat?
7. What information-sharing procedures regarding security protocols exist between your organization and those that share similar types of venues?
    a. Would your organization alert other venues and facilities in the area about this situation?
    b. How does your organization's leadership provide, receive, or coordinate information from independent sources?
    c. What process do media outlets use to relay received threat information to appropriate stakeholders?
    d. Who from your organization is responsible for communicating and coordinating with media outlets?
8. How does your organization communicate internally about credible threats?
    a. What protocols govern this process?
    b. How does your organization communicate this information to employees?
9. Do stakeholders in your organization receive instructions from leadership regarding what actions to take concerning imminent threats?
10. How would your organization alert individuals and organizations that use the facility, such as vendors, to this situation?
11. Does your organization conduct any specific training based on general or credible threats?
12. What security recommendations, if any, are local, state, and federal law enforcement making to private sector stakeholders at this time?

MODULE TWO: INCIDENT

Scenario

[Insert Location]

[Month, Day, Year + 20 Days]: [Time]

[Insert your facility name] is busy as usual. A janitorial crew is making routine rounds to collect trash when they notice an unusual waste receptacle. The bin is covered in a tarp, and when an employee approaches it, they notice a strong rotten egg odor and wires sticking out from under the tarp.

The maintenance employee calls the security office for [insert your facility name], who then reports the incident to law enforcement.

Rumors about an on-site explosive device are quick to spread throughout the facility. The arrival of local responders to the scene and immediate evacuation of the building attracts the attention of news outlets as well as social media platforms. Law enforcement works to secure the site while the bomb squad assesses the package.

Discussion Questions

1. Does your organization have an existing Emergency Operations Plan (EOP) that is adaptable to evolving threats?
    a. If so, how recently has your organization reviewed and updated the plan?
    b. Has your organization made local first responders aware of your EOP?
    c. Have local first responders ever visited your facility?
2. How does your organization alert employees to an incident?
    a. How does your organization alter local and state law enforcement to an incident?
    b. What emergency communications plans currently exist within your organization?
3. How does your organization coordinate response operations with local, state, and federal agencies?
    a. Who is responsible for this coordination?
4. What type of command structure would the responders establish?
    a. Who would be in charge of the command structure?
    b. What is the role of your organization and other private sector stakeholders in this command structure?
    c. Are other private sector stakeholders trained on incident command procedures?
5. What would be the role and responsibility of your organization's security?
    a. What assets would security have on hand (guards, cameras, etc.)?

b. Are there specific procedures in place, or does a more general emergency response plan address the actions of security guards?

c. What are security's priorities?

d. With whom is your organization's security communicating?

i. Who in your organization is responsible for contacting local responders?

ii. Who in your facility would your organization notify, and who is responsible for this?

iii. What systems does your organization use to communicate with first responders (in-person, radio, 911 / dispatch, etc.)?

iv. Has your organization's security previously cross-trained with local first responders in responding to an incident?

6. Did someone in your organization activate the Emergency Operations Center (EOC)?

a. Who would staff the EOC in this incident?

7. What information would your organization disseminate to the public?

a. How quickly would your organization notify the public of the incident?

b. Are there "canned / pre-scripted" messages for the public that your organization can easily edit for a specific incident?

c. Who is responsible for this messaging?

d. How do the different agencies and organizations coordinate this messaging?

8. Does your organization have pre-identified Public Information Officers (PIOs)?

a. Does your organization train PIOs for such incidents?

b. Have your PIOs ever had the opportunity to work with local first responder and the jurisdiction's PIOs?

c. How does your organization integrate PIOs into the command structure?

d. In addition to your organization's public messaging efforts, would other organizations be providing public information?

i. Realistically, when would your organization address public information?

ii. What would be your organization's public information priorities following an incident?

iii. Are there plans to coordinate public information between your organization, first responders, and other public and private partners?

9. Does your organization conduct an accountability check of your employees?

a. If so, who is responsible for this? Who collects the information? What is done if an employee does not respond?

b. Do your organization's plans and procedures outline this process? If so, are your employees aware of these existing plans and procedures?

10. What crowd control procedures exist for an incident of this type?
    a. Who is responsible for crowd control?
    b. Does your organization pre-determine ingress and egress routes?
    c. What directions, if any, would your organization give to the crowd?
    d. What plans or procedures exist to work with special needs populations?
11. Would your organization implement an evacuation or shelter-in-place order for employees and guests in the facility?
    a. Who makes the decision to evacuate or shelter-in-place?
    b. How does your organization communicate that decision to employees and guests in the facility?
    c. Does your organization pre-designated a rally point for employees?
    d. Does your organization train and drill employees in either of these responses?

This page is intentionally left blank.

MODULE THREE: RECOVERY

Scenario

[Insert Location]

[Month, Day, Year (Incident Date) + 1 Day]: [Time]

Shortly after the maintenance employee identified the suspicious package, bomb technicians arrived on scene to investigate. After a thorough investigation, law enforcement determined that the suspicious package was a viable IED and successfully neutralized the threat. Law enforcement have reported the scene secure, precautionary searches for secondary devices are underway, and authorities are searching for potential suspects. The medical facility and 911 call centers continue to receive numerous requests for information about the incident. Media packed the entire entrance of the emergency room trying to report on the situation. Some employees and patrons are also showing signs of distress after learning about or experiencing the entire incident.

Discussion Questions

1. How does your organization determine the status of your facilities before, during, and after an incident?
    a. If your organization implements a lockdown, at what point would you lift it?
2. Do your organization's plans, policies, or procedures specifically address resource management?
    a. What type of mutual aid agreements or memorandums of understanding (MOUs) does your organization have with surrounding hospitals to assist with patient care or resource shortages?
3. What type of resources are available to hospitals new to the hospital system?
    a. How do hospitals obtain those resources?
4. How does your facility handle incoming calls from people searching for loved ones?
5. What are the priorities at your facility or organization post-incident?
    a. Do your organization's plans, policies, or procedures specify these priorities?
    b. How does your organization communicate these priorities internally?
    c. Does your organization coordinate priorities with county emergency management?
    d. Does your organization coordinate priorities with state or federal agencies?
6. Whom must your organization inform when normal operations are disrupted?
    a. What information does your organization need to provide?
    b. How would your organization communicate that information?
    c. At what point does your organization distribute that information?
    d. Do your organization's plans, policies, or procedures specify this information?

7. What information is your organization communicating with the public?
    a. Who in your organization is responsible for making this communication?
    b. Are there social media resources available during and immediately after an incident?
    c. What measures does your organization take to mitigate the distribution of misinformation?
8. What type of trauma counseling or mental health services does your facility offer following an incident, if any?
    a. Does your organization provide trauma counseling or mental health services for both employees and patients?
9. How much time would your organization estimate is necessary before resuming business operations?
    a. How long might an investigation take? How does it impact business continuity operations?
    b. How will your organization receive situational updates from law enforcement?
    c. At what point would your organization consider your facility back to steady-state operations?

APPENDIX A: EXERCISE PARTICIPANTS

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

This page is intentionally left blank

APPENDIX B: RELEVANT PLANS

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

This page is intentionally left blank.

APPENDIX C: ACRONYMS

Acronym	Term
AAR	After-Action Report
CISA	Cybersecurity and Infrastructure Security Agency
CTEP	CISA Tabletop Exercise Package
DHS	Department of Homeland Security
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
EPT	Exercise Planning Team
FBI	Federal Bureau of Investigation
HPH	Healthcare and Public Health
IED	Improvised Explosive Device
IP	Improvement Plan
MOU	Memorandum of Understanding
NTAS	National Terrorism Advisory System
PIO	Public Information Officer
POC	Point of Contact
SitMan	Situation Manual
SME	Subject Matter Expert
TTX	Tabletop Exercise


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY